

Kroll

A Division of
DUFF & PHELPS

Global Fraud and Risk Report 2019/20

MAPPING THE NEW RISK LANDSCAPE

11TH ANNUAL EDITION



Contents

RESEARCH FINDINGS	01	COUNTRY/REGION OVERVIEWS	73
Preface	01	Global Risk Map	73
Research Summary: The Broadening of the Risk Landscape	02	NORTH AMERICA	
		Canada	75
		United States	77
RISK, RELATIONSHIPS AND REPUTATION	14	EUROPE, MIDDLE EAST AND AFRICA	
Holistic Due Diligence in the Age of Relationships	15	Italy	79
Fake News, Real Problems: Combating Social Media Disinformation	19	Middle East	81
The Case of the Telltale Tree: Digital Sleuthing for Asset Recovery	21	Russia	83
Reputation on the (Goal) Line: Shielding the Club Brand in the Sponsorship Arena	23	Sub-Saharan Africa	85
		United Kingdom	87
RISK MANAGEMENT IN PRACTICE	26	ASIA	
Thinking Like a Creditor	27	China	89
Avoiding a False Sense of Security	29	India	91
IP Protection in a Borderless World	33	Japan	93
The Seven Elements of Successful Investigations	37	LATIN AMERICA	
		Brazil	95
		Colombia	97
		Mexico	99
COMPLIANCE	40	INDUSTRY OVERVIEWS	101
Why Compliance Programs Fail	41	Industry Risk Map	101
Keeping Growing Pains Under Control: Expanding the Business—but Not the Risk of Fraud	43	Construction, Engineering and Infrastructure	103
Beyond Compliance: Creating a Culture of Integrity	47	Consumer Goods	105
		Extractives	107
		Financial Services	109
TECHNOLOGY	52	Life Sciences	111
Proceed with Caution: Using Controls to Manage Risk in Digital Currency Transactions	53	Manufacturing	113
Harnessing Machine Learning for Due Diligence: Realizing the Possibilities	57	Professional Services	115
Cybersecurity Breaks Out of Its Silo	59	Retail, Wholesale and Distribution	117
		Technology, Media and Telecoms	119
		Transportation, Leisure and Tourism	121
RISK ON THE GLOBAL STAGE	64		
Illicit Fund Flows in Ten Steps	65		
Corruption at Scale: Managing Risk with Governments and State-Owned Enterprises	67		
When Business and Geopolitics Converge	69		

Preface

Since its founding more than 45 years ago, Kroll has worked with corporations, governments and organizations around the world to help them better understand and mitigate risk in all its forms. The nature of corporate risk has evolved dramatically during that period, and so have we. In 2018, Kroll became a division of Duff & Phelps, a global consulting firm that shares our commitment to helping clients maximize, protect and restore value in volatile times. Our association with Duff & Phelps enables us to draw upon an even broader range of resources and expertise to advise boards, CEOs and other decision makers as they navigate a new generation of risks brought about by globalization, digital transformation, geopolitical forces, and other factors.

This year's *Global Fraud and Risk Report*, "Mapping the New Risk Landscape," is the first to be published under the aegis of Duff & Phelps and its Governance, Risk, Investigations and Disputes division. As in previous years, a survey of senior executives, representing a range of industries and countries around the world, forms the heart of the report; we have redesigned the survey to reflect the wider range of threats our clients are now facing and the strategies they are using to counter those risks. The survey findings are accompanied by a collection of articles that probe issues from the role of corporate culture in combating corruption to strategies for addressing social media disinformation. The report concludes with a discussion of research findings pertinent to individual regions and industries.

I hope you will find the 2019 *Global Fraud and Risk Report* to be both a useful guide and a source of thought-provoking ideas for confronting—and thriving in—the expanding risk landscape. We look forward to hearing from you.



CARL JENKINS

**MANAGING DIRECTOR, GLOBAL HEAD
GOVERNANCE, RISK, INVESTIGATIONS
AND DISPUTES**

BOSTON, MA, US

carl.jenkins@duffandphelps.com



**RESEARCH
SUMMARY**

Research Summary: The Broadening of the Risk Landscape

The results of our annual fraud and risk survey reveal a dynamic mix of new and longstanding threats.

Mitigating business risk has always relied on knowledge of markets and counterparties, and of the forces that could disrupt a company's agreements and assumptions. In the pre-digital, pre-global age, gaining such knowledge was made easier by implicit boundaries that governed the way most organizations conducted business.

Suppliers, lenders and business partners were drawn from fairly well-established pools of referrals and contacts. Clearer categories for industries and sectors meant that enterprises knew their place in the larger economic ecosystem, enabling them to adopt and conform to established business models and vocabularies. Growth was often predicated on increasing a product's existing market share or on moving into markets adjacent to those where a solid presence already had been established.

Of course, even in that environment, plenty of risks existed, and naturally the ability of enterprises and their leaders to navigate those risks ranged widely. But it is also fair to say that many aspects of business operated incrementally, and that their incremental nature made navigating risk simpler. This is particularly evident viewed through the lens of the past decade, in which traditional boundaries and assumptions, already weakening, eroded further. Globalization is one example. Not so long ago, "globalization" often meant that enterprises from a handful of developed countries were setting up operations or joint ventures in developing markets. Now the planet has a truly distributed network of business relationships, in which Asia invests in Europe and the Middle East has business partnerships in Latin America. Meanwhile, mobile connectivity and social media have created a digital world in which information asymmetries have greatly lessened, giving rise to different consumer expectations and business models. Those new business models are scrambling the traditional definitions of industries and sectors. All of these developments dramatically increase the number of unknowns—and thus the risks—with which organizations must contend.

The broadening of the risk landscape is visible in the types of significant incidents our survey respondents report experiencing in the last 12 months and in the priority levels they assign to various risk mitigations. The most frequently cited incident is leaks of internal information, reported by 39 percent. But this perennial challenge now coexists with risks from relatively recent threats, such as data theft, and even newer threats, such as adversarial social media activity.

Risk management today is centered on responding to—and trying to stay ahead of—rising threats while continuing to battle long-established risks. Newer risks differ from old ones in their ubiquity. While money laundering and counterfeiting, for example, take the greatest toll on particular industries and countries, virtually every enterprise is potentially vulnerable to social media attacks or collateral damage from a business partner's scandal. Adding urgency to the new risks is the need to establish appropriate systems and capabilities for combating them. So it is that every risk on our list is either a significant or high priority for more than half of our survey respondents.

SURVEY METHODOLOGY

For the 2019 *Global Fraud and Risk Report*, Kroll commissioned Forrester Consulting to conduct an online survey of 588 senior executives who have responsibility for, or significant involvement in, determining their organization's risk management strategies. Survey respondents were drawn from the 13 countries and regions and 10 industries listed in the report's table of contents. Ninety-two percent of the organizations operate in more than one country, and 55 percent have annual revenues of \$1 billion or more. The survey was conducted in March and April 2019.

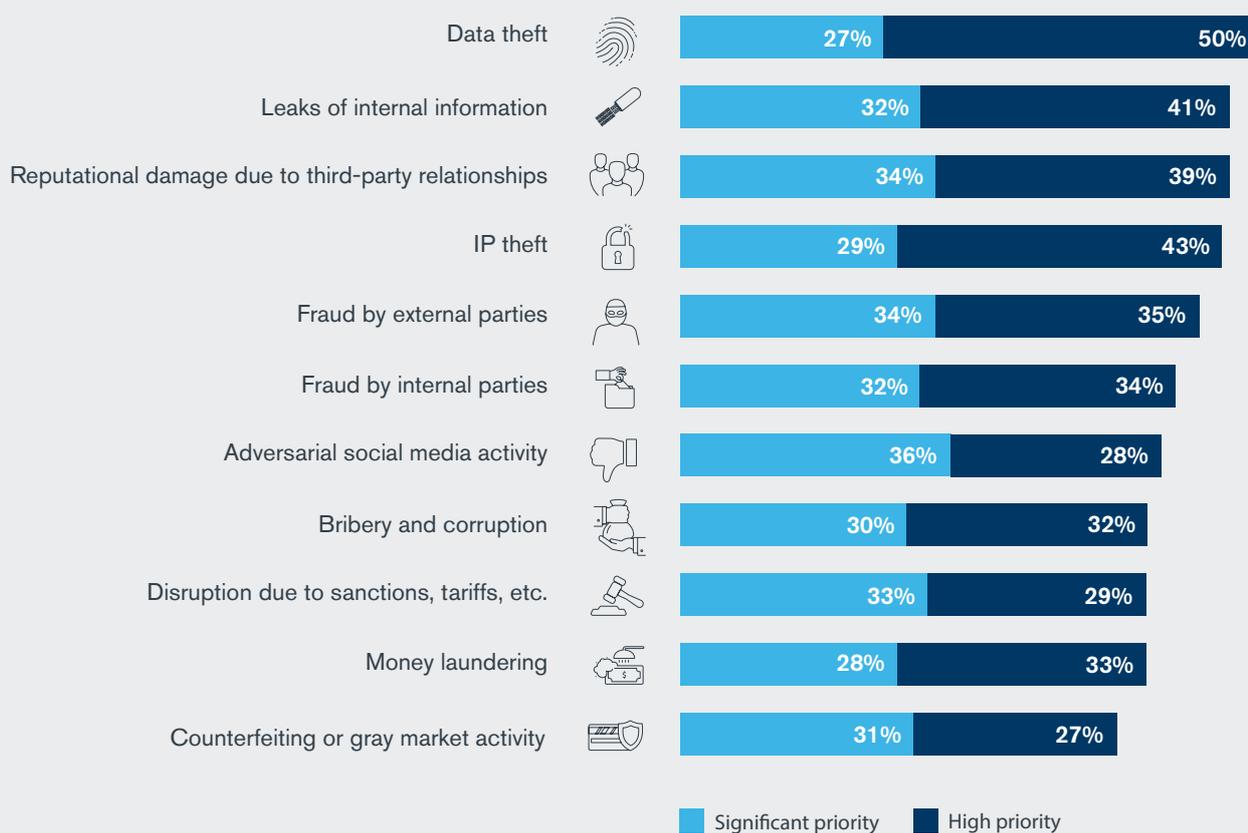
FIGURE 01

WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED ORGANIZATIONS IN THE LAST YEAR?



FIGURE 02

WHICH RISKS ARE PRIORITIES FOR RESPONDENTS?



The Who, How and Where of Risk

PERPETRATORS EVERYWHERE

The results of our survey confirm that threats can originate from any point in the web of an organization's relationships. No more than 13 percent of any of the various types of incidents discussed in our survey were committed by unknown actors—and often their percentage was in the low single digits. Generally, threats come from those within the organization and within the other organizations in its network. At the same time, while threats can come from anywhere, particular types of threats are more likely to come from certain actors.

Employees, more than any other entity, are responsible for internal fraud and leaks of internal information. This is not surprising. But our survey results also reveal that this group perpetrates the greatest share of data theft. Moreover, employees are a significant source of reputational damage and the leading source of bribery and corruption incidents. This last point serves as a reminder that while regulations against bribery and corruption typically focus on third parties, such incidents usually require a willing participant inside the organization.

Third parties such as **joint venture partners, suppliers and vendors** can be thought of as hybrids of internal and external entities, and this hybrid nature is evidenced by the wide range of incidents in which they play a part. For example, third parties are the leading cause of reputational damage, befitting their external position. Reputational damage has always been a risk of working with third parties, but now that risk has been heightened by greater public sensitivity to reputation by association, and amplified by constant citizen surveillance via social networks. Third parties are also the main source of problems stemming from sanctions and tariffs, demonstrating

the ripple effects of these policies. Meanwhile, the internal access granted to third parties enables them to be the leading cause of counterfeiting as well as significant perpetrators of data theft. Finally, they are a primary vector of adversarial social media activity, second only to an organization's competitors.

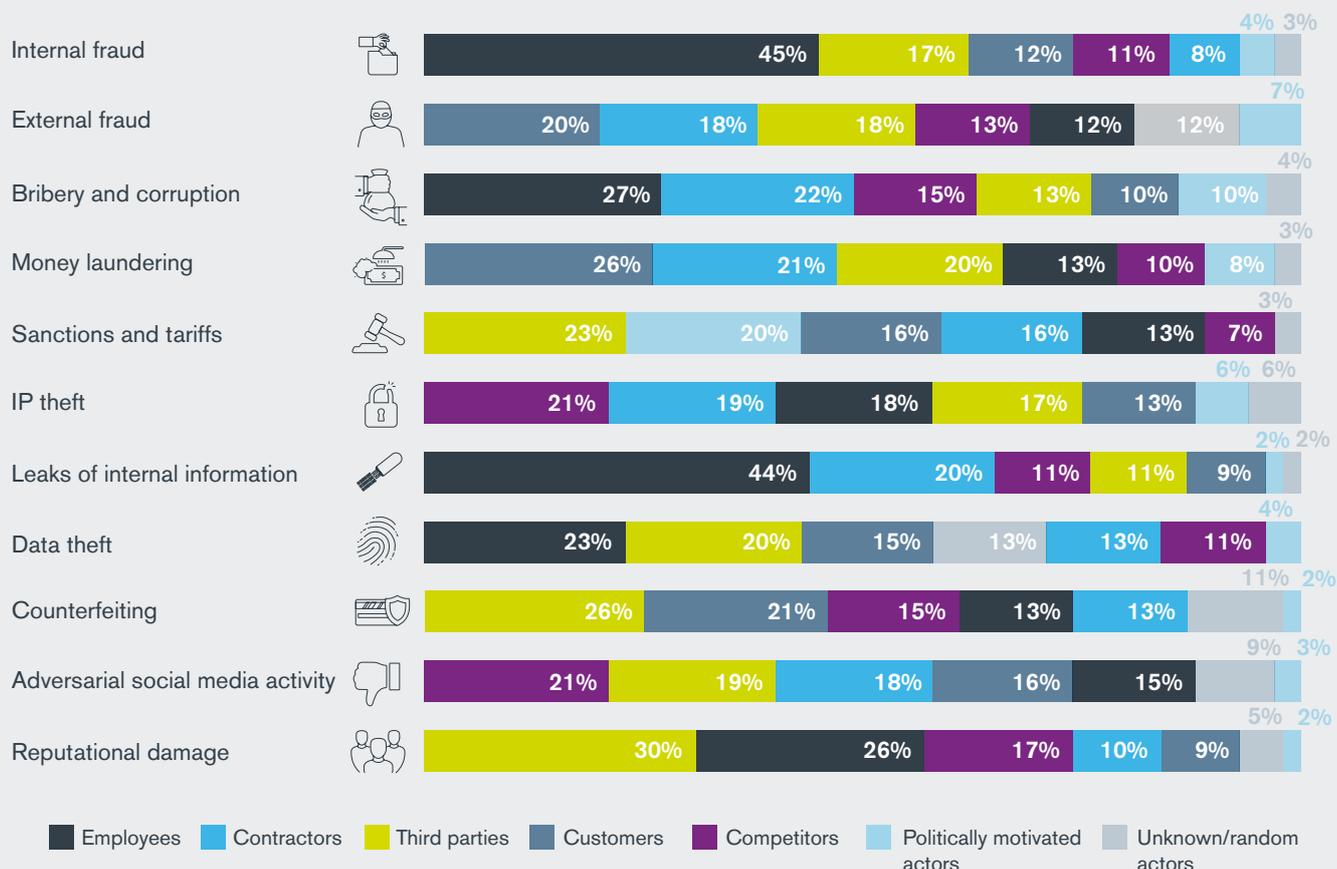
Today's business models have made **contractors** increasingly important at many organizations, but as with third-party business partners, there are risks associated with granting them insider access. Contractors are a major source of IP theft as well as of adversarial social media activity.

Reputational damage has always been a risk of working with third parties, but now that risk has been heightened by greater public sensitivity to reputation by association.

Customers and **competitors** are purely outsiders, and this status shapes the risks they pose. Competitors are the leading cause of both adversarial social media activity and IP theft, whereas customers are most often associated with money laundering and external fraud.

FIGURE 03

WHO ARE THE KEY PERPETRATORS OF EACH TYPE OF THREAT?*



THE DIGITAL TRANSFORMATION OF CRIME

The last decade has seen cybercrime evolve from an IT issue to a boardroom concern, mirroring the digital transformation of the global economy on the macro level and of business operations on the micro level. The more the business world integrates digital elements, the more likely it is that computer systems have or will become a pathway for crime.

Our survey shows that, while certain incidents are more likely to involve a large cyber component, cyber intrusions cause at least some instances of every type of adverse event. Furthermore, even in categories of incidents where cybersecurity breaches are endemic, perpetrators also commit analog crimes. For example, cyber breaches were most likely to be a factor in data theft, leaks of internal information and IP theft. But even for these transgressions, cybersecurity deficiencies played a central role less than half the time.

The conclusion is clear: As with so many other silos, the one isolating digital systems and assets has broken down. Cybersecurity needs to be integrated into an organization's overall risk management strategy. (For more details from our survey results, see "Cybersecurity Breaks Out of Its Silo," page 59).

Cyber breaches played a primary role in 42 percent of incidents involving reputational damage from third-party relationships. This fact highlights the importance of vetting a counterparty's cybersecurity practices when conducting due diligence. Indeed, for bad actors, exploiting the cyber vulnerabilities of business partners and software providers is a time-tested method of gaining access to the fortified systems of larger organizations with significant digital assets.

*"Don't know/Not applicable" responses excluded. Percentages do not total 100 percent due to rounding.

Mitigation Methods and Mindsets

THE CURRENCY OF REPUTATION

More than ever before, organizations are judged by the company they keep. A supplier that is found to violate child labor laws, a high-profile promoter of the brand who is responsible for inflammatory posts on social media (no matter how long ago), a board member with unresolved allegations of sexual harassment—all of these relationships can quickly escalate into full-blown corporate crises. Thus, to protect an organization's reputation, its leaders must compile a fuller picture of its counterparties' business practices, operations, community standing, and personal and business relationships. Such information is also critical in connection with loans and other agreements where asset recovery may be necessary.

Our survey shows that most organizations have expanded their traditional financial and legal due diligence processes to include these broader reputational concerns. When considering the various due diligence subjects covered in our survey, respondents report conducting some level of reputational due diligence at least 79 percent of the time.

However, the data also show that organizations are still working to incorporate reputational factors more fully into their overall due diligence processes. Ideally, reputational due diligence should be conducted at onboarding and throughout the duration of the relationship, whether on a regular schedule or in response to the third party's risk rating. Few companies accomplish this. Some consider reputational factors at onboarding only, while others postpone addressing reputational factors until after onboarding.

Notably, 21 percent of respondents report that they conduct no due diligence on investors. In an earlier time, when companies typically dealt with smaller pools of known investors, it may have been safe to let the money speak for itself. In today's risk environment, however, reputational risk can emerge from any party with which an organization is associated, so it is essential to know where the investors' capital comes from and to identify the other enterprises in which the investors may have a stake.

FIGURE 04
WHEN DO ORGANIZATIONS CONDUCT REPUTATIONAL DUE DILIGENCE ON THIRD PARTIES?*

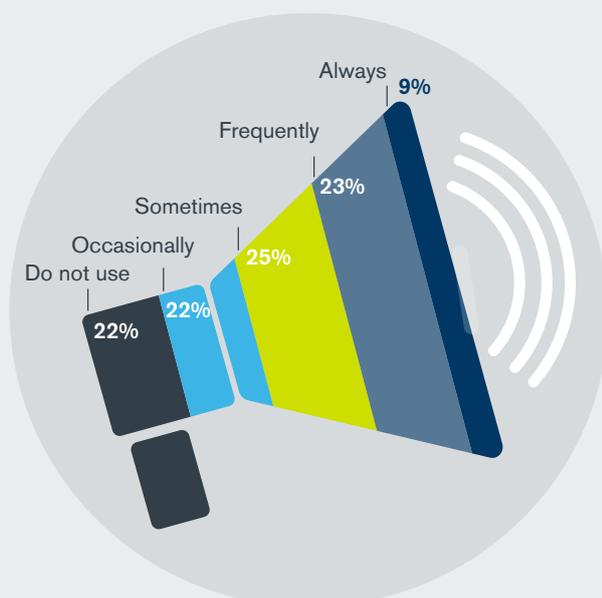
DUE DILIGENCE SUBJECT	AT ONBOARDING ONLY	AT ONBOARDING AND ACCORDING TO FIXED SCHEDULE	AT ONBOARDING AND ACCORDING TO RISK RATING	ACCORDING TO FIXED SCHEDULE ONLY	ACCORDING TO RISK RATING ONLY	NO REPUTATIONAL DUE DILIGENCE CONDUCTED
Board or senior executive candidates	32%	10%	9%	25%	16%	9%
M&A targets	31%	12%	12%	0%	30%	16%
Suppliers	26%	12%	12%	40%	0%	10%
Investors	25%	10%	12%	33%	0%	21%
Business partners	19%	8%	9%	28%	28%	8%
Brand ambassadors or influencers	19%	7%	3%	29%	26%	15%
Customers	15%	8%	10%	28%	27%	12%

*Asked only of respondents whose organizations work with these groups.

The importance of thorough reputational due diligence can be seen in how frequently such investigations prompt organizations to take action. Forty percent of respondents report having uncovered bribery, corruption or sexual harassment issues at a level sufficient for them to terminate a potential or existing relationship. Almost half of survey respondents required potential affiliates and other third parties to remediate shortcomings in their data-handling procedures; problems involving social media and the subjects' own third-party relationships needed to be rectified nearly as often. (For relevant details from the survey, see "Holistic Due Diligence in the Age of Relationships," page 15.)

The extent to which reputation has become a valuable corporate asset can be seen in the widespread adoption of brand ambassadors and influencers, used to some extent by 78 percent of survey respondents. Businesses have long employed celebrities and other high-profile people for endorsements, but the power of social media has upped the ante: Now the influencer provides the organization with not only an endorsement but also—and even more importantly—access to an extended network.

FIGURE 05
HOW OFTEN DO ORGANIZATIONS USE
BRAND AMBASSADORS OR INFLUENCERS?*



*Percentages do not total 100 percent due to rounding.

78%
of survey respondents use
brand ambassadors
or influencers

THREAT DETECTION: WHEN TIME IS OF THE ESSENCE

Risk management often centers on prevention, yet other components—such as detection, response and recovery—are equally critical. In this year’s survey, we asked respondents to rate aspects of their organization’s detection capabilities in light of significant risk incidents their organization had experienced within the last year.

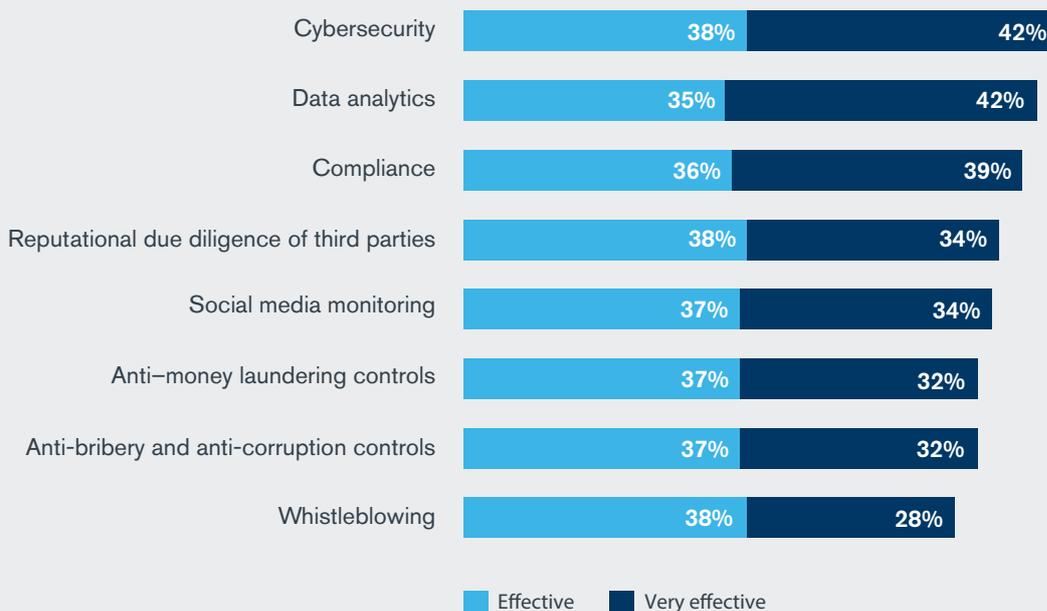
Most organizations rate their detection mechanisms as either “effective” or “very effective.” Respondents are most likely to give high marks to their organization’s cybersecurity capabilities. But this finding warrants closer examination. In reality, most cyber intrusions take place months or years before they are detected. This lag allows, for example, the sale of stolen passwords on underground marketplaces and unauthorized access to customer accounts for long periods before the breach is discovered. And during the period between breach and discovery, the organization has no reason to think its cybersecurity is anything but fine.

A different lesson can be drawn from the place of whistleblowing at the bottom of the list. Establishing a

whistleblowing program that meets regulatory requirements can be fairly straightforward. But creating an *effective* whistleblowing program—one that preserves confidentiality (if not anonymity), investigates cases in a timely manner and resolves them in a consistent way—is a challenge. Such a program requires that whistleblowing be supported with sufficient resources and integrated with functions throughout the organization. It demands adequate staffing of call centers along with prompt analysis and escalation of sensitive incidents. Failing to establish these and similar protocols will undermine both the program’s effectiveness and its credibility.

That respondents give their detection mechanisms high marks suggests a broad recognition that internal detection is crucial for risk management. For that reason, organizations would do well to assess those detection systems with a critical eye, considering not just functionality but also speed and accuracy. Organizations can ensure their detection systems’ effectiveness by providing them with appropriate resources throughout the enterprise.

FIGURE 06
HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS?



THE COLLECTIVE TASK OF DISCOVERY

In this report, we stress the notion that many risks to an organization emanate from its network of lenders, investors, business partners, customers and competitors, among others. Yet just as risks arise from many quarters, so too does incident detection. Predictably, internal and external audits play a leading role; together they account for between 36 and 58 percent of incident discovery, depending on the type of transgression. The sizable remainder underscores the importance of other entities: whistleblowers, customers, suppliers, company management, regulators and law enforcement.

This array of participants highlights the challenges currently facing the internal audit function. Addressing each new threat requires the organization to develop appropriate procedures and capabilities. Monitoring social media activity, for example, calls for different tools, practices and training compared with the detecting money laundering. To secure the organization in this ever-expanding risk landscape, internal audit must identify priorities and fight for resources.

One notable finding from our survey is that although internal audit uncovers the largest share of bribery and corruption incidents, it is only marginally more effective in doing so than whistleblowing. Whistleblowing is an important element in the incident detection ecology, but it is a relatively extreme measure; people who take that step often do so because they lack confidence that normal organizational channels will address the problem. Indeed, whistleblowing may not take place until after significant damage has already been done.

Consequently, organizations can benefit from paying closer attention to their internal practices for detecting bribery and corruption. The use of proactive data analytics, for example, can enable management to identify problems before they escalate.

FIGURE 07
HOW WERE INCIDENTS DISCOVERED?*

INCIDENT	INTERNAL AUDIT	EXTERNAL AUDIT	WHISTLE-BLOWER	CUSTOMERS/SUPPLIERS	REGULATOR/LAW ENFORCEMENT	COMPANY MANAGEMENT
Reputational damage due to third-party relationships	32%	12%	9%	17%	12%	16%
Leaks of internal information	35%	14%	12%	13%	8%	18%
Adversarial social media activity	19%	22%	12%	15%	12%	19%
Disruption due to sanctions, tariffs, etc.	22%	12%	11%	16%	19%	20%
IP theft (e.g., trade secrets)	30%	13%	15%	11%	17%	13%
Data theft (e.g., customer records)	37%	16%	8%	11%	12%	14%
Counterfeiting or gray market activity	19%	17%	15%	12%	21%	18%
Money laundering	22%	18%	13%	15%	18%	13%
Fraud by internal parties	38%	20%	11%	10%	5%	15%
Fraud by external parties	19%	25%	15%	15%	12%	15%
Bribery and corruption	24%	14%	21%	13%	14%	15%

* "Don't know/Not applicable" responses excluded. Percentages do not total 100 percent due to rounding.

CULTURE AS A LINE OF DEFENSE

Organizations need strong internal mechanisms for detecting fraud, corruption, compliance failures and other incidents—but the effectiveness of such mechanisms may be undercut by the organization’s culture. Cultures in which personnel consider checks and balances to be a tax on the normal course of business make themselves more vulnerable to adverse incidents than do organizational cultures that stress transparency and accountability as business best practices.

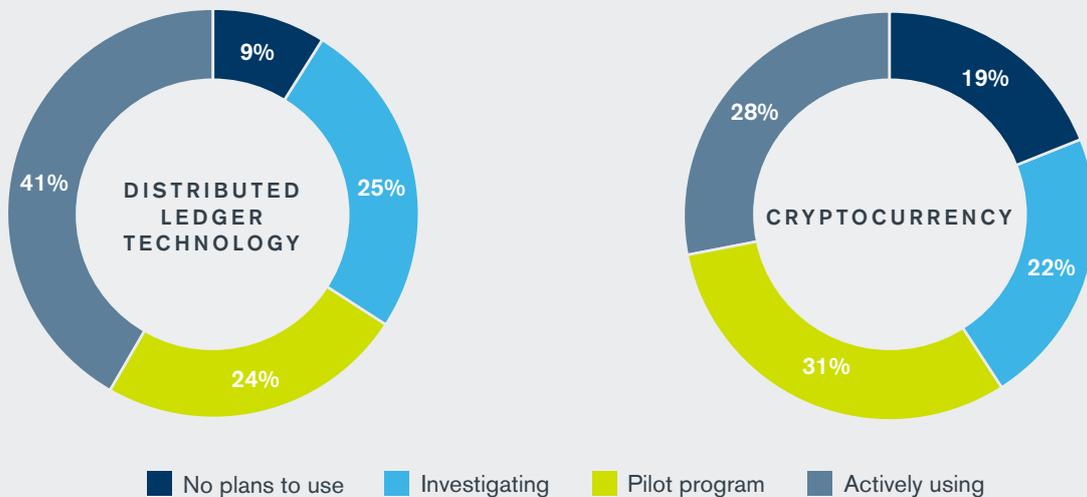
In our work on these issues with clients around the globe, we have identified a number of factors that affect the ability of an organization to build and sustain such a culture, including establishing the proper tone from the top, aligning performance goals with ethical behavior and providing ongoing education to help employees navigate ambiguous situations. Eight practices for building a culture of integrity are discussed in our survey; each of them is followed by approximately three-quarters of respondents. (For survey results in detail, see “Beyond Compliance: Creating a Culture of Integrity,” page 47.)

Widening the Aperture

GEOPOLITICS

The globalization of the world economy is largely the result of deliberate policy choices made in the period following the end of the Cold War. In recent years, however, the foundations of globalization have been weakened by greater protectionism, rising diplomatic tensions and governments’ inclination to use economic policy to pursue foreign policy objectives. Meanwhile, cross-border investment and trade have reached new heights—increasing the impact that geopolitical developments can have. As a result, organizations are incorporating geopolitical factors into their risk assessments. For each type of geopolitical risk mentioned in our survey—ranging from political unrest to government influence on a counterparty such as a business partner or supplier—approximately half of those surveyed reported that their organizations had been affected to some extent. Practices such as actively monitoring their counterparties’ local political and economic climate and knowing their organization’s total exposure by jurisdiction were followed by at least two-thirds of the organizations surveyed. (For these survey results in detail, see “When Business and Geopolitics Converge,” page 69.)

FIGURE 08
ADOPTION OF DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOCURRENCY



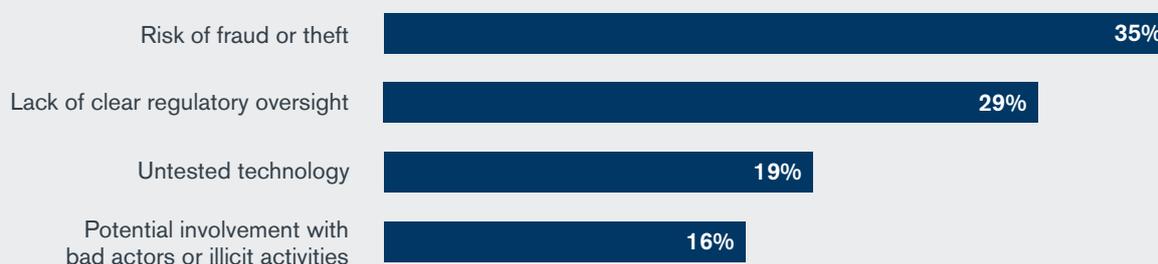
EMERGING DIGITAL ASSET TECHNOLOGIES

In the first phase of the digital transformation of business, participants focused on building an infrastructure that was suitable for commerce. Databases and networks were created and standardized to establish a digital world that mirrors analog reality. Now we are deep into the second phase of transformation, in which data determines what is “real” and which digital objects can take on monetary value. Two recent developments, distributed ledger technology and cryptocurrency, have the potential to further scramble the business world’s conventions and assumptions. Despite the uncertainty surrounding these innovations, most people acknowledge that they will, in some form, figure into the digital infrastructure of the future. Only 9 percent of survey respondents say their organizations have no plans to incorporate distributed ledger technology, while 19 percent have no plans to use cryptocurrency (see Figure 8). Given that cryptocurrency is exchanged using distributed ledger technology, the lag in cryptocurrency’s adoption suggests respondents feel somewhat wary about employing that technology to create assets, as opposed to merely tracking their ownership.

New technologies open new frontiers. They also introduce a variety of risks. The technology itself may fail to deliver, as may the business models built around those technologies. Companies may be outmaneuvered by more innovative or agile competitors. In the interim, it takes time to adequately regulate new business environments and to establish sufficient controls, whether dictated by regulation or best practices. Consider, for example, the extent to which society is still discovering risks associated with social media, and the resulting struggle to address its fundamental problems with regulatory measures that also preserve established rights.

These concerns weigh heavily on business decision makers. Asked to name the single largest concern they have with distributed ledger technology and cryptocurrency, our survey respondents say they are far less concerned about the technologies themselves than about operating in that realm before the regulations and practices necessary to prevent fraud and theft have been established (see Figure 9).

FIGURE 09
GREATEST CONCERN REGARDING DISTRIBUTED LEDGER TECHNOLOGY AND CRYPTOCURRENCY



RISKS OF THE FUTURE

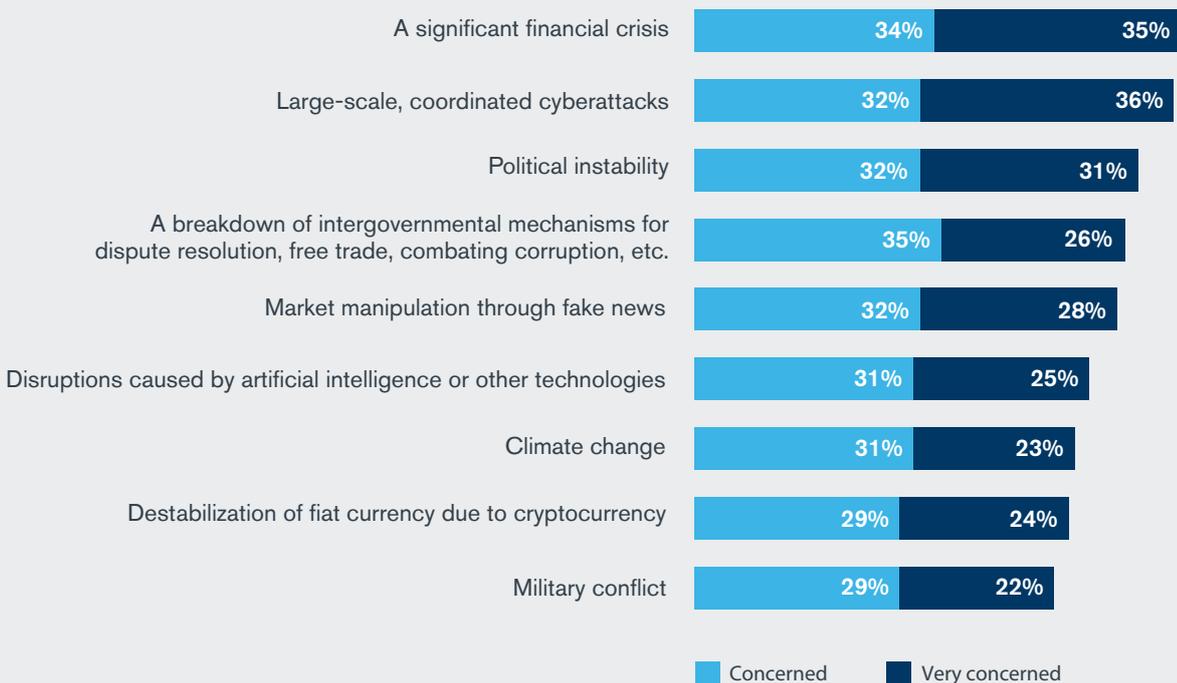
Organizations have a full agenda as they come to grips with the current expansion of the risk landscape. Yet that landscape will continue to expand and become increasingly complex as various technological, political and ecological forces develop and combine in unforeseen ways. Attempting to anticipate future risks that could have a broad impact allows organizations to factor those risks into their long-term decision making and begin mitigating them before a potential crisis hits.

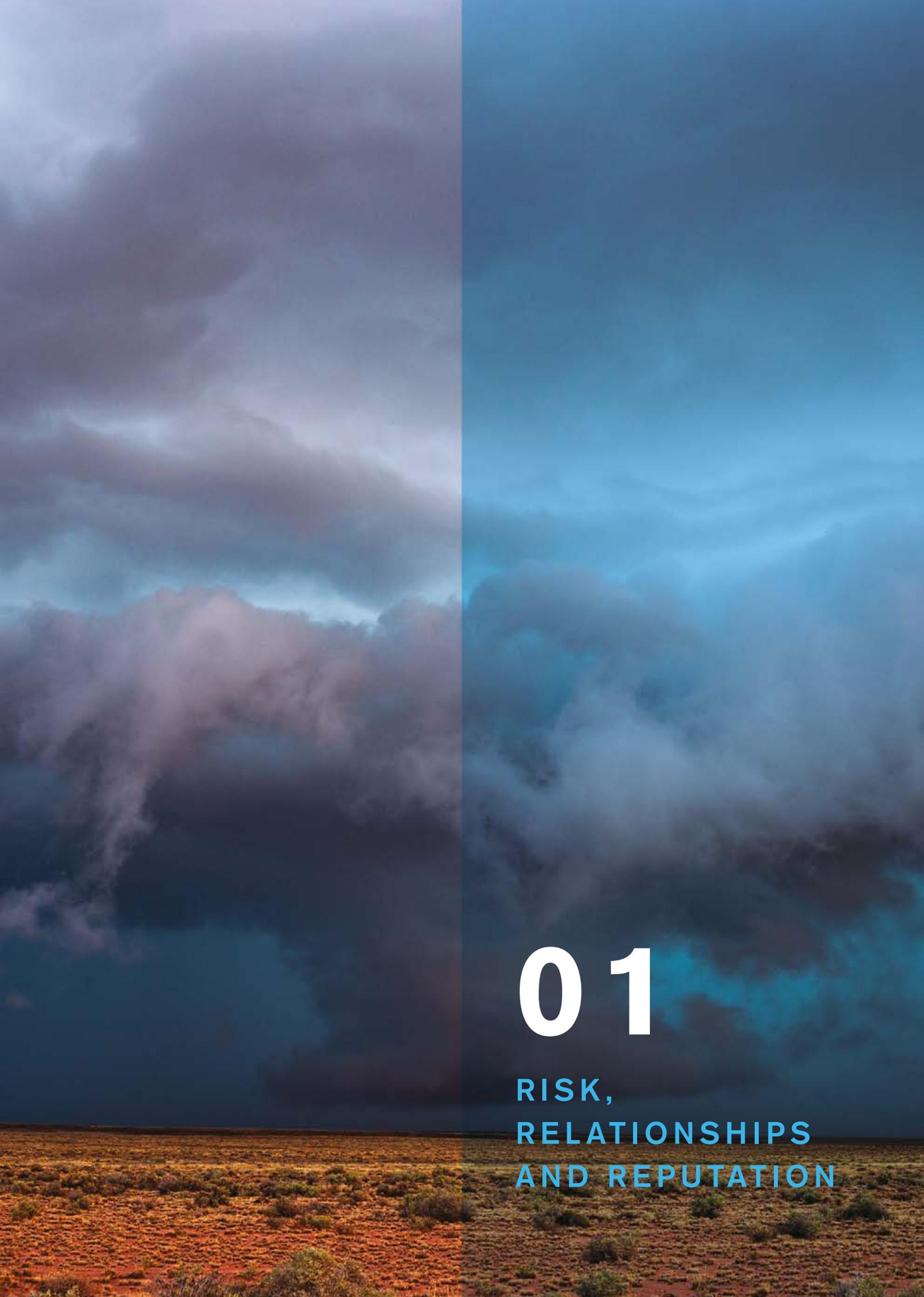
While at least half of the survey respondents expressed concern about every risk we mentioned, they worry particularly about the possibility of another financial crisis or a widespread cyberattack that might disable multiple infrastructure systems simultaneously. This may be because such scenarios echo current and recent history: the 2008 financial crisis and the ongoing waves of data breaches that have been disrupting digital commerce.

At the same time, the fact that so many respondents are concerned about all risk types illustrates how broadly decision makers are having to think about threats in today's highly volatile environment. Consider, for example, the 60 percent of respondents who expressed concern about market manipulation through fake news. Market manipulation due to disinformation is nothing new, but the possibility today is much greater given the ability of bad actors to introduce false or altered information into the internet's rapidly moving data stream.

The future risks most likely to elicit concern are those that echo current and recent history.

FIGURE 10
LOOKING AHEAD FIVE YEARS, WHICH RISKS ARE OF GREATEST CONCERN?





01

RISK,
RELATIONSHIPS
AND REPUTATION

Holistic Due Diligence in the Age of Relationships

As value chains grow and social media creates a web of continual scrutiny, organizations need to know their business partners and customers as never before.

The idea of the organization as a self-contained entity is giving way to the realization that an organization is a single node in a network of relationships—with social media and viral videos putting every element of that network under relentless scrutiny. Third parties have become increasingly central in virtually every sector. Collaboration and partnerships provide the agility and new resources needed for innovation. Globalization has created a wealth of new markets and new suppliers. Social media marketing campaigns rely on “influencers” and “brand ambassadors” to build online followings.

When an enterprise is defined in large part by its relationships, a new level of due diligence is necessary to assess and mitigate the risk of those relationships. Historically, due diligence has centered on legal and financial issues. In recent years, due diligence has expanded to incorporate other issues, such as a potential partner’s ownership structure and cash flows (owing to sanctions) and cybersecurity and data privacy practices (owing to regulations and public expectations). Today, reputational risk is further expanding the concept of due diligence, covering issues such as workplace conditions; social media activity; business practices; and the subject’s own network of customer, supplier and lender relationships.

Due diligence is also becoming bilateral, reflecting the fact that reputational risk flows both ways. A company that sells an asset to a buyer that runs into regulatory problems, maintains substandard working conditions or merely mismanages a once-thriving business can no longer expect those problems to stay exclusively with the buyer; the seller’s reputation may be affected as well.

Our survey found that 79 percent or more of organizations are incorporating reputational factors into their due diligence of candidates for board seats, investors, brand ambassadors and other third parties, depending on the person or entity involved. However, our experience working with clients suggests that organizations vary greatly in their ability to execute a holistic due diligence strategy that is systematic, sustainable and risk-based.



STEVEN BOCK

Managing Director, Global Head
Compliance Risk and Diligence

New York, NY, US
steven.bock@kroll.com



KEVIN BRAINE

Managing Director, EMEA Head
Compliance Risk and Diligence

London, UK
kevin.braine@kroll.com

CREATE THE RISK PROFILE

There is no effective one-size-fits-all approach to due diligence; every relationship brings its own set of potential risks and issues. The first step is thus for the organization to create a risk profile of the party in question. That party's **applicable regulatory regimes** provide a starting point. A publicly held company in North America or Western Europe is likely to already be under multiple layers of regulatory scrutiny. In such cases, due diligence is still necessary, but less may be needed because much has already been done by others. At the other end of the risk spectrum, a third party that is privately held in a country with weak anti-corruption enforcement would warrant closer examination.

The **industry** of the third party is another important element. Certain industries, such as import/export, have relatively high concentrations of illicit activity. Similarly, industries like cryptocurrency and gaming may have still-evolving regulatory structures and thus a greater potential to attract bad actors. Alternatively, a particular industry in a given jurisdiction may have well-developed regulatory regimes but a poor collective track record of enforcement or compliance.

But regulatory compliance is only the start. Given the wide range of non-regulatory standards across jurisdictions for issues such as business practices, working conditions and

sustainability, it is entirely possible for a third party to be in compliance with local regulations yet still represent a reputational risk. Indeed, merely identifying which issues to examine can be challenging, requiring a close understanding of the third party's business. For example, if their products use mica—a ingredient found in everything from cosmetics to metallic paint—they need to be sure that they do not source it from suppliers linked to illegal mining operations using child labor. This is one illustration of the level of holistic thinking required today to stay ahead of a reputational crisis.

Finally, consider the **nature of the relationship**—the product or service in question, the size of the contract and the level of involvement with the organization's brand identity. A provider of mission-critical software or a franchisee carrying the company's name is likely to warrant a deeper level of scrutiny than an office-supply vendor.

While each potential relationship requires its own risk profile based on these factors, certain combinations of risk variables will recur, enabling organizations to create over time a portfolio of risk profile templates that can make the due diligence process more efficient. Such templates remain useful after the onboarding process as rubrics for periodic monitoring of any subsequent changes in the third party's business or standing.

MAP BREADTH AND DEPTH

Having established a relationship's risk profile, one can then determine the breadth and depth of the data collection process so that particular areas of concern can receive more-thorough treatment. Consider the example of an M&A target. It is standard practice to examine the personal and professional histories of management team members. One could also choose to gather similar information on their family members and prior business associates. Similarly, due diligence on a supplier might include examining the due diligence of their own suppliers. Each additional step, however, requires more time and greater commitment of finite resources.

The sheer number of relationships to manage and the amount of information to be gathered about each one make merely collecting the data a significant task. But if due diligence stops here, it is incomplete, with information taken at face value and dots remaining unconnected. A truly holistic approach to due diligence requires depth as well as breadth. For example, does

a company that represents itself as a commodities broker have a history that aligns with the number of transactions it purports to conduct? How transparent is the beneficial ownership of the various entities that emerge in an examination of transactions? Digital facades are easy to construct; questions such as these can help expose the structure underneath. But here too, organizations must balance the value of additional information against the expenditure of time and resources.

Whatever the scope of the data collection process, it needs to include a thorough screening of social media posts. It goes without saying that anything objectionable or controversial should raise red flags. But scrutinizing social media activity of a potential executive hire, for example, can also provide significant insight into the person's values and behavior, which can then be examined for his or her fit with the brand image and corporate culture.

BUILD A RESPONSE MECHANISM

Once information has been collected, the exceptions and adverse effects need to be translated into **timely and proportionate action**. This is not trivial. Consider how often post-crisis investigations uncover red flags that had been ignored. Conversely, a hair-trigger negative response can derail valuable relationships. The guiding principle needs to be the extent to which, when combined with other information, the adverse event—a CEO with a DUI, a facility with safety violations—constitutes a risk indicator sufficient to cause a rethinking of the relationship. Local context is also important, particularly when considering third parties in other jurisdictions. The significance of having a police record, for example, can vary greatly from country to country. But even in cases without cross-border considerations, the data amassed on a subject will vary in its reliability and importance and cannot be taken at face value. Instead, companies need to develop a response

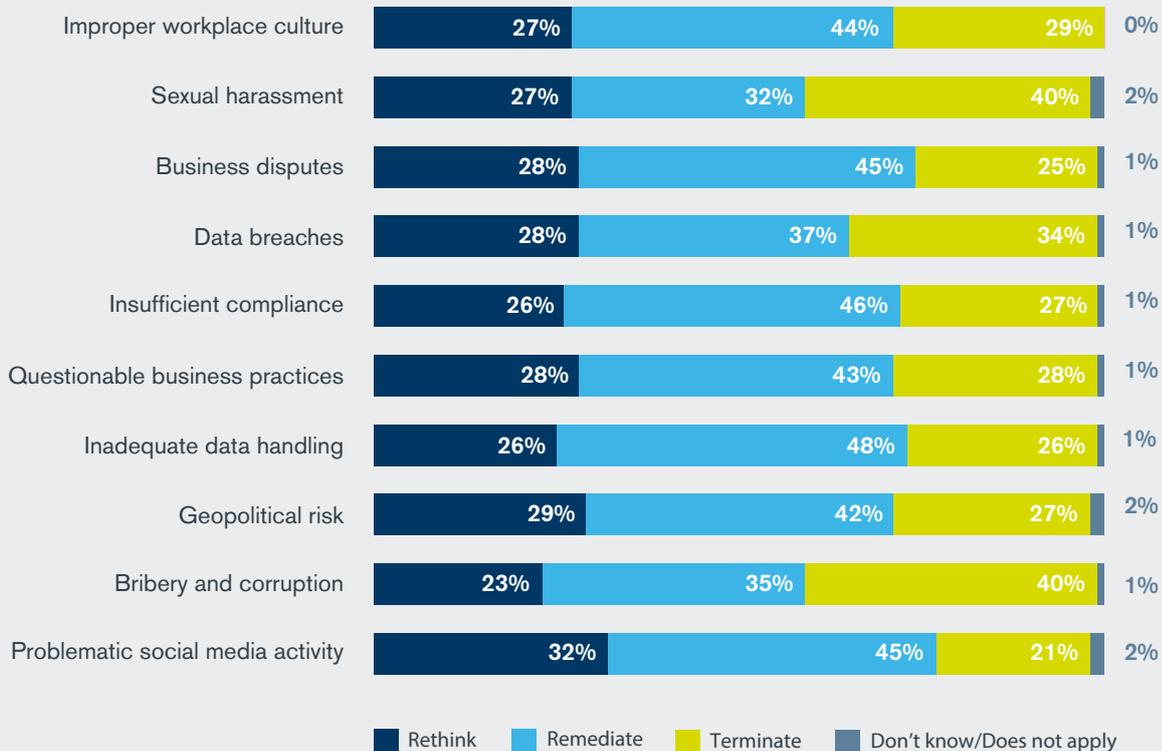
mechanism to help them evaluate what they find. As part of that mechanism, it can be useful to assign adverse information to one of three categories:

- **Rethink:** immediate action not warranted based on the information uncovered, but the issue should be noted and monitored
- **Remediate:** situations that need to be addressed as a prerequisite for pursuing the relationship
- **Terminate:** grounds to end the relationship

Even though such categorization is subjective, it provides a framework for acting on due diligence findings.

The importance of reputational due diligence can be seen in the frequency with which it uncovers issues that fall into one of the above categories (see Figure 11).

FIGURE 11
WHAT ISSUES HAVE BEEN UNCOVERED AND ACTIONS TAKEN IN RESPONSE TO DUE DILIGENCE DISCOVERIES?*



*Percentages do not total 100 percent due to rounding.

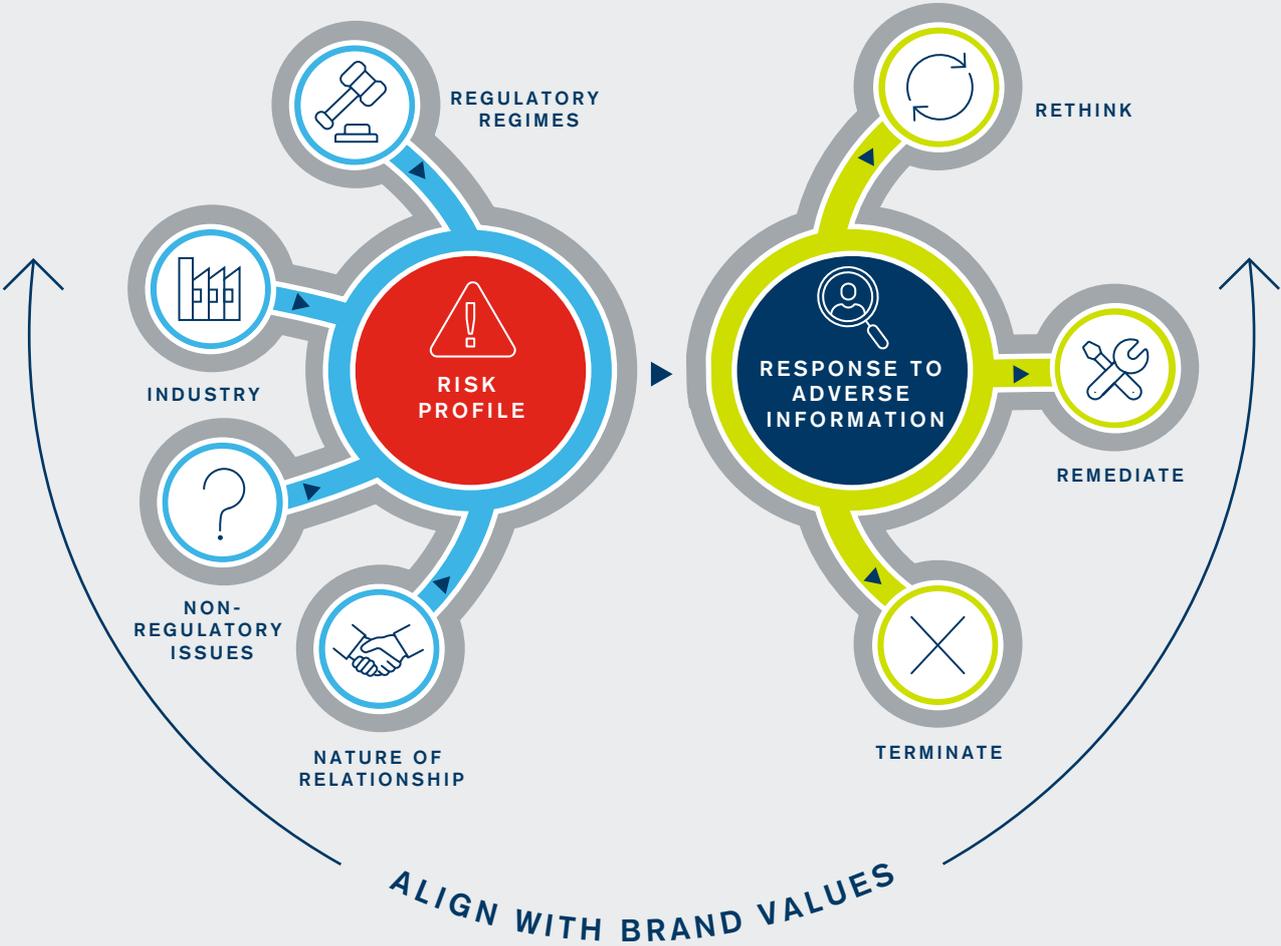
ALIGN WITH BRAND VALUES

Historically, the main drivers for due diligence have been transactions and compliance requirements, leading some people to view due diligence as a housekeeping task. However, the always-on hyper-network of traditional and social media, combined with rising public expectations for corporate citizenship, has greatly increased the importance of reputational issues. Because due diligence plays a critical role in mitigating that risk, the due diligence process must reflect the organization's brand values. Enterprises with high profiles in corporate social responsibility, for example, will want to

pay extra attention to those issues. Global consumer brands should ensure that their extensive supply and distribution chains reflect their messaging as much as their marketing and advertising do.

In an environment of greater scrutiny, higher risk and more unknowns, due diligence requires more effort than it once did. However, that effort can reap rewards that render due diligence not just a necessary task but also an important differentiator and strategic asset.

FIGURE 12
REPUTATIONAL DUE DILIGENCE IN ACTION





ALEXANDER BOOTH

Associate Managing Director
 Business Intelligence and
 Investigations
 London, UK
 abooth@kroll.com



BENEDICT HAMILTON

Managing Director
 Business Intelligence and
 Investigations
 London, UK
 bhamilton@kroll.com



MARIANNA VINTIADIS

Managing Director, Southern
 Europe Head
 Business Intelligence and
 Investigations
 Milan, Italy
 mvintiadis@kroll.com

Fake News, Real Problems: Combating Social Media Disinformation

Social media is a powerful tool for brand building and communication—and a double-edged sword that can cause significant damage in the hands of an adversary.

Brands have been valuable assets since before the first trademark was granted. For much of that time, companies were able to control and shape their brands through their marketing, advertising and other communications strategies. Today, however, social media has transferred much of that control to online communities. Under the right conditions, a small band of loyalists can grow virally into a dedicated following and give a company or a cause a global presence seemingly overnight. But adversaries ranging from competitors to short sellers can harness the same platform to hijack the reputation of a company or one of its employees through fake news stories, malicious posts and other underhanded tactics, as illustrated by these recent Kroll engagements:



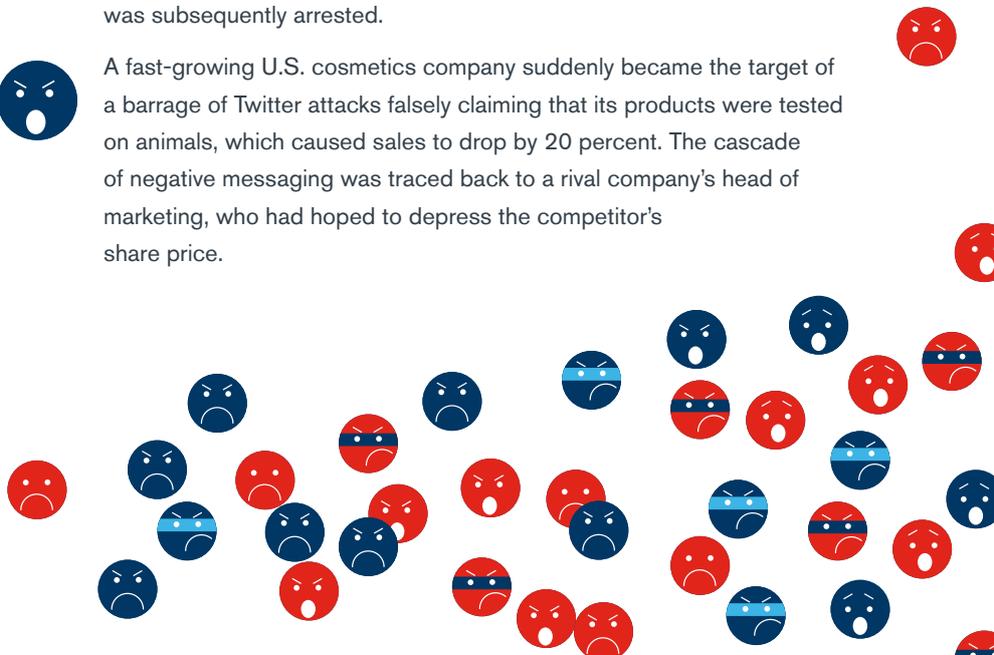
After an African bank was purchased by a rival institution, the purchaser was confronted with a negative social media campaign, complete with fabricated news stories and manipulated closed-circuit television footage. The instigators turned out to be a group of shareholders of the acquired bank who had opposed the sale.



An employee of an authorized repair center of a global automobile manufacturer found her social media page filled with photos of herself and her children that had been photoshopped onto pornographic images. The perpetrator was identified as a disgruntled customer, who was subsequently arrested.



A fast-growing U.S. cosmetics company suddenly became the target of a barrage of Twitter attacks falsely claiming that its products were tested on animals, which caused sales to drop by 20 percent. The cascade of negative messaging was traced back to a rival company's head of marketing, who had hoped to depress the competitor's share price.





As with other types of threats, like cyberattacks or physical security breaches, early detection and quick response are essential when a company or brand faces an online disinformation campaign. This is particularly true at the moment, when even countries with well-functioning legal and regulatory systems are grappling with the question of what restrictions on social media are appropriate. Companies thus need to arrange for ongoing monitoring of online sentiment and have predetermined strategies for countering disinformation when it appears. Knowing the source of the story—and thus the underlying motivations of the other side—often provides useful raw material with which to develop effective counter-messaging.

While online disinformation is a global phenomenon, the regions in which an organization does business may increase its vulnerability to such attacks. For example, regions that combine a young, cyber-literate population and a mainstream media with weak editorial standards will find that it is easier for misinformation to migrate through mainstream channels once it has been established online. Absent an effective court system, parties in a dispute may feel they have little to lose by waging an aggressive battle in the court of online public

opinion. Alternatively, having a vibrant industry press covering the intersection of the internet with law, business and society helps keep the public informed of online threats and scams.



Social media can be a powerful vector for fraud as well as disinformation. In one recent case, an ultra-high-net-worth individual had one of her social media accounts hacked when her password was guessed based on the hobbies she posted about. In addition to harassing the individual by posting embarrassing material on her page, the intruders were able to access her email account and read exchanges between her and her bank. Based on this information, the intruders sent emails to her bank mimicking her writing style and directing a transfer of funds. Fortunately, the bank became suspicious and did not make the transfer. Nonetheless, this series of events demonstrates how a social media breach can have far-reaching consequences. Indeed, the ubiquity of digital communication, combined with an always-on work culture, means that access to personal accounts can easily expose sensitive business information. Because of this, companies should ensure that employees are taking appropriate social media precautions, including the following:



1 Establish separate business-facing and personal social media accounts—and consider using only a first name in the latter. Don't post anything in one that can be linked to the other.



2 Use randomly generated passwords at least ten characters in length.



3 Disable GPS metadata for social media posts.



4 Educate family members regarding defensive social media behavior.



5 Periodically review social media posts and delete anything that could be used in damaging ways. If the post has not been commented on or saved by others, deletion is likely to keep it from view.

Social media's value as a communications channel will only continue to grow. Both individuals and companies expend considerable effort in leveraging that channel, but they must also take defensive measures to ensure that the channel does not become a weapon turned against them.



The Case of the Telltale Tree: Digital Sleuthing for Asset Recovery

A new generation of investigation methods combines social media savvy with old-fashioned detective work.

Social media is now an integral part of personal life. For vast numbers of people—and particularly for those with little or no memory of the world before the internet—an experience isn't complete until it has been posted online. As it turns out, this impulse extends even to people who attempt to misappropriate assets. As a result, social media analysis, combined with enhanced image analysis and old-fashioned sleuthing, has become an important component of asset recovery work, used for everything from helping governments locate funds embezzled by unscrupulous officials to helping banks identify holdings of customers who have defaulted on loans.

Recently, Kroll was tracing assets on behalf of a client during a high-profile business dispute. In its social media analysis, the Kroll team discovered that a relative of a counterparty in the dispute had been tagged numerous times in photos of a villa in a golf resort in the United States. Luxury real estate, of course, is a common asset in which to hide missing funds.

Although this was a promising lead—particularly since the counterparty was known to be an avid golfer—there were thousands of such properties in that particular resort town. The social media photo album, however, offered two more clues: a picture that included the name of a bar, and a picture of the relative at a restaurant. From those two data points, the team narrowed down the area of the villa's possible location.

The Kroll team then scrutinized the photos of the villa more closely and noted a number of attributes, including the shape of the villa's pool, the patio and nearby sand bunkers. The team then attempted to use satellite imagery to identify a property with these features. While a number of properties on several golf courses emerged as possibilities, there was no clear match between the villa in the social media photo album and any of the satellite images.

At this point, modern digital analysis was augmented with old-fashioned sleuthing. A Kroll analyst travelled to the resort, conversed with locals and walked the perimeter of each of the area's golf courses to try to identify the property in question. However, when viewed up close, none of the properties matched the social media photos.



JONATHAN HARMAN

Associate Manager

Business Intelligence and
Investigations

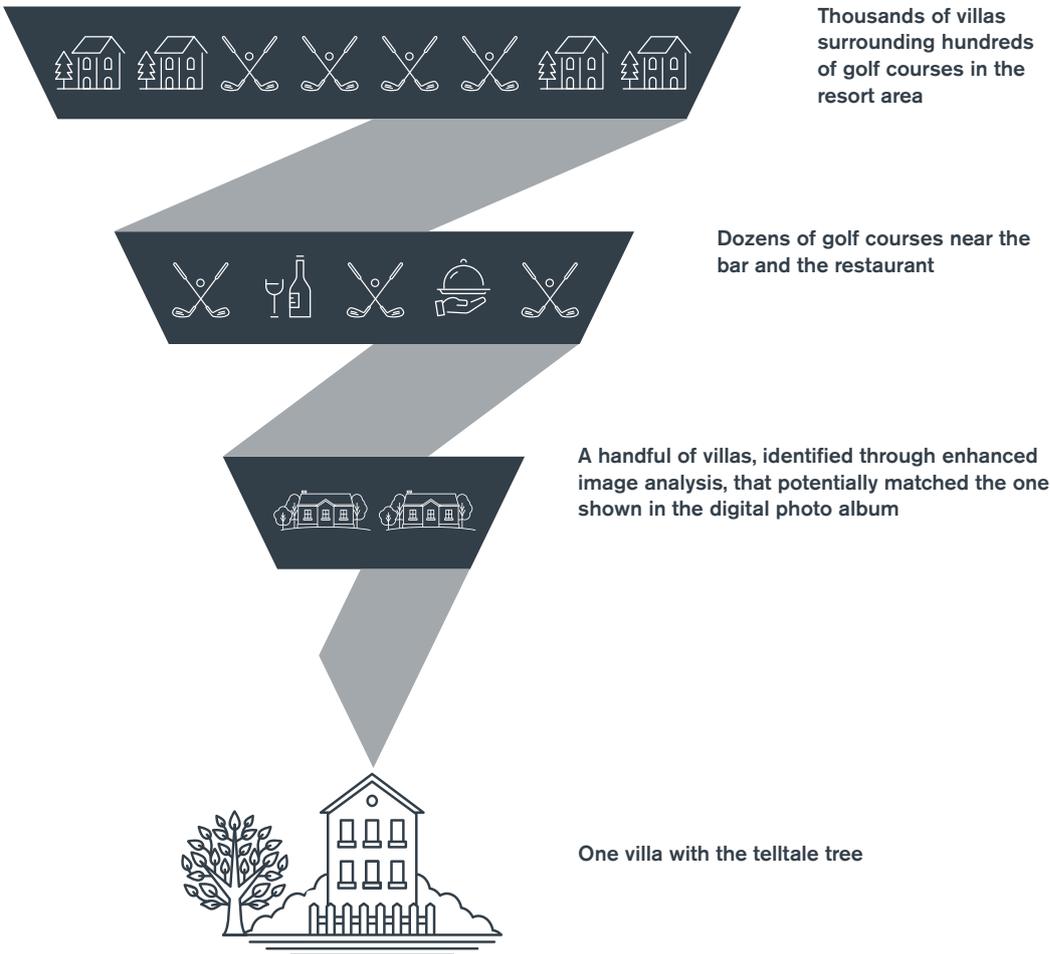
London, UK

jonathan.harman@kroll.com

The analyst began to suspect that sometime after the pictures in the social media album were taken, the villa underwent renovation, changing its appearance. The analyst then returned to the social media photographs, hoping to identify other clues that might have survived a renovation. As it so happened, one of the photographs of the villa included in the background a tree with a distinctive branch structure. The analyst then began looking for the tree rather than the villa. This time, a match was made—a tree with the distinctive branching was found, next to a villa that looked nothing like the one depicted in the social media album.

A subsequent in-person search of local property records confirmed what the analyst had suspected: The subject had purchased the villa—for several million dollars—and then, not long after the photos were taken and uploaded to the relative's social media account, the property was knocked down and completely rebuilt. The analyst was then able to obtain publicly available architectural plans, submitted during the renovation application process, that revealed precise details of the elaborate changes. While the entire villa had been thoroughly modernized, the telltale tree in the background remained as a silent piece of evidence.

FIGURE 13
FINDING THE HIDDEN ASSET AMONG THOUSANDS OF POSSIBILITIES



Reputation on the (Goal) Line: Shielding the Club Brand in the Sponsorship Arena

Football's rapid commercialization and reach into new regions calls for a new kind of defense.

In today's interconnected environment, the necessity of thorough due diligence in managing reputational risk extends to all businesses. Even a behind-the-scenes distributor of industrial supplies would suffer reputational damage if its goods ended up being used, for example, in chemical warfare. But reputational due diligence is particularly critical when brand equity is central to the value of the business. And there is probably no sector in which that is truer than professional sports. In sports, the brand is the business.

Football (soccer) provides a vibrant illustration of the importance of taking measures to protect a club's image. This is not only because of football's popularity but also because the sport is undergoing a rapid commercialization. In some cases, such as England's Premier League, clubs have been signing a series of lucrative sponsorship deals. Elsewhere, in markets such as Brazil, rising operational costs, combined with challenges stemming from a tradition of non-professional management, have led to a hunt for new sources of revenue.



IAN COOK

Associate Managing Director
Business Intelligence and
Investigations
São Paulo, Brazil
ian.cook@kroll.com



ANDREW WHELAN

Senior Manager
Business Intelligence and
Investigations
London, UK
andrew.whelan@kroll.com

Kroll's investigations on behalf of sports clubs have uncovered potential sponsors whose senior principals have been accused of money laundering, fraud and other criminal activity.



A RECIPE FOR REPUTATIONAL RISK

All sponsorship arrangements, like any third-party relationships, carry relationship risk. However, the current commercialization of football magnifies that risk for a number of reasons. The first is the nature of the football sponsorship market. While there are some global, well-established companies that seek agreements with football clubs, top-tier brands have many other advertising opportunities available to them. This means that the pool of potential football sponsors also includes organizations that aspire to a global audience but vary in their ability to reach that level of exposure. Indeed, many of those enterprises want to associate themselves with a football club precisely to gain greater prestige. Some may even be exploring club sponsorships for the first time.

This isn't to say that many of these companies aren't legitimate or wouldn't make good corporate partners. But that can only be determined by conducting thorough due diligence, and there is more than reputation at risk. For club sponsorship to be meaningful, it must be long term. Clubs need independent verification that a potential sponsor is in no danger of going under, that it has the financial resources that it claims to have and that those funds are from reputable sources—none of which can be taken for granted.

THE FACTORY THAT WASN'T THERE

Due diligence can result in eye-opening revelations. Kroll's investigations on behalf of sports clubs have uncovered potential sponsors whose senior principals have been accused of money laundering, fraud, and other criminal activity. In one case, a major British football club asked Kroll to conduct due diligence on a manufacturing company in the Far East that was hoping to become a sponsor. In addition to examining corporate filings, media references and court records, the Kroll team spoke with local sources familiar with the company and made discreet visits to the factory to observe how the business was actually run. Far from being the stable enterprise the company claimed to be, the business was on the brink of insolvency; the manufacturing plant had closed and the owner was at the center of multiple Ponzi scheme allegations.

HAVING THE RIGHT BACKFIELD SUPPORT

Many clubs are pursuing sponsorships more aggressively and farther afield than ever before, making thorough due diligence all the more necessary. Clubs without experience in conducting extensive on-the-ground research and reputational inquiries are at risk of becoming ensnared in undesirable or unstable commercial relationships.

The disadvantages of inexperience are often multiplied by a sense of urgency. Just as little-known companies have strong motivations to land high-profile sponsorships, football clubs are eager to establish a presence in untapped markets such as Africa and the Middle East. But while these regions present great potential for expanding a club's fan base, clubs often lack an understanding of local nuances, including which companies and individuals they should avoid. The combination of a finite number of clubs and a finite number of desirable, viable sponsors all pursuing deals can result in clubs taking action before they have gathered all the details they need to make a fully informed decision.

The commercialization of football has the potential to broaden the reach of what is already the world's most popular spectator sport, provide companies with an invaluable platform for reaching new audiences and give clubs an important channel for monetizing their brand. As this process unfolds, it is critical that clubs protect their most valuable asset—their reputation. Due diligence that looks beneath the surface to generate real insight into potential partners can help clubs avoid damaging missteps while providing them with the confidence to enter into relationships that provide substantial long-term benefits.





02

**RISK
MANAGEMENT
IN PRACTICE**



RESHMI KHURANA

Managing Director,
Southeast Asia Head
Business Intelligence and
Investigations
Singapore
rkhurana@kroll.com



LOUIS-DAVID MAGNIEN

Managing Director
Business Intelligence and
Investigations
Paris, France
louis-david.magnien@kroll.com



ALESSANDRO VOLCIC

Managing Director, Russia
and CIS Head
Business Intelligence and
Investigations
Moscow, Russia
avolcic@kroll.com

Thinking Like a Creditor

Investing or lending in new markets has the potential for high returns. But if the deal goes bad, asset recovery on the counterparty's home turf can be challenging.

The current combination of economic turbulence and long-term growth potential in regions throughout the world is driving corporations, private equity firms and lenders to expand their geographic reach and to invest in or lend to entities in new markets. While expanding into new markets brings opportunities, it also begets considerable additional risks. The new market's legal and commercial systems may be confusing to outsiders. Because those entering the market often lack an extensive network of local relationships, it is easy for third parties to misrepresent themselves. And if a deal goes bad and assets need to be recovered, those assets are likely to be on the counterparty's home turf, governed by rules and timetables that the party knows how to manipulate. That advantage can be magnified if the dispute is being adjudicated in the counterparty's jurisdiction.

FIGHTING AN ASYMMETRICAL WAR

If a conflict does arise, even sophisticated organizations can find that they are unprepared for the asymmetrical warfare that ensues. In asset recovery, the legal issues may only be the tip of the iceberg—a comprehensive strategy across multiple fronts, from business intelligence to forensic accounting to physical security, is often required.

Of course, the optimal strategy is to avoid bad deals in the first place. To do so, it is essential to conduct enhanced due diligence that goes beyond the typical legal and financial checks. A financial statement, for example, will not disclose if a business owner is litigious, has a history of bankruptcies or has a reputation for poor business management. This level of information must be gleaned from on-the-ground intelligence. And because a counterparty's situation can change over time, that initial intelligence gathering should be complemented with ongoing, periodic monitoring.

The business and assets in question need to undergo the same holistic scrutiny given to the owners and management. For example, if a company applying for a loan is part of a portfolio of companies, it is critical to know the financial stability of each element of the portfolio. A lender may provide capital to a healthy company, only to see those funds siphoned off to floundering enterprises elsewhere in the portfolio. The mapping of corporate structure is particularly critical in jurisdictions where it can be difficult to trace ultimate beneficial ownership through layers of corporate entities. The key in these environments is to think like a creditor: Does the collateral on paper really exist? Can the collateral be seized in a worst-case scenario? When a company is backed by the personal assets of a founder, it is important to scrutinize those assets in a similar way.

THE CASE OF THE PURLOINED OFFICE BUILDING

When a transaction does move forward, it is necessary to be prepared in case a dispute arises. Consider the case of a Western company seeking to expand its presence in Eastern Europe. Following a crash in the local commercial real estate market, the company sought to lease an office building in a country's capital city. A suitable building was found, terms were negotiated that reflected the depressed market and a binding lease agreement was signed. The company moved into its new headquarters.

When the local real estate market rebounded, however, the landlord sought to get out of the deal, either to rent the building at a higher price or to sell it. The landlord had the copy of the lease that was on file with municipal authorities surreptitiously altered to allow for unilateral termination, and then stole the tenant's copy of the contract from the tenant's office. Next, the landlord hired a team of armed enforcers who overwhelmed the tenant's minimal security staff and prohibited the tenant's employees from entering the building. The tenant turned to the local police for help in recovering access to the building and filed an injunction with the local court to restore the contract. However, the police refused to intervene in what

they saw as a commercial dispute, and the tenant lost its case in court.

In desperation, the tenant turned to Kroll. We designed a multifaceted solution, connected the tenant with appropriate local counsel and provided research that convinced local authorities to investigate the forgery of the contract. Kroll then coordinated expert testimony and helped shepherd the case through both the local legal system and the London Court of

The local police refused to intervene after the tenant's minimal security staff was overwhelmed and employees could not enter the building.

International Arbitration. Although the company prevailed in both legal venues, this experience led it to base its regional operations elsewhere.

FINDING THE LEVERAGE POINTS

In another case, a specialty lender was approached for a loan by a business in a region where the lender had little direct experience and no physical presence. On the surface, the borrower's financial history seemed to be in order. After the loan was made, however, the borrower quickly fell into arrears. Kroll was able to determine that the borrower had used the funds to hide losses incurred by sister portfolio companies that had not undergone due diligence when the loan was applied for. More importantly, Kroll also discovered that the borrower had applied to the government for a new business license. The bank leveraged this intelligence by issuing an ultimatum: Work with us on a schedule to repay the loan, or we will inform the government of the arrears—potentially putting the

license application in jeopardy. This proved to be a much more effective, and less expensive, strategy than litigation would have been.

Companies moving into new markets need to protect themselves with comprehensive due diligence and by being prepared to act decisively and strategically if a dispute arises. Advance planning is crucial. A party conducting a transaction in a new market needs to have a crisis plan to respond promptly to adverse events. After all, in an asset recovery situation, time is of the essence. Given that there are likely to be many parties trying to recoup losses, it's essential to move faster than everyone else.



SIMON ASHENDEN

Associate Managing Director,
Asia Pacific Head
Security Risk Management
Singapore
simon.ashenden@kroll.com



NICK DOYLE

Managing Director, EMEA Head
Security Risk Management
London, UK
ndoyle@kroll.com



TIMOTHY V. HORNER

Managing Director, Global Head
Security Risk Management
New York, NY, US
thorner@kroll.com



RAFAEL LOPEZ

Associate Managing Director
Security Risk Management
Mexico City, Mexico
rafael.lopez@kroll.com

Avoiding a False Sense of Security

An organization's physical security program may not be commensurate with the actual risks and threats the enterprise faces. Development of a master security plan can lead to rightsized solutions.

This year's *Global Fraud and Risk Report* highlights how the risk landscape has broadened to include social media, geopolitics and other threat vectors. Even with the addition of these concerns, however, physical security—controlling access to facilities and assets and protecting personnel—remains a central component of risk management. Evidence of this can be seen in two results of our survey. Two of the three most frequent types of incidents—leaks of internal information and data theft—often involve unauthorized access to, or use of, company assets. Second, employees are the most common perpetrators of both incident categories. In combination, these two findings underscore the importance of access control in mitigating theft and misappropriation. Many organizations that experience these and other types of intrusions have installed physical security systems such as access control card readers, video surveillance cameras, security guards and vehicle bollards. Yet there is often no underlying strategy for which systems are implemented or how they are to be employed. The result is a hodgepodge of frequently misused tactics that fails to provide the basis for comprehensive protection, detection and response.



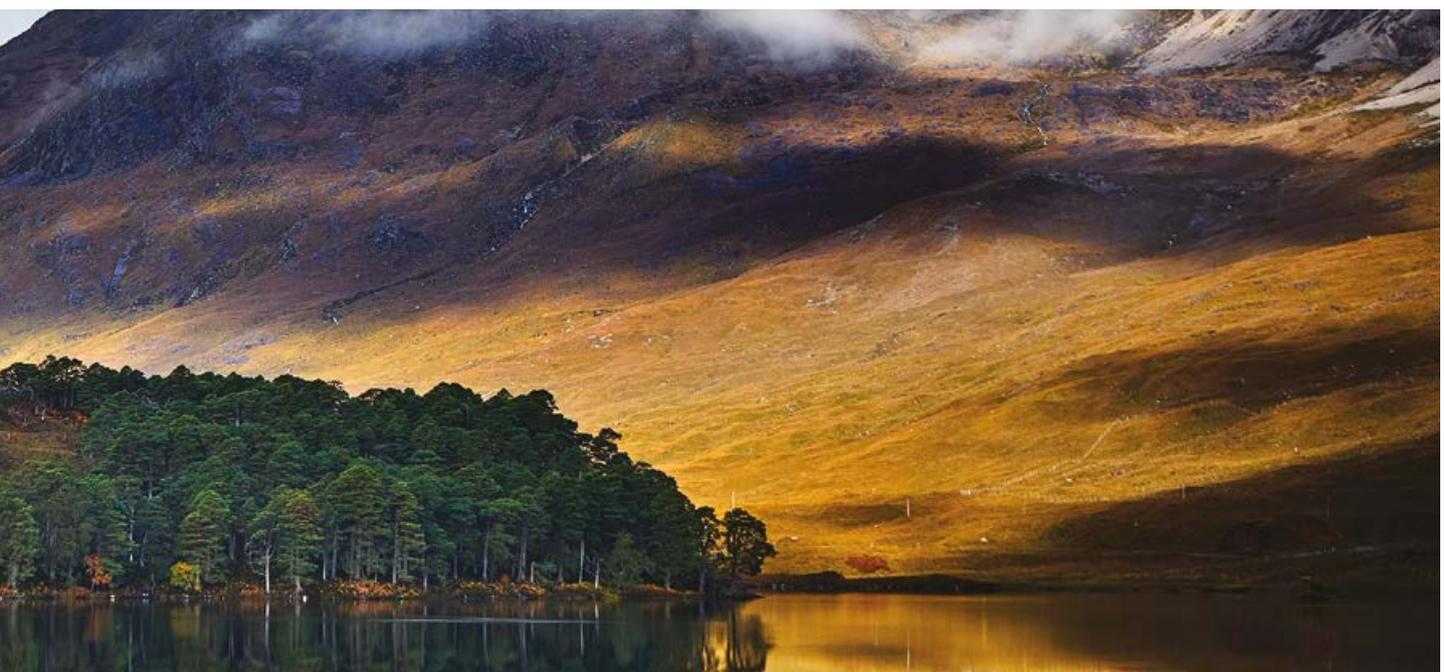
HOW PHYSICAL SECURITY FAILS

Consider video surveillance cameras, for example. Used properly, these systems can be highly effective in helping organizations detect and respond to unauthorized access incidents. But effective use requires cameras that are appropriately positioned and fully operational, as well as active monitoring of the video feeds by a sufficient number of personnel trained in threat response. However, this scenario rarely occurs. Instead, cameras are often placed in low-risk locations, camera functionality goes untested, monitoring stations are understaffed and workers are poorly trained. A video surveillance system, like any technology, isn't self-sustaining. To be effective, it must be supported by the right procedures, policies and personnel.

Necessary risk-management initiatives can sometimes be sidelined because security measures are viewed by company leaders as undermining the organization's culture. This perspective has become increasingly common as more enterprises adopt informal, egalitarian workplaces. For instance, a company may balk at the recommendation that access to the offices of its C-suite leaders be restricted with keypads or card readers, believing this barrier would hinder

a spirit of open collaboration. The reality, however, is that a chief executive officer or chief financial officer is more likely to have sensitive material in his or her office and to be the target of disgruntled employees. Companies with egalitarian cultures should understand that equality among people doesn't necessarily mean equality in their threat profiles.

Unfortunately, the weaknesses caused by an ineffective risk management program are usually not immediately apparent. The enterprise may appear to be well secured until an incident occurs, an antagonist strikes or a threat is imminent. Kroll's Security Risk Management team is frequently contacted by companies that have received threats from a recently fired employee or that realize a former employee may still be in possession of trade secrets or other sensitive information. In such cases, the first step is to review the security procedures currently in place. This often uncovers shortcomings that require immediate action, such as significantly increasing on-site security staff or locking down portions of the premises—remediations that can be far more costly, disruptive and unnerving to employees than building in adequate physical security procedures from the beginning.



MOVING FROM GUESSWORK TO CLARITY

Organizations can avoid these problems by conducting a thorough threat and risk assessment. This assessment incorporates multiple factors, including how facilities are laid out, which employees need access to which assets and how valuable the relevant assets are. The assessment also includes gathering intelligence to determine whether the firm or its principals could be targets of malicious actions and evaluating collateral risks arising from facility locations and nearby enterprises. For example, are the parking lots in the area susceptible to automobile break-ins? Is the facility located next to an enterprise involved in high-risk or controversial activity that could invite protests or violence? In addition, the assessment systematically analyzes the history of incidents experienced by the company to uncover patterns of vulnerability that might otherwise go unnoticed.

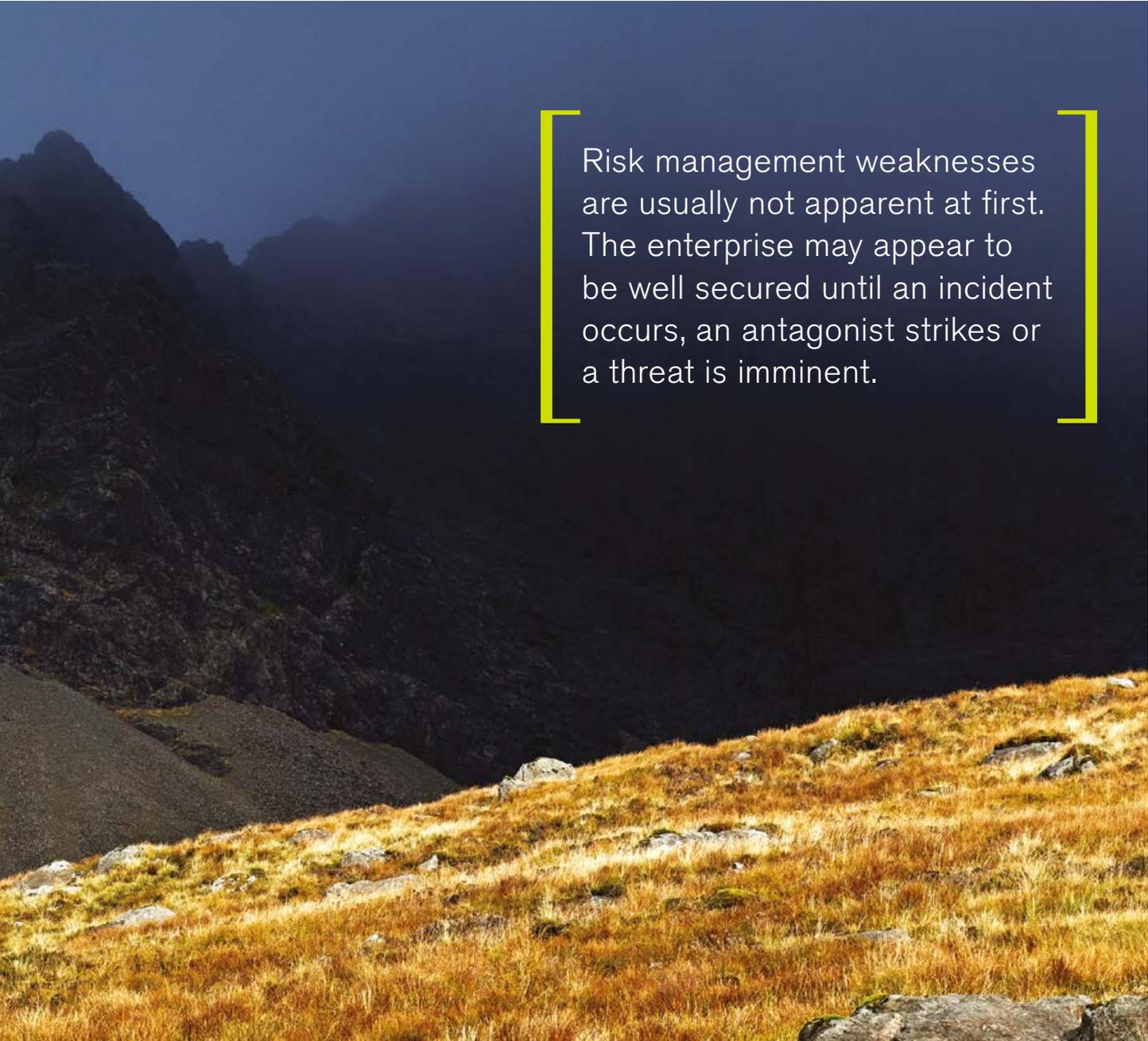
Following a threat and risk assessment, an organization can develop a master security plan that includes the following components:

- The types of electronic security measures needed (such as access-control card readers and intrusion detection systems) and their minimum specifications and implementation requirements
- The types of architectural security measures needed (such as vehicle bollards and window blast protection) and their minimum specifications and implementation requirements
- The policies and procedures necessary to support those measures
- Training for security staff as well as the larger workforce
- A plan for integrating security measures with one another and into operations
- A system for regularly auditing, testing and maintaining security system performance
- Contingency plans for scaling, if needed



The security master plan would also specify access-control measures, including where card readers need to be placed, the types of credentials to be used, methods for determining access privileges, who will grant and update access privileges and how anomalies or exception events are monitored and investigated. It would outline the coordination of access permission with human resources procedures for hiring and termination. The plan would also discuss ways of integrating card readers with the video surveillance system to capture attempts at forced or unauthorized entry. Repeating this level of analysis for all systems results in a comprehensive framework for effective physical security.

No matter how digital the economy becomes, the physical protection of facilities and people will always present a fundamental security challenge. Basing physical security on a detailed threat and risk analysis can help ensure that such measures provide real protection when threats materialize.



Risk management weaknesses are usually not apparent at first. The enterprise may appear to be well secured until an incident occurs, an antagonist strikes or a threat is imminent.

**CHRIS BAKEWELL**

Managing Director
Disputes
Houston, TX, US

chris.bakewell@duffandphelps.com

**PAUL BENSON**

Director
Disputes
Minneapolis, MN, US

paul.benson@duffandphelps.com

**TAD KAGEYAMA**

Regional Managing Director, Asia
Pacific
Business Intelligence and
Investigations
Singapore
tkageyama@kroll.com

IP Protection in a Borderless World

Today's dynamic international trade environment and mosaic of national regulations make intellectual property protection as complex as it is important.

Guarding against IP theft is a priority of 72 percent of the respondents to this year's *Global Fraud and Risk Report* survey. Furthermore, 43 percent name it a *high* priority, which means that, overall, respondents assign IP theft an urgency second only to that of data theft. Our survey shows that this concern is warranted: 24 percent of respondents said their organizations experienced a significant incident of IP theft within the last year, up from the 20 percent reported in the 2017–2018 survey.

THE ARRAY OF THREATS

Survey respondents identify a range of perpetrators of IP theft or misappropriation. Competitors, contractors, employees and third parties (such as joint venture partners, vendors and suppliers) are each responsible for approximately one-fifth of the reported incidents. The wide variety of perpetrators underscores the many ways in which IP theft or misappropriation occurs.

Contractors and employees, for example, respectively account for 19 percent and 18 percent of IP theft. Perpetrators from these groups often commit IP theft by taking confidential information with them when hired away by a competitor, or by engaging in espionage, selling the company's secrets to its rivals. Motives abound: The employee or contractor could have been disgruntled, bribed or even secretly employed by a competitor all along.

Seventeen percent of IP incidents arise from **third parties**, such as joint venture partners, suppliers and vendors. Without proper safeguards, business partnerships and supply chain relationships can bring IP risk because they are generally predicated on sharing sensitive information. This risk warrants particular focus when these relationships cross borders, as is increasingly the case in today's globalized economy. Enforcement in response to IP theft can be challenging and should be given ample attention when developing the partnership terms. Patents and trademarks offer protection only in the jurisdiction where they are issued, and trade secrets and proprietary know-how don't have the same legal protection across jurisdictions from competitors, foreign governments, employees and other bad actors. The effectiveness of enforcement varies among countries as well. The resulting patchwork of protection makes any IP holder particularly vulnerable to theft or infringement when its supply chain, operations or distribution networks extend to foreign countries.

This vulnerability may be increased further by a country's policies on foreign investment. One area of tension between the United States and China, for example,

has been “forced” technology transfer arising from Chinese regulations that make it very difficult for a foreign company to operate in China without partnering—and thus sharing its IP with—a Chinese company. China recently introduced legislation that would ease foreign investment rules, but only time will tell if this change will have a meaningful impact on this deep-rooted conflict. Intellectual property is a key issue in U.S.–China bilateral trade negotiations, and it will be important to see what, if any, terms are agreed to.

Competitors account for 21 percent of reported IP theft incidents. While such incidents can arise from deliberate actions such as direct infringement, espionage or reverse engineering, indirect infringement also can be a common problem, especially because it can occur inadvertently. Consider a scenario in which a German company contracts with a Taiwanese firm to manufacture a medical imaging device according to a particular design and set of specifications. In manufacturing the device, the Taiwanese firm uses a technology for which a rival medical imaging company holds the German patent, and for which the German company does not have a license. The German company might risk infringing on the rights of the patent-holding competitor as soon as it distributes the device in Germany—and without proper planning, may not even know that it is doing so. Investigating, managing and measuring the impact of these issues can be challenging, and organizations may find it beneficial to have their plans reviewed by third-party specialists.

MITIGATING RISK

To mitigate against IP-related risks, companies can take several steps. A company’s first step is to make sure it is taking adequate precautions to **protect its IP within its own facilities**. After all, employees and contractors together were responsible for 37 percent of the IP theft incidents reported in our survey. Access to intellectual property should be restricted and monitored, and then promptly revoked upon an employee’s termination or resignation. Management should develop policies to address which personnel have rights to access IP and then monitor access to ensure compliance. Such policies should also address and limit any potential to copy or distribute the company’s confidential information.

Secondly, organizations that establish IP sharing agreements with business partners, suppliers and manufacturers should **consider a defensive mindset** when drafting the appropriate contractual safeguards. For example, contracts need contingencies to address a counterparty’s potential acquisition, whether a license granted to the counterparty extends to the counterparty’s subsidiaries, and the counterparty’s right to sub-license the IP; the terms of such an arrangement should be crafted so as to consider, and possibly prevent, the counterparty licensing the IP to competitors. Companies sharing IP with third parties need to specify the physical and cybersecurity measures under which the counterparty must hold the intellectual assets, such as access-restriction policies and the encryption of sensitive information.

FIGURE 14
WHO ARE THE PERPETRATORS OF IP INCIDENTS?



Thorough due diligence is also crucial. Examining a company's financials and performance track record is not sufficient; proper due diligence will include business conflicts and litigation involvements of the entity, its management and its board members. The process should also involve investigating the counterparty's ability to execute and maintain the specified security procedures.

When third-party relationships cross borders, organizations should step back and **map the local IP landscape**.

This means understanding not only the IP regulations and protections in each country, but also each country's effectiveness in enforcing its protections, and the capacity, disposition and transparency of its courts in handling IP matters. All of these factors determine, in practical terms, the company's level of recourse should infringement occur. To the extent possible, appropriate clauses addressing these factors should be incorporated into any license agreement or business partnership. A holistic view of the entire IP strategy—including enforcement, licensing and monetization scenarios—is essential to informed decision making and preparation. The counsel of an experienced local law firm is also essential to incorporating this strategy into agreements.

A country's IP landscape includes the places where IP protection intersects with the government's **foreign and domestic policy**. This includes such issues as the restrictions on foreign investment discussed above, as well as any history of compulsory licensing, including situations in which the government essentially allows local companies to selectively infringe on foreign patents. These infringements may be permitted by the government under the cover of advancing a public good, such as improving access to healthcare. Take special care when entering into IP-sharing agreements with state-owned enterprises, which may have a local advantage in the adjudication of any conflict that may arise.

Finally, if there is **the potential for theft or infringement**, that risk needs to be thoroughly assessed and incorporated into the relevant business decision making.

WHEN INFRINGEMENT OCCURS

Regardless of how carefully a company might work to mitigate its exposure to IP risk, unfortunately, infringement and theft do occur. When that happens and legal action ensues, the strength of the case will rest on how compellingly the company can demonstrate actual harm. The complexity and global nature of the typical company's operations and supply chain often make this a challenge. The effort is usually shepherded by the in-house legal department, working with outside counsel to provide expertise on the type of IP theft or misappropriation and on the jurisdiction in which the company is pursuing legal action. Other professionals can provide important input as well. Economic experts, working with technical and marketing experts, combine industry expertise with qualitative and quantitative intelligence to assess and quantify the damages inflicted by the infringement or theft. Doing so may require, for example, isolating the incremental value of the intellectual property in question, and then quantifying the economic harm resulting from the wrongdoing. Constructing these economic arguments calls for a team with deep understanding of IP disputes, acute analytical skills, and experience in addressing the full range of relevant issues and potential IP damages.

LOOKING AHEAD

The impediments that arise from the wide range of national approaches to IP protection and enforcement have motivated many companies to attempt to establish a global approach to intellectual property. However, regulatory differences among jurisdictions make doing so difficult. Understanding the impact of reform efforts in individual countries—China, Brazil, and India among them—will form a basis for a global framework. There is now broad awareness among countries that sufficient and reliable IP protection is a powerful differentiator in the competition for foreign investment. The increased attention paid to IP issues in bilateral trade agreements is another factor to monitor and assess. Regardless of whatever advances may be made, companies must continue to be alert to the range of IP risks and be prepared to integrate the appropriate mitigations into both their IP monetization strategies and their operations.

Any potential for IP theft or infringement needs to be thoroughly assessed and incorporated into business decision making.



MARCELO CORREIA

Associate Managing Director,
Iberia Head
Business Intelligence and
Investigations
Madrid, Spain
marcelo.correia@kroll.com



BILL NUGENT

Managing Director
Business Intelligence and
Investigations
Philadelphia, PA, US
bnugent@kroll.com



RICH PLANSKY

Regional Managing Director,
North America
Business Intelligence and
Investigations
New York, NY, US
richard.plansky@kroll.com

The Seven Elements of Successful Investigations

Knowing what a complex investigation involves can help a company choose the right partner—and minimize risks that can arise from the investigation itself.

Organizations seeking an outside resource for strategic business intelligence and investigations have more possibilities to choose from than ever before, from large accounting firms to small detective agencies. Knowing the elements of a successful engagement enables an organization to evaluate the range of options and be an informed partner of the firm that is ultimately chosen. Such engagements, whether for corporate or government clients, require global data collection and research capabilities, in-depth knowledge of the client's business, and a seasoned understanding of human behavior. Each of these capabilities enhances the others in a holistic approach, enabling a clear, comprehensive picture of the situation under investigation to emerge.

A multifaceted approach to investigation is particularly important given how threats can morph and combine. A contractor's insufficient cybersecurity measures can lead to a leak of internal information, which could then feed social media attacks on the company. A counterfeiting scheme may be part of a larger money laundering operation, with funds invested in foreign real estate owned by shell companies. Because it is rarely known at the outset where an investigation will lead, a successful engagement requires investigators to extract insights using a range of capabilities, which can be grouped into five categories:



Open source/public records research. Bad actors often know exactly where the blind spots in control processes are and how to exploit them to obscure illicit activities. Sophisticated research using the growing trove of publicly available data can combine information from disparate areas—from real estate records to offshore corporate registries—to construct chains of events and generate detailed profiles of people and institutions.

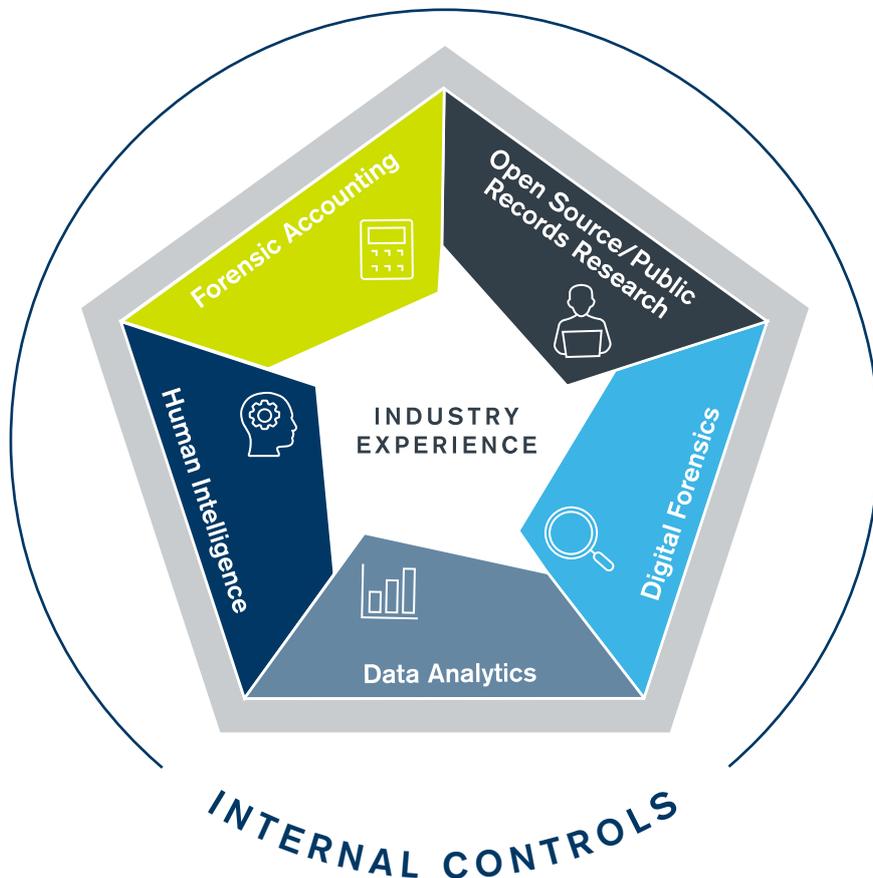


Digital forensics. A great deal of workplace behavior takes place on computer systems, smartphones, trading platforms and other devices that store information in digital form. Digital forensics leverages sophisticated tools to identify, secure and extract meaning from this ocean of digital data, often dramatically affecting the outcome of an investigation.



Data analytics. Large-scale investigations increasingly require powerful artificial intelligence platforms that can discern patterns in massive data sets, such as millions of emails or transaction records. Effective use of these tools, however, requires ongoing investment in technology as well as specialized expertise.

FIGURE 15
A MULTIFACETED APPROACH TO INVESTIGATIONS



Human intelligence. Oftentimes, the best intelligence comes from other people, whether in the form of investigative interviews, field observations, or tactical methods like surveillance or undercover approaches, all of which require experience and ingenuity. In one case, Kroll was asked by a beverage manufacturer to determine if one of its distributors was surreptitiously distributing the product outside of its contractually determined sales area and thus infringing on the territory of other distributors. To solve the case, investigators purchased the product in 80 different locations throughout the country and traced the origin of the products through information on the labels.



Forensic accounting. Accounting records play a key role in detecting or confirming fraud and theft, provided one knows where to look. Bad actors can hide illicit activity behind a facade of accepted accounting practices. An investigations firm should include a dedicated, experienced accounting team that can pierce that facade to reconstruct fund flows, transactions and timelines.

Because it is rarely known at the outset where an investigation will lead, a successful engagement requires investigators to extract insights using a range of capabilities.

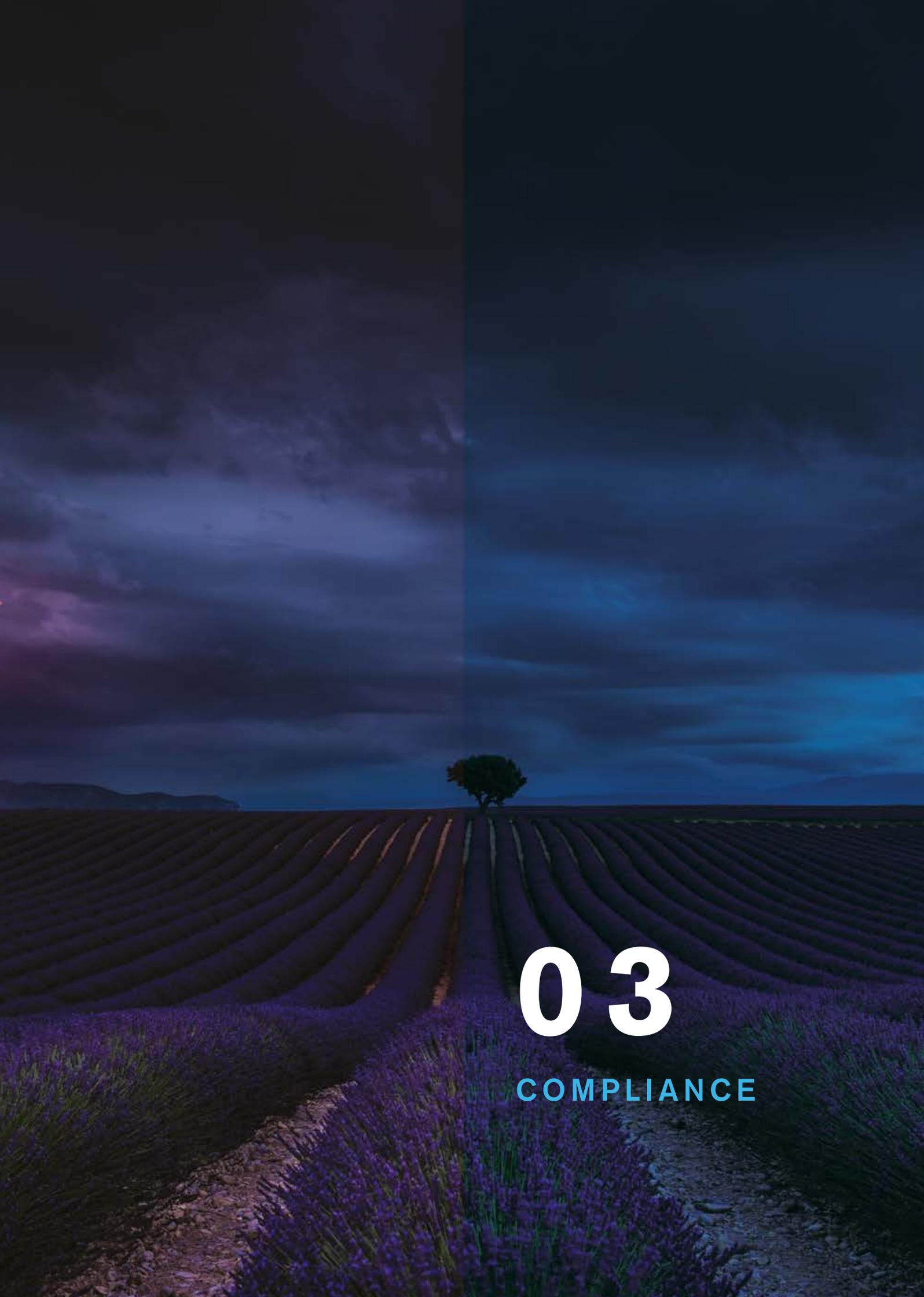
While organizations engage business intelligence and investigations firms in response to an existing or potential incident, an investigation itself can also pose a threat. Investigations firms that lack global experience can inadvertently expose an organization to additional risk by making errors in judgment, failing to scrupulously follow local laws and regulations or misreading the larger context. For example, improperly gathered evidence may be inadmissible, taint the entire case, lead to a failed prosecution and thus leave the client without redress in court.

An investigations firm therefore needs to have safeguards in place to mitigate those risks. In addition to the five skills discussed above, intelligence and investigations firms need two additional, overarching capabilities:

- **Industry experience.** The incidents that prompt a business intelligence and investigation assignment take place within the context of the business itself and its particular threat vectors, risk assessments and mitigation strategies. Money laundering, for example, is different for import/export businesses than for financial services firms. Further, addressing today's threats should be done with an eye toward improving processes and controls to reduce future risks. An investigations firm must be able to work as professional peers with C-suite leaders and help the organization identify necessary remediations.
- **Internal controls.** Business intelligence and investigations assignments usually involve highly sensitive situations. The investigations firm must have the internal culture and controls necessary to ensure compliance with government regulations and industry best practices for issues ranging from data handling to conducting surveillance. Legal and regulatory changes must be closely monitored by the firm's counsel, who must thoroughly vet any third parties engaged for specialized assignments within the investigation.

The process of conducting an investigation or gathering intelligence on a strategically important matter often comes at an inflection point in an organization's history. Choosing the right partner for the task can help ensure that the engagement provides insight, closure and a solid foundation for averting future risks.





03

COMPLIANCE

Why Compliance Programs Fail

Too often, compliance programs seem to be working as intended—until regulators or crises prove otherwise.

In recent years, compliance programs have moved further up the agenda of corporate boards, reflecting the greater scrutiny corporate behavior is receiving from governments and regulators, investors, employees, customers and the public at large. A properly implemented compliance program provides crucial assurance to all stakeholders that the organization's personnel are abiding by all applicable regulations, internal ethical principles, codes of conduct and other guidelines governing their actions.

The unfortunate reality, however, is that many compliance programs fail to avert the transgressions they were designed to prevent. On the surface, a compliance program may appear to provide systems for identifying and mitigating risks such as money laundering, bribery and corruption, cyber breaches, safety deficiencies and numerous other concerns. In the program's implementation, however, gaps can occur that will hinder its effectiveness. Because months or even years can pass between an incident's occurrence and its detection, compliance programs often appear to be working even though they are not. An organization can have all the pieces in place to show that it is a good corporate citizen—until a regulator comes knocking on the door or a rogue employee commits fraud, whereupon the company discovers that its compliance program isn't as robust as it was thought to be.

There are a number of key reasons for the failure of compliance programs.



ASTRID LUDEMANN

Senior Manager

Business Intelligence and Investigations

London, UK

astrid.ludemann@kroll.com



JUSTINE RADNEDGE

Manager

Business Intelligence and Investigations

London, UK

justine.radnedge@kroll.com



PERMITTING A DISCONNECT BETWEEN THE COMPLIANCE DEPARTMENT AND THE REST OF THE ORGANIZATION

Organizations commonly design their compliance programs with little or no input from the people who will have to adhere to them. Compliance departments thus may impose requirements that seem reasonable in theory but in practice are onerous. Common examples include requiring excessive information before undertaking a transaction and implementing controls that do not align with normal business processes. This creates the perception among operational staff that compliance requirements are the tail wagging the dog.

This situation all but invites employees to develop workarounds, giving the impression that all necessary boxes have been checked while in reality overlooking the substance behind the compliance requirements. Such workarounds put the company at risk of non-compliance.



FAILING TO KEEP PACE WITH CHANGE

Given that regulatory regimes and organizational risk profiles are both highly dynamic, compliance programs cannot simply be a static set of rules. The leveraging of personal data for marketing purposes, for example, was a legitimate, organic response to the growth in online business until the EU's General Data Protection Regulation placed stricter constraints on what was permissible. Organizations should be mindful of changes required by their compliance programs (whether due to regulatory requirements or best practices) when moving into new markets or adopting new business models.



UNDERESTIMATING BAD ACTORS

Organizations often implement compliance regimes and controls specifically designed to satisfy regulatory requirements. This approach can fail to take into account the motives and often considerable skill and experience of those who would attempt to circumvent those controls.



FOCUSING ON MECHANICS RATHER THAN MINDSET

If an organization views its compliance function primarily as a set of obligations to fulfill, its compliance education and training is likely to be perfunctory, and compliance will be regarded by managers and employees as less important. Companies with strong compliance programs instill a culture of integrity through clear communication about the need for compliance. They provide regular training in decision-making practices with which employees can successfully navigate real-world scenarios. Fostering a compliance mindset throughout the organization also makes it more likely that legal, sales, human resources and other functions will approach compliance challenges collaboratively.



ALLOWING RELATIONSHIPS TO OVERRIDE POLICY

Much of the conflict between the compliance department and day-to-day business operations derives from the fact that so much of commerce—within the organization as well as between the organization and the world at large—is based on personal relationships. Personal relationships are built on trust, and trust exempts people from the dispassionate questioning that is central to a compliance mindset. In truth, robust compliance arrangements can strengthen relationships by sending a clear and consistent message to external stakeholders. The reality that a rigorous compliance program can coexist with strong professional relationships should be constantly reinforced.

Most organizations rely on internal audit or similar functions to periodically assess the performance of their compliance programs. Generally, these efforts involve verifying that the necessary compliance procedures are in place. This is a good first step, but just as financial audits are not designed to identify fraud, corruption or money laundering, a standard compliance audit—even when conducted by independent outside parties—can sometimes fail to uncover problems. For deeper insight into whether and how their compliance procedures are being circumvented, organizations must move beyond compliance auditing to *compliance stress testing*. Compliance stress testing applies an investigative mindset to the compliance program itself, identifying and probing weak points to test the company's ability to detect and mitigate risk. Beyond merely confirming adherence to procedures, stress testing goes further to determine if risks are actually being addressed. Are assets that have been posted for collateral valued accurately, and can they be recovered? Have red flags in required credentials and documentation been identified and acted upon? Were transactions flagged as potentially suspicious actually reviewed and escalated? Did quality control procedures check for the weaknesses that lead to product failure?

Compliance programs are essential for ensuring adherence to regulations and avoiding proscribed practices. To work as designed, compliance programs themselves must undergo review and examination. Compliance stress testing provides a rigorous means of identifying and remediating weaknesses before regulators and crises bring them to light—which is often too late.

Keeping Growing Pains Under Control: Expanding the Business— but Not the Risk of Fraud

Companies in growth mode need to ensure that their financial and operational controls keep pace.

Reaching a strategic milestone in corporate growth—such as securing a major private equity investment, adding a business unit through acquisition or expanding operations into new regions—is cause for celebration. Too often, however, such events quietly sow the seeds of future crises by significantly increasing the company's vulnerability to fraud, theft and other types of misappropriation. High-growth companies frequently neglect to scale their financial and operational controls to keep up with their expanding complexity. In most cases, there will be no outward sign that the controls no longer align with the size of the company and the volume of its transactions. The deficiencies often become apparent only in hindsight.

Consider an enterprise that has secured a private equity investment to roll up a number of smaller competitors. Each of those competitors will have its own methods for handling financial reporting, accounting, treasury and internal audit. After the acquisitions, management may first push to standardize certain functions across the organization that are necessary for strategic planning, such as financial reporting. Other functions, such as internal audit, may end up waiting for assessment and necessary upgrades while acquirer and target focus on the long, difficult process of integrating management teams and business operations. As these inconsistencies continue, eventually the controls of each division will vary in effectiveness; this variation makes it difficult for the corporate headquarters to maintain clear financial oversight and thus increases the risk of fraud, theft or inappropriate financial reporting.

Frequently there will be no outward sign that the controls no longer align with the size of the company. The deficiencies often become apparent only in hindsight.



ANN GITTLEMAN

Managing Director

Disputes

New York, NY, US

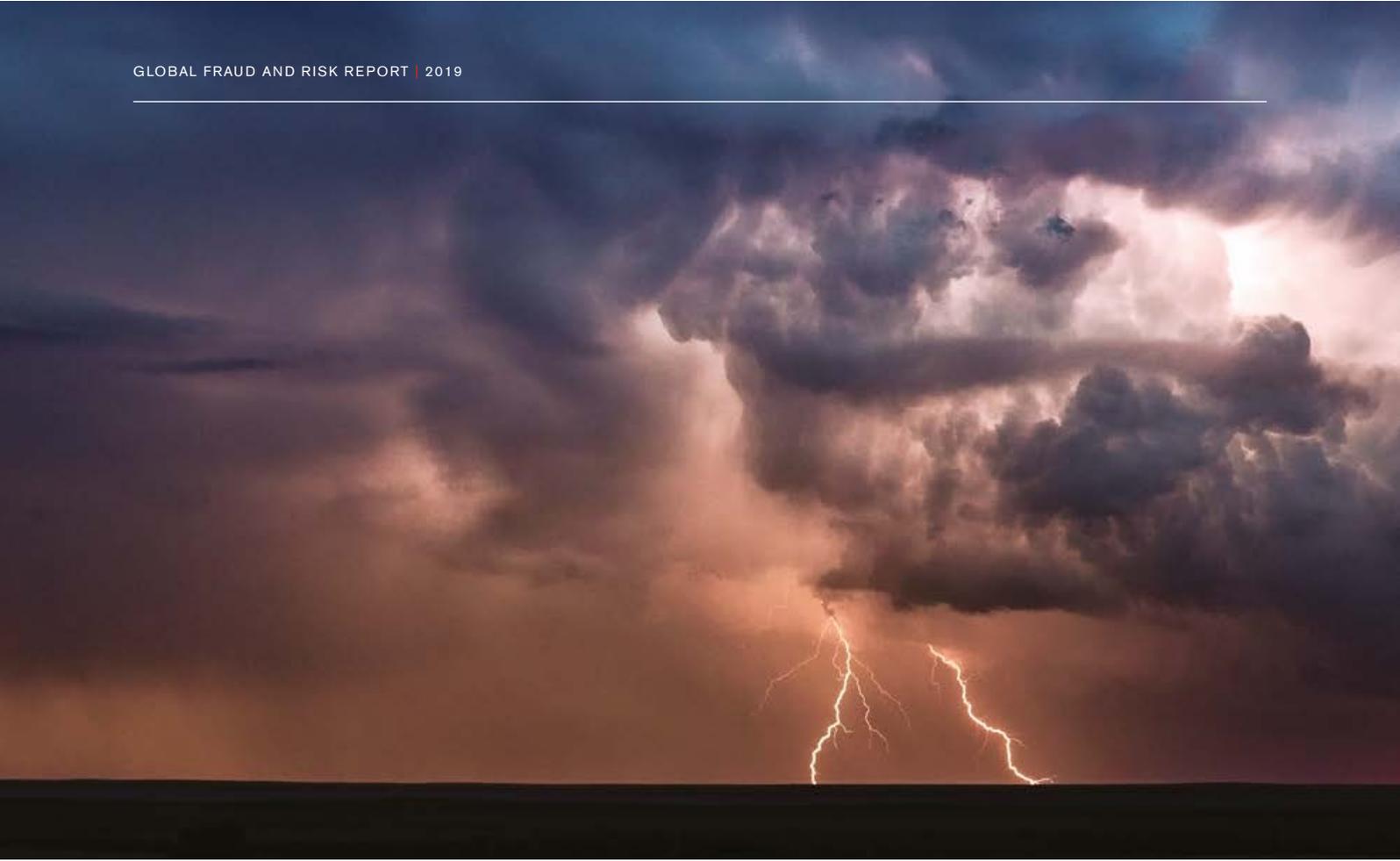
ann.gittleman@duffandphelps.com

The control weaknesses that follow acquisitions tend to multiply when those acquisitions occur in foreign jurisdictions. Because those jurisdictions will have different accounting and reporting standards and regulations, a recently acquired subsidiary could conform to local practices but fail to comply with corporate standards that have been established to protect the company's assets in jurisdictions with a higher incidence of bribery, corruption, and money laundering. Ideally, companies should adopt policies tailored to the specific risks and threats of each jurisdiction. This can be costly and challenging, however. The most practical solution is to implement a single set of financial policies and procedures throughout the entire organization.

While the problem of keeping controls in line with growth can be magnified after acquisitions, the problem can occur due to organic expansion as well. Any quickly growing company needs to be aware of this issue.

In addition to processes and controls, the capabilities of the internal finance and accounting team and external advisors must keep pace with the organization's trajectory. As the enterprise expands, the chief financial officer and other senior members of the financial function must be familiar with more sophisticated practices—such as the Committee of Sponsoring Organizations' risk-based frameworks—and have greater experience in identifying and mitigating problems in their early stages. The senior financial team must go beyond acting as accountants-in-chief, working instead to establish the desired culture of transparency and accountability, hire and develop the right people, and ensure that robust controls continue to grow with the organization.





Enterprises can take these five steps to ensure that growth does not increase the risk of fraud, theft and other forms of misappropriation:

1

Make the assessment of controls an integral part of M&A due diligence.

The state of a target's financial and operational controls should be as much a part of due diligence as its financial statements. Merely meeting accounting standards and regulatory requirements may not be sufficient. Rather, examine the target's current financial and operational controls against the target's risks and threats as well as the acquiring company's existing practices, and develop a plan and budget for making the necessary changes.

2

Incorporate control quality into performance benchmarks.

Performance benchmarks are designed to direct management's focus. These benchmarks usually stress factors such as revenue or product development goals; they tend to push down the importance of everything else, including the maintenance of adequate financial and operational controls. Including control quality in corporate performance benchmarks keeps the issue of controls on management's agenda. And private equity investors, who typically make their continued involvement in the company contingent on its hitting financial targets, will find that incorporating controls into their evaluations materially protects their investment.

3

Establish a culture of transparency and accountability.

Rapid growth will test the strength of an enterprise's culture, particularly with the influx of many new hires who have no history with the organization. The CEO and top management need to send a consistent message that transparency and accountability are integral to performance and that managers will be held responsible on this score.

Including control quality in corporate performance benchmarks keeps the issue of controls on management's agenda while materially protecting investors.

4

Assume these crimes will happen and prepare accordingly.

Companies that have never experienced fraud, theft or other forms of misappropriation naturally assume that their luck will hold. But organizational growth increases financial complexity and thus the opportunities for malfeasance. The company's financial leadership needs the knowledge and experience to stay ahead of burgeoning threats by continually monitoring and upgrading controls.

5

Actively promote and enforce compliance with corporate standards.

Standards don't enforce themselves. Indeed, left to their own devices, offices and divisions will develop their own processes and workarounds; these improvisations weaken the overall control structure. At the same time, corporate leaders can't simply impose a set of standards; all of the organization's functions need to buy into the changes and take ownership of upholding the new expectations. This will require the ongoing education of employees, reinforcement of procedures, and diligent oversight.

Making financial and operational controls an ongoing priority is a challenge for most business leaders, who are usually judged on revenue, profit margin and similar factors reflecting bottom-line performance. Maintaining a focus on controls is even tougher when the company is in growth mode, working to secure investments and perform against revenue benchmarks. Yet investing the effort to ensure that controls keep pace with the business is a modest price to pay for protecting the company's expanding assets.



AMINE ANTARI

Managing Director,
Middle East Head
Business Intelligence and
Investigations
Dubai, UAE
amine.antari@kroll.com



HIROKI KATAYAMA

Managing Director, Japan Head
Business Intelligence and
Investigations
Tokyo, Japan
hiroki.katayama@kroll.com



RECAREDO ROMERO

Regional Managing Director, Latin
America
Business Intelligence and
Investigations
Bogotá, Colombia
rromero@kroll.com

Beyond Compliance: Creating a Culture of Integrity

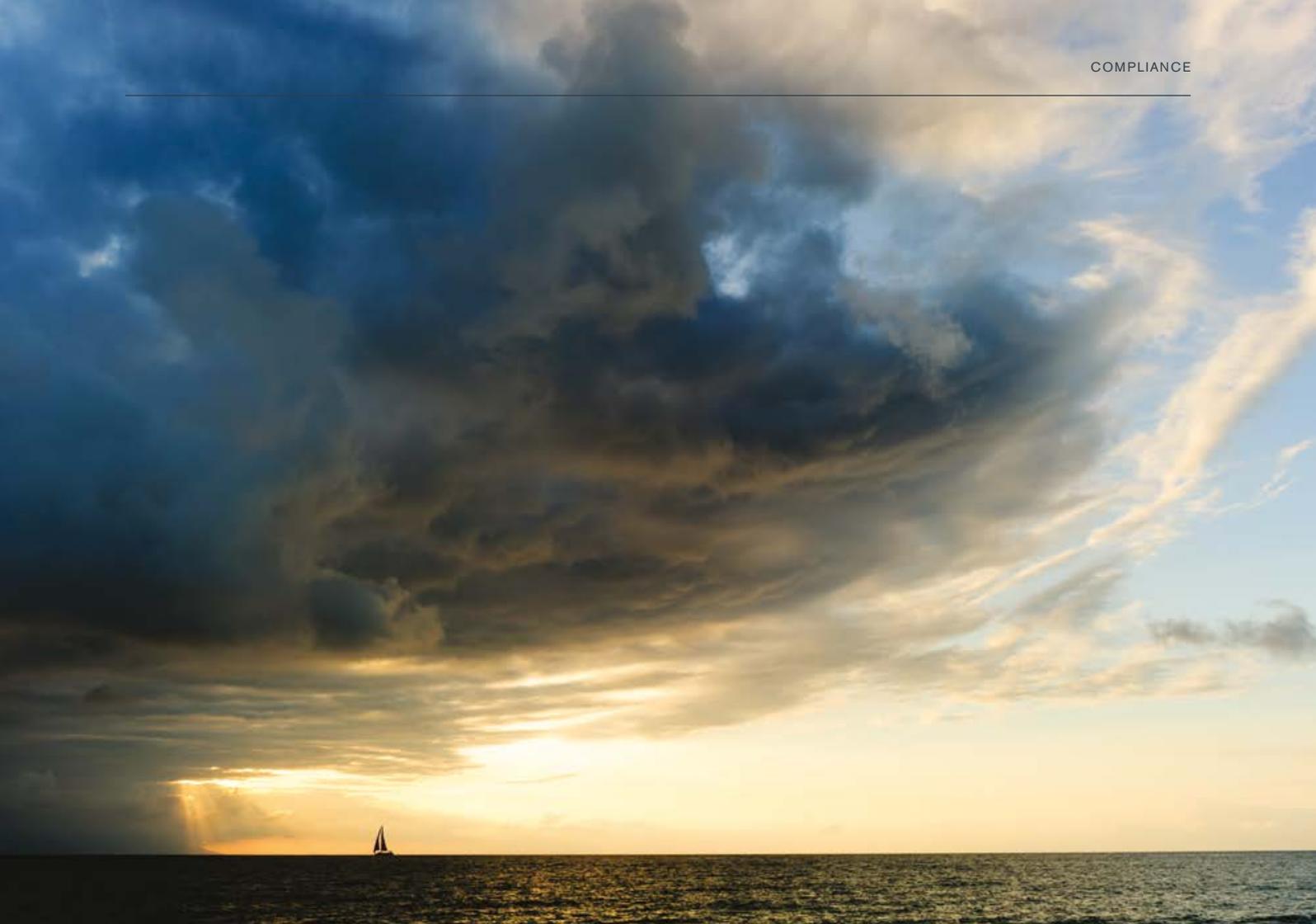
Integrating transparency, accountability and ethical behavior into company culture can help organizations mitigate risk and keep ahead of regulatory change.

Compliance forms an integral part of virtually every organization's operations. Depending on the organization's ownership structure, industry and location, everything from its accounting to its human resources may be subject to a regulatory regime, industry association guidelines or internal codes of conduct. Organizations that operate in more than one jurisdiction will, of course, have to contend with different regimes in each place.

The significant legal, financial, and reputational damage that a violation can bring is reason enough for enterprises to stress compliance. Yet compliance is also critical, because poor compliance often signals the larger problem of poor business practices, which expose the organization to further risk. Ultimately, compliance is about more than fulfilling regulatory or other obligations: It involves establishing a culture of integrity that is centered on transparency, accountability and ethical behavior.

A culture of integrity yields benefits beyond those that come with scrupulous behavior. Government regulations, which can seem ubiquitous, are also often in flux. Any jurisdiction's regulatory priorities can vary significantly over time, depending on the administration in power and other variables. An effort at regulatory reform at the national level may filter down unevenly to the local level or may cross industries. In addition, emerging industries often find that they are operating in regulatory gray areas. At those times, companies with strong cultures of integrity can stay ahead of regulatory change. Moreover, enterprises from more stringent jurisdictions will prefer to do business with companies where compliance is just considered the right thing to do.

The real test of the commitment to a culture of integrity is how it responds to questionable or prohibited behavior—particularly when the transgression involves a key employee or a member of management.



However, building a culture of integrity is a broader, more complex undertaking than simply ensuring that checklists and reporting mechanisms are in place. In our experience working with governments and corporations to help build, sustain and monitor such cultures, we have found that they rest on a foundation of six distinct elements:

- 1 Tone from the top:** An organization takes its direction from its leaders. A board that emphasizes compliance will likely be able to communicate that message much more powerfully than the head of compliance or internal audit.
- 2 Resourcing:** A stated commitment to transparency and accountability must be backed up with the resources needed to build and maintain such a culture.
- 3 Processes and controls:** The right procedures provide a framework that ensures that decision making and actions are transparent and do not involve conflicts of interest. Controls allow the organization to identify and respond to exceptions and weaknesses that are more systemic.
- 4 Education:** Everyone in the organization must understand what is expected. Executives and employees also need ongoing reinforcement and training so that they can apply their judgment in unexpected or ambiguous situations.
- 5 Performance goals and incentives:** Ultimately, executives and employees act according to how they are incentivized. Board members and senior management must understand that unrealistic deadlines or budget constraints can constitute risks in their own right. Managers should set performance goals that can be achieved without compromising integrity, transparency, or compliance.
- 6 Response and remediation:** The real test of an organization's commitment to a culture of integrity is how it responds to questionable or prohibited behavior. Particularly in cases where the transgression involves a key employee or a member of management, the temptation to rationalize or overlook the misdeed can be high.

In our survey, we asked respondents about the extent to which they followed various best practices for instilling a culture of integrity (see Figure 16). Globally, each of the eight best practices is followed by roughly three-quarters of the organizations surveyed. However, while 35 percent say they have adopted all eight practices, one in four organizations say they have adopted half at most.

It is notable how few respondents *strongly* agree that their organization's performance goals and incentives do not conflict with its risk management practices. While all of the practices listed are important, ensuring that performance goals and incentives can be met without compromising integrity is arguably the single most important step that organizations can take in building a culture of integrity.

While 35 percent of organizations say they have adopted all eight practices, one in four have adopted half at most.

For most organizations, building a culture of integrity is an ongoing task, with each element at a different level of strength at any given time. Organizations can use a matrix to assess the state of their culture of integrity and prioritize areas requiring further work (see Figure 17).

FIGURE 16
HOW DO ORGANIZATIONS PROMOTE A CULTURE OF INTEGRITY?



FIGURE 17

THE INTEGRITY MATRIX

WEAK	EMERGING	MODERATE	STRONG
TONE FROM THE TOP			
<p>Leadership does not acknowledge the importance of integrity.</p> <p>Management exhibits an “ends justify the means” mentality.</p>	<p>Leadership gives a pro forma acknowledgement of the importance of following procedures.</p> <p>Compliance is separated from other company functions.</p> <p>The board is not involved.</p>	<p>Fully staffed compliance office delivers intermittent updates to the board.</p> <p>Integrity as good business is reinforced in ongoing internal communications from the CEO and in day-to-day decision making throughout the organization.</p> <p>Company executives consciously set an example through their actions.</p>	<p>The chief compliance officer has direct access to and support of the CEO and board and is included in strategic decision making.</p> <p>The organization consciously guards its reputation for integrity in its partnerships and business decisions.</p> <p>The audit committee incorporates oversight of company integrity into its work.</p>
RESOURCING			
<p>The compliance function is minimally staffed and resourced.</p>	<p>Compliance receives the resources it needs to fulfill requirements, but rarely more.</p>	<p>Compliance is viewed as an investment rather than an expense. Programs are adequately resourced without cutting corners.</p>	<p>Management makes strategic investments to continuously improve the compliance program.</p>
PROCESSES AND CONTROLS			
<p>A minimally sufficient compliance mechanism exists, in order to conform to regulations.</p> <p>Controls are weak or absent.</p>	<p>The compliance mechanism is robust.</p> <p>Some controls are in place.</p>	<p>Processes extend beyond compliance to reinforce transparency and accountability at key points within the organization.</p>	<p>Extensive processes are paired with effective controls that are actively monitored.</p> <p>Controls are holistically analyzed to “connect the dots.”</p>
EDUCATION			
<p>Education is minimal and strictly focused on compliance procedures.</p>	<p>Compliance procedures are instilled and reinforced through training and regular retraining.</p>	<p>Education extends beyond compliance to include the importance of transparency and accountability.</p>	<p>Education includes opportunities to sharpen judgment and to practice dealing with unknown or ambiguous situations.</p>
PERFORMANCE GOALS AND INCENTIVES			
<p>Performance goals are aggressively set with no consideration of ethics or integrity.</p> <p>Incentives and disincentives are based entirely on “making one’s numbers.”</p>	<p>Employees do not feel pressured to act unethically, but neither is there reinforcement of ethical behavior.</p>	<p>It is implicitly and explicitly understood that high performance does not excuse unethical behavior.</p>	<p>Integrity is incorporated into evaluations and promotions.</p> <p>Executives and managers are evaluated in part on their teams’ integrity.</p>
RESPONSE AND REMEDIATION			
<p>Responses to ethical breaches are completely situational.</p>	<p>A written code of conduct and other guidelines sets forth expected behavior and consequences for ethical breaches.</p> <p>No escalation policy exists to ensure that ethical breaches are addressed at the proper level in a timely fashion.</p>	<p>Executives and managers are expected to respond in a consistent manner to ethical breaches.</p> <p>Ethical breaches that result in compliance failures are self-reported to the appropriate agency.</p> <p>An escalation policy, including an effective whistleblower mechanism, is in place.</p>	<p>Employees have confidence that standards are applied consistently.</p> <p>The board ensures that the CEO and senior management are held to high ethical standards.</p> <p>Serious ethical breaches are met with thorough internal investigations; findings are used to improve processes.</p>





04

TECHNOLOGY

**ALAN BRILL**

Managing Director
Cyber Risk
Secaucus, NJ, US
abrill@kroll.com

**HUGO HOYLAND**

Associate Manager
Business Intelligence
and Investigations
London, UK
hugo.hoyland@kroll.com

**KEN C. JOSEPH**

Managing Director, Global Head
Disputes
New York, NY, US
ken.joseph@duffandphelps.com

**JOSHUA MCDOUGALL**

Director
Cyber Risk
Denver, CO, US
joshua.mcdougall@kroll.com

Proceed with Caution: Using Controls to Manage Risk in Digital Currency Transactions

A case study of cryptocurrency theft provides a primer on some of the risks that can accompany digital assets, as well as possible mitigations.

More and more organizations, from governments to the private sector, are capitalizing on the benefits and efficiencies of digital currency in their payments and settlements systems. Indeed, 28 percent of respondents to this year's *Global Fraud and Risk Report* survey confirmed that they already use cryptocurrency in some way. Facebook's announcement of the Libra initiative, involving several major financial services institutions, provides further evidence of the gathering momentum behind digital currency.

However, venturing into digital currency is not without peril for organizations. The threats include fraud, theft, money laundering, terrorist financing, tax evasion, manipulation and illiquidity—all encased in a wrapper of regulatory uncertainty. Enterprises need to respond with a coherent risk-based strategy that identifies the unique challenges faced by each organization and then mitigates and controls those risks across a range of environments, including legal, regulatory and operational compliance; risk management; information technology; data privacy and security; finance; and internal audit. Putting compliance and controls at the center of technology adoption is crucial to managing the risk of new and complex ventures.

THE CASE OF THE MISSING MILLIONS

Recent investigations conducted by Kroll have highlighted some of the risks, threats and costs that an organization may face as a result of an ineffective system of compliance and controls in the use of digital currency. A number of cryptocurrency exchanges, for example, have contacted us after suffering losses from criminals who have exploited weaknesses in the exchanges' know your customer (KYC) and payment processes. In this work, we have found that traditional techniques can be quite effective when conducting investigations in the digital world of cryptocurrency. These techniques include constructing fictional digital personas to communicate with suspected thieves and mapping corporate structures, internet traffic and social media activity to reveal hidden relationships between actors. In one case, for example, Kroll was contacted by a cryptocurrency payment-processing company claiming it had to refund millions of dollars to several customers whose bitcoin accounts had been hacked. Kroll was able to uncover suspiciously close ties between the purported victims and the payment-processing company; the matter is now being investigated by law enforcement.

REGULATION AND TRANSPARENCY

Several observations can be gleaned from the matters we have investigated. First, tracking the transactions frequently proves to be a major obstacle. Cryptocurrency is often touted for its transparency; in theory, anyone with access to the underlying blockchain can trace the path of a cryptocurrency block from its origin to each transaction it has touched. The reality, however, is not so straightforward. Tracking crypto transactions can be time-consuming and inconclusive due to the anonymity of the parties in each transaction. Indeed, some cryptocurrencies seek to differentiate themselves from their competitors by promoting the strength of their anonymity. Hopefully, the draft guidance issued in June by the Financial Action Task Force (FATF), which recommends that virtual asset service providers adopt KYC safeguards and share customer information, will be a first step toward true transparency.

The new FATF guidance underscores the importance of cryptocurrency's global regulatory and enforcement framework, which at the moment is very much in flux. This situation is partly due to the usual lag that occurs when regulation has to catch up to technological innovation. So it is that countries with weak or no cryptocurrency regulations have the potential to become safe havens for perpetrators who wish to obscure their transactions and operate away from regulatory scrutiny.

But regulating crypto requires confronting an even deeper challenge. Cryptocurrency was developed precisely to facilitate transactions outside the frameworks established by government agencies and the financial services industry. In fact, crypto constitutes a direct challenge to the state's heretofore exclusive right to issue currency. The market's desire for crypto's benefits, however, is forcing the crypto industry and governments to create regulations for an entity that was designed to be unregulated. Not surprisingly, that task has been an arduous one.

Meanwhile, as that framework emerges, other risks loom beyond those related to fraud and theft. Unfortunate timing is one: Organizations that are early adopters may develop extensive procedures only to have to change them in the wake of evolving regulation (as, for example, the European Union's General Data Protection Regulation, California's Consumer Privacy Act and similar legislation from other jurisdictions are forcing organizations to do with respect to data privacy). The lack of adequate regulation can also delay broader public confidence in crypto, leading to adoption rates that fall short of what the organization anticipated when management decided to invest in a cryptocurrency system. Enterprises need to account for variables of this sort when devising their crypto strategies.

THE IMPORTANCE OF CONTROLS

Recent thefts at cryptocurrency exchanges highlight the need to maintain proper controls—not just at exchanges but at any organization using cryptocurrency. In one investigation, Kroll discovered that the exchange could not access information about how the payment service provider settled transactions and moved cash; further, the exchange released uncollateralized bitcoin to buyers before payment had been received—a practice very much at odds with standard procedures for exchanging tangible goods for fiat currency. This anomaly helps illustrate a key principle: Fundamentally,

any transaction involving cryptocurrency should be handled as it would be if it involved fiat currency. For example, if a transaction in excess of \$10,000 requires the approval of two corporate officers, the same controls should apply whether the transaction is in fiat or cryptocurrency—just as they should apply whether the transaction is in dollars or euros. The onboarding process for new customers should involve the same level of due diligence, whether those customers are paying in crypto or fiat currency. In fact, due diligence of a client's cryptocurrency transactions should be integrated into

the organization's existing KYC procedures to deliver a single panoramic view of customer risk.

Insufficient crypto controls often come about because organizations view cryptocurrency as an IT or cybersecurity issue and fail to include the perspective of compliance, internal audit and other key functions. Under these conditions, not only are controls inadequate, but important internal information regarding cryptocurrency transactions also goes uncollected, making it difficult to fully reconstruct fraud or theft involving crypto.

When imposing controls on crypto-based transactions, organizations will need to adapt the rules somewhat to account for the mechanics behind digital currency. In one recent case, the perpetrators used "bitcoin blenders" to scramble transactions and hobble the tracing of activity on the blockchain ledger. Other fraud techniques seek to take advantage of the time lag—usually between 10 minutes and one hour—that occurs before a transaction is authenticated on the cryptocurrency's underlying blockchain. This vulnerability can be mitigated, however, by altering the transaction process: Rather than releasing the acquired goods immediately, a company could impose a short waiting period to allow the transaction to be confirmed by the required number of users on the blockchain.

Sometimes the necessary changes to controls are not immediately apparent. Suppose, for example, that both the CEO and the CFO must approve certain transactions, whether executed in fiat or cryptocurrency. In a disaster scenario such as a plane crash involving those two officers, the board of directors and the general counsel could pass the appropriate resolutions and, with the company's financial institutions, implement the necessary transition so that the company could retain full access to its capital. With crypto, however, the company would have to anticipate the problem, perhaps by storing credentials in "virtual escrow" to allow continuing access in case of such an emergency.

A similar risk is that of cryptocurrency becoming inaccessible due to a ransomware attack that locks users out of the organization's computer network. Cryptocurrency has all the same vulnerabilities as other digital files, so an organization's crypto-assets are only as safe as the cybersecurity protecting them. Organizations thus should consider using offline ("cold") cryptocurrency wallets and incorporating crypto-specific security guidelines such as the CryptoCurrency Security Standard (CCSS) into their overall cybersecurity framework.

Insufficient crypto controls often come about because organizations view cryptocurrency as an IT or cybersecurity issue and fail to include the perspective of other key functions.

MAINTAINING A HEALTHY SKEPTICISM

Given the various risks associated with crypto, organizations are well advised to maintain a healthy skepticism when evaluating their level of adoption. This entails making sure crypto proponents are not the only ones involved in the discussion. In addition, at each decision point, risk analysis should involve not just IT and cybersecurity but also legal, treasury, corporate compliance and internal audit functions. As the organization's use of crypto deepens, enterprises need to ensure that key players, such as the chief information security officer, have adequate experience to accurately evaluate crypto's costs and benefits. When it comes to establishing sufficient cryptocurrency controls, corporations do not want to find themselves in the vulnerable position of learning as they go along.

When incidents do occur, it is important that they be approached with the same expertise in investigations that

would be brought to a traditional fraud or theft. In the exchange case discussed at the beginning of this article, for example, the evidence that established the likelihood of collusion came about through the same process of gathering information and testing hypotheses that is used to solve analog crimes.

Cryptocurrency undoubtedly offers benefits in a world that places a premium on speed and efficiency. But it will be some time before regulators, law enforcement and industry have fully established foundational safeguards. In the interim, organizations that embrace crypto must take it upon themselves to ensure that digital currency's risks are thoroughly identified and mitigated.



Harnessing Machine Learning for Due Diligence: Realizing the Possibilities

A wave of technology solutions driven by advances in artificial intelligence promises to revolutionize due diligence. However, it's essential to keep expectations realistic and to know how your machine learning program learns.

The increased emphasis on due diligence and the ever-growing amount of open source and proprietary data available on due diligence subjects combine to create an ideal use case for machine learning technology. While automated due diligence platforms offer tantalizing possibilities, they can also lead to frustration and unfulfilled expectations. Organizations considering these solutions can greatly increase the chances of success by approaching implementation holistically and by knowing how to evaluate technologies critically.

WHAT TECHNOLOGY CAN—AND CANNOT—DO

As with all technology, implementation of a due diligence platform powered by machine learning needs to begin not with the technology but with the larger context of improving the function itself. This means starting with a comprehensive review of the due diligence workflow. What are the regulatory or best-practice requirements that must be met? How are data and risk assessments about customers and other third parties shared across the organization? How adequate is the response mechanism to identified risks? Mapping the overall due diligence function and identifying gaps and bottlenecks will provide a blueprint for progress. Some of those gains will be powered by technology, but others will require changes in processes or capabilities. For example, a due diligence platform may help an institution increase the throughput volume and the consistency of risk ratings, but achieving meaningful gains in due diligence effectiveness may also require thorough data remediation and a clarified risk escalation framework. Making technology part of a larger solution thus allows the institution to specify its technology requirements—and expectations—with greater precision. That solution also should reflect the institution's overall preference for either building in-house compliance capabilities or outsourcing them.

After determining the requirements for the technology, the enterprise must factor in perspectives from its various divisions. The IT department's view will be based on how the due diligence technology needs to integrate with existing systems. The cybersecurity team will need to ensure that no vulnerabilities are being introduced, and the finance department will want to know the expected return on investment.



DARREN BURRELL

Vice President
Compliance Risk and Diligence
Reston, VA, US
darren.burrell@kroll.com

PEERING INSIDE THE BLACK BOX

These steps provide a framework for establishing the platform's functional requirements, but that is only part of the equation. Organizations must also be able to evaluate the technology itself, a task made all the more challenging by the ubiquity of the term *machine learning* and the absence of a clarifying legal standard for it. Consequently, organizations evaluating due diligence platforms need to be sure they understand exactly what those products deliver. Such understanding is critical because an application's inner workings directly determine the volume, accuracy and speed it will achieve under real-world conditions.

The most common form of machine learning uses what is known as *supervised learning*. In supervised learning, an algorithmic model is fed large amounts of historical data and seeks predictive patterns. For example, it might use data on the size, location, amenities, and sales price of homes. As the model analyzes the data, it attempts to predict the sales price of each home, checking its prediction against the actual price information that is included in the dataset. With each prediction it makes, the model fine-tunes itself until it can satisfactorily predict a home's sales price based on the other variables. In the due diligence context, a model might be used to identify and classify risk-relevant information, reduce false positives when researching against open source data or assign a money laundering risk score to a customer based on transaction history, currency used, industry, jurisdiction and other attributes.

Two key takeaways emerge from this overview. First, while human programmers necessarily revise the learning algorithm to improve its accuracy, the prediction process itself occurs with no outside intervention. This defining characteristic of true machine learning is an essential criterion in any product evaluation. Some due diligence programs that claim to be driven by machine learning actually use low-cost labor through platforms like Amazon Mechanical Turk to make predictions by applying simple checklists.

Second, the quality of the algorithmic model is largely determined by the quality and quantity of the data used to train it. Indeed, this explains why firms like Google and Facebook distribute machine learning programs as open source software: These companies use the massive amounts of data their programs collect to refine the proprietary machine learning models they use internally. The data is actually more valuable than the algorithms themselves, because of its volume and because, being naturally generated, it reflects the nuance and randomness of the real world. Thus, for due diligence models, training datasets collected by analysts in the course of research and discovery are superior to datasets that have been artificially assembled. Naturally-generated datasets represent real-world scenarios more accurately while also capturing the thought processes of the expert analysts who compiled the data during their due diligence work.

Machine learning technology can be a powerful component of an organization's due diligence arsenal. However, enterprises considering using such a tool need to specify its role in detail and to subject its internal workings to careful review.





ANDREW BECKETT

Managing Director, EMEA Head
Cyber Risk
London, UK
andrew.beckett@kroll.com



BENEDETTO DEMONTE

Managing Director, North America Head
Cyber Risk
New York, NY, US
bdemonte@kroll.com



PAUL JACKSON

Managing Director,
Asia Pacific Head
Cyber Risk
Hong Kong, China
paul.jackson@kroll.com



JASON SMOLANOFF

Managing Director, Global Head
Cyber Risk
Los Angeles, CA, US
jason.smolanoff@kroll.com

Cybersecurity Breaks Out of Its Silo

Cyber intrusions can quickly morph into legal, financial and reputational crises. To keep pace, cybersecurity is transcending its traditional boundaries.

In a world in which digital assets can be more valuable than physical assets, and computer networks control operations from production to customer service, cybersecurity can no longer be seen as a stand-alone function. Instead, it is now part of a larger security picture, just as cybercrime is now simply crime pursued by digital means rather than some narrow form of technical malfeasance. This trend is highlighted in our survey results, which show that across a range of incident types, computer networks were the primary channel of the intrusion in one-fifth to almost one-half of cases. But even for incident types where cybersecurity breaches are most likely to be a primary cause—such as data or IP theft—plenty of cases exist in which cyber breaches played only a partial or even little to no role. The traditional silo around cybersecurity, like so many other silos today, is breaking down (see Figure 18 on page 62).

Companies that spend millions of dollars on technology solutions must ensure that they also provide the ongoing resources, policies and procedures needed to make that technology work.

MOVING BEYOND THE ARMS RACE

This convergence of risk is bringing about a new way of thinking about cybersecurity and **who in the organization is responsible for it**. It is increasingly common, for example, for organizations to charge either the general counsel or a chief security officer with overseeing the entire risk portfolio, including cybersecurity. The chief information security officer thus becomes part of a team of executives whose collective remit might include physical security, threat assessment, crisis management and more.

Risk convergence is also leading organizations to adopt a broader strategy to **cyber risk assessment**. Traditionally, cybersecurity has been approached as a technology-driven arms race against bad actors. Today, however, forward-thinking enterprises set cybersecurity priorities by looking inward to identify the most important elements of the business and the data and technologies those elements involve. This examination is followed by a deceptively simple question: Exactly why do we need a cybersecurity program? For example, a freight company might see cybersecurity as a means of meeting insurance requirements, whereas a bank may consider cybersecurity a key element of its brand promise.

Placing cybersecurity within the organization's larger strategic picture also sheds light on the types of **threat actors** that an organization faces, because different threat actors gravitate toward different assets. Organized crime, for example, typically targets payment processors. State-sponsored

hackers, by contrast, prefer intelligence gleaned from airline passenger itineraries. Each category of actor will have its own characteristic set of behaviors and tools to be countered. This more holistic view of the cyber threats a company faces allows it to better determine what steps will bring its cybersecurity risk below its risk appetite threshold.

Just as organizations are taking a broader view of their cyber risk, so too are they taking more sophisticated approaches to **risk mitigation**. The continual emergence of new risk vectors means that serious intrusions are no longer a question of *if* but *when*. As a result, cyber strategy is no longer dominated by protection; organizations are working to distribute attention among identification, protection, detection, response and recovery. Doing so requires the coordination of multiple aspects of the organization, including the business, compliance, communications, internal audit and legal departments.

Implementing this broader approach calls for a greater understanding across the organization of what is required and what is at stake. An organization's cybersecurity leaders no longer make the mistake of thinking that issuing a policy is the same as enforcing one; they also have more sensitivity to the cost in time and convenience that cybersecurity requirements impose across the enterprise. In turn, the rest of the business increasingly understands its role in preventing cyber breaches and the very real impact those incidents can have.



WHY CYBERSECURITY FAILS

Even a comprehensive and well-designed cyber program, however, can fall short in its implementation. Indeed, most cyber breaches occur not because of a lack of design but rather because of poor execution. The ability to execute depends on the **operational maturity** of an organization's cyber measures—that is, how well those measures are supported by other aspects of the business. A first-class cyber threat detection system, for example, is of little use without an adequate number of trained personnel who can respond quickly to the alerts generated by that system. A commitment

to remediate the harm done to customers who have had their account records stolen needs to be backed up with customer service centers that can quickly scale to handle the influx of calls certain to occur after an incident.

It is ironic that operational maturity is of such importance to cybersecurity yet so often gets little attention. Companies that spend millions of dollars on technology solutions must ensure that they also provide the ongoing resources, policies and procedures needed to make that technology work.



REACHING OPERATIONAL MATURITY

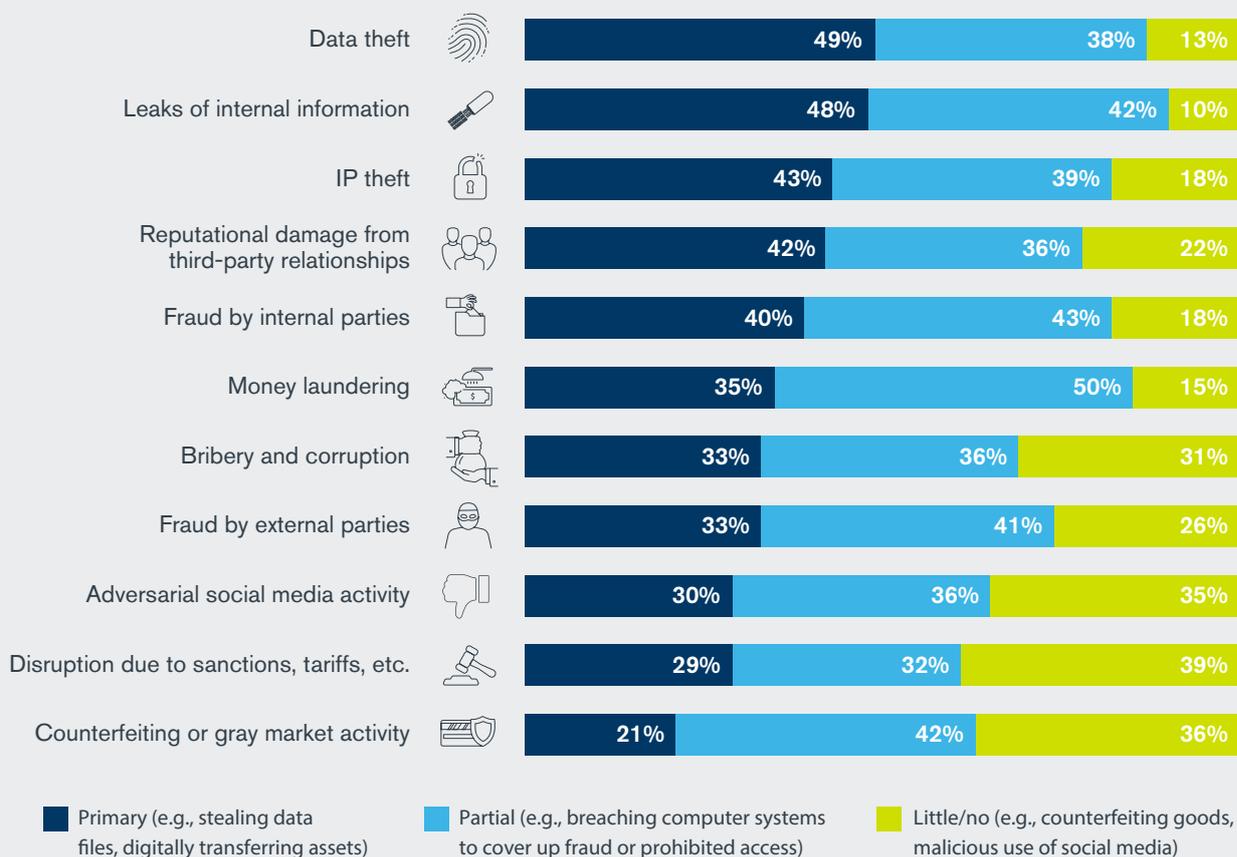
Organizations can take two important steps to accelerate their operational maturity. The first is to have adequate **strategic and tactical governance**. This helps ensure that a holistic cyber strategy has been developed, sufficient resources have been allocated and the necessary processes and procedures have been put in place. At a tactical level, good governance provides the mechanisms for resolving conflicts between policy and implementation that come about even when everyone involved is sensitive to the costs and necessity of cybersecurity compliance. Further, conflicts arise between various aspects of security. Network security and information security, for example, have different approaches and priorities, frequently requiring mediation between the two.

Second, organizations need to establish the sufficient **internal audit and control capabilities** to monitor the performance

of their cybersecurity systems as well as the elements, like the security operations center, that support it. To the extent possible, that auditing should involve quantitative measures of performance rather than merely subjective assessments. Real-time monitoring should be complemented with tabletop exercises that test the responses of people and systems under more extreme conditions.

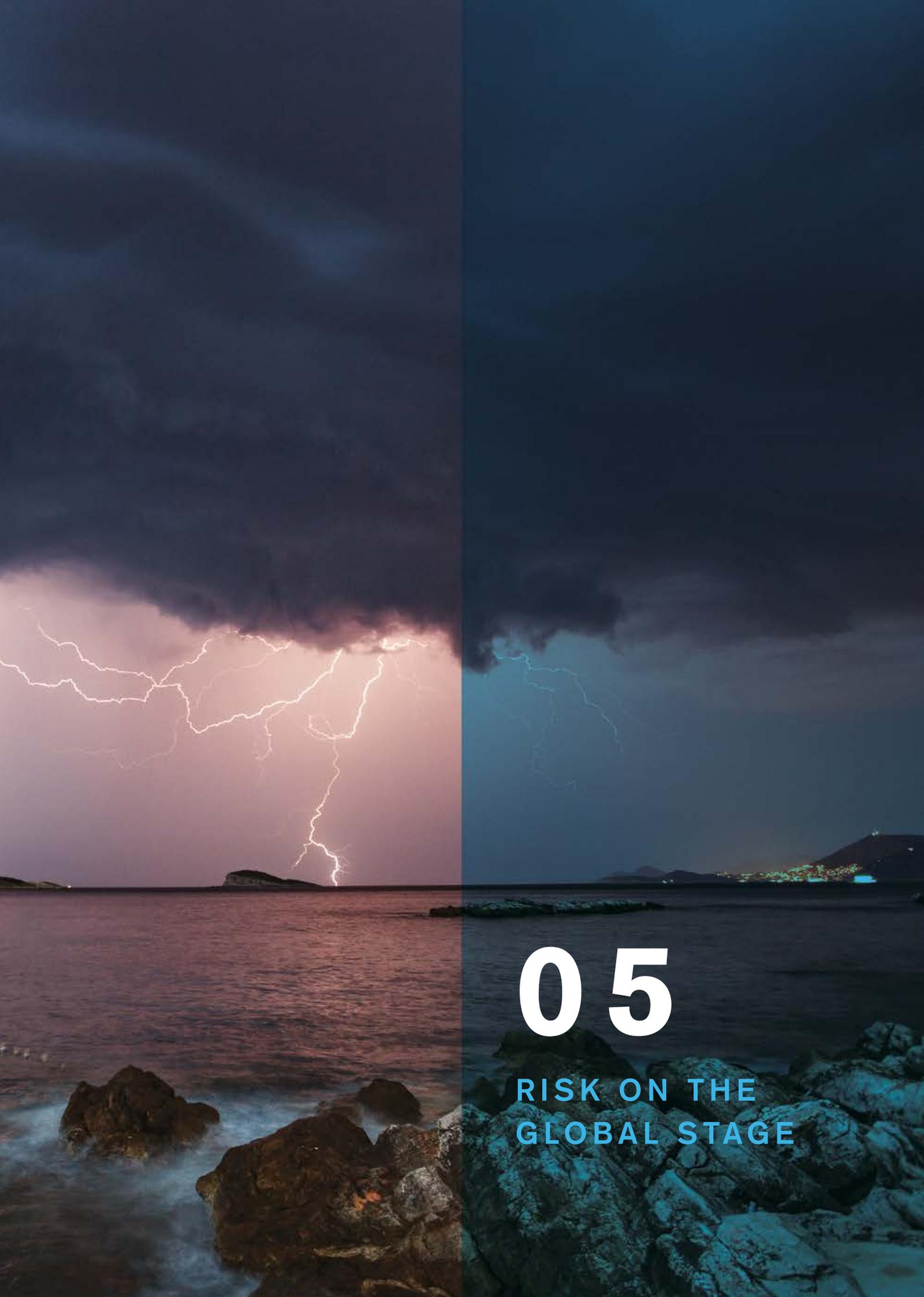
Cybersecurity poses systemic challenges to many organizations: Its boundaries shift constantly, it requires ongoing commitment and it doesn't directly generate revenue. Yet it does help create trust and confidence, which are both essential for revenue-generating relationships. Furthermore, now that cyber issues are so deeply woven into the fabric of most businesses, expanding an organization's cybersecurity efforts will significantly mitigate risks throughout the enterprise.

FIGURE 18
WHAT ROLE DID COMPUTER SYSTEM BREACHES PLAY IN INCIDENTS DURING THE LAST YEAR?*



*"Don't know/Not applicable" responses excluded. Percentages do not total 100 percent due to rounding.





05

RISK ON THE
GLOBAL STAGE

Illicit Fund Flows in Ten Steps

Illicit fund flows present a significant risk to global trade. Here's how they can occur.

Illicit fund flows are estimated to total as much as \$1 trillion each year. Large-scale fraud, corruption and money laundering frequently involve the complicated and rapid movement of funds among organizations in multiple countries. While jurisdictions are increasingly collaborating to fight illicit fund flows, each still has its own regulatory and enforcement infrastructure, policies, capabilities and priorities. These differences create gaps that make it possible for sophisticated actors to evade detection.

Examples of conditions that can give rise to illicit fund flows include:

- Developing countries with abundant natural resources but weak financial crime controls that are susceptible to the misappropriation of sovereign funds by unscrupulous government officials
- Banks or other financial institutions with insufficient credit or risk assessment procedures that are targeted by organizations seeking to procure capital for unauthorized purposes
- Companies that exercise insufficient oversight of subsidiaries in countries with high levels of illicit activity, making it possible for their local staff to collude with bad actors to circumvent background or security checks

Figure 19 illustrates a typical illicit fund flow scenario, in which a bank is defrauded of €10 million as a trade financing loan it made is used to buy a resort villa. Many of the vulnerabilities in this scenario can be avoided by having a clear approach to risk management. These steps include:

- Comprehensive due diligence before any potential partnerships are undertaken
- Operationally effective risk assessment policies and procedures
- Regular monitoring of activities in the context of the risks posed—for example, by the activities undertaken or by jurisdictions of operation
- A governance and risk-control framework to provide stakeholders and management with adequate oversight of activities and of the sufficiency of the mitigations that are in place



PAUL NASH

Associate Managing Director
Business Intelligence and
Investigations
London, UK
paul.nash@kroll.com



CLAIRE SIMM

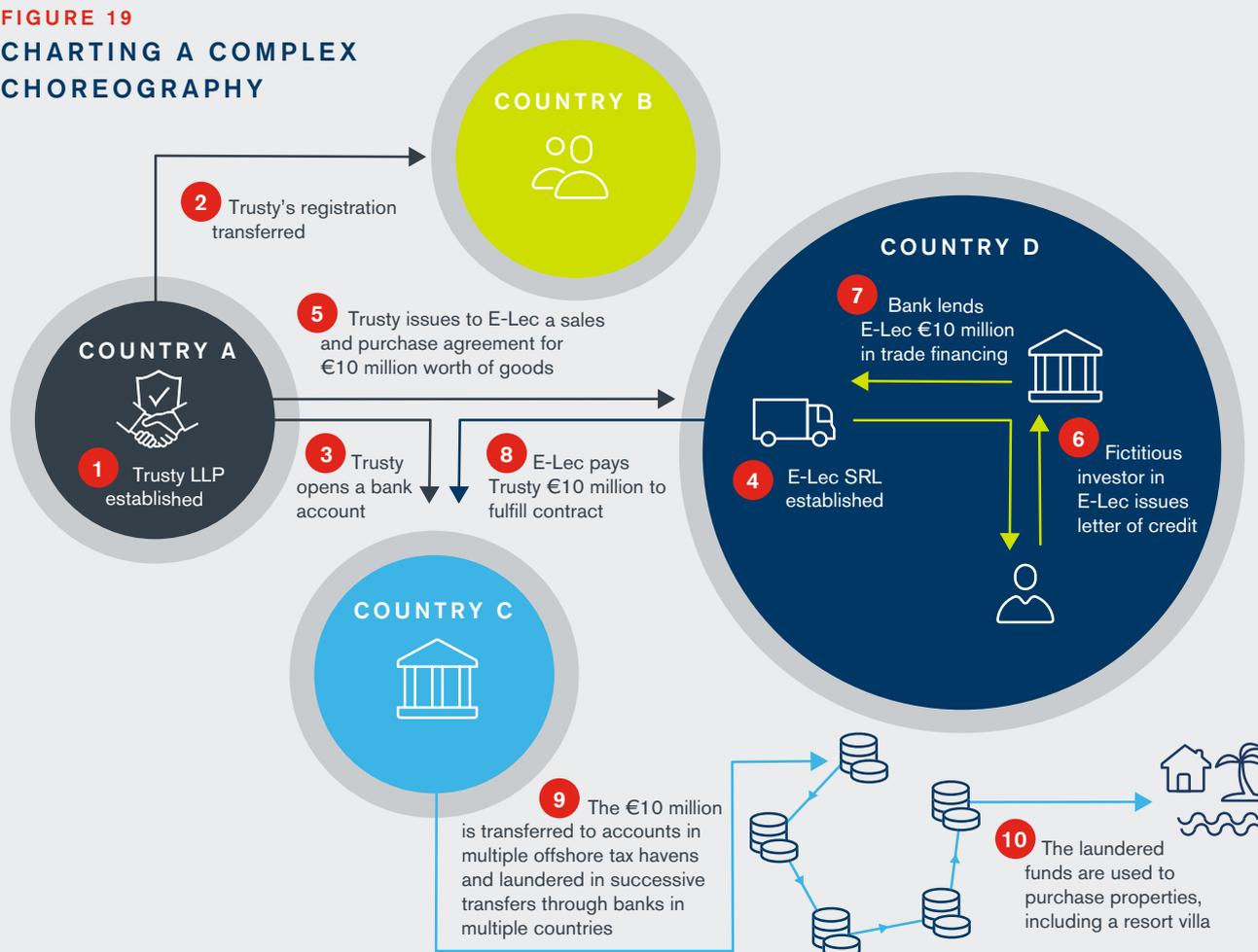
Managing Director
Compliance and
Regulatory Consulting,
London, UK
claire.simm@duffandphelps.com



DENNIS VINOKOUROV

Associate Managing Director
Business Intelligence and
Investigations
Moscow, Russia
dennis.vinokourov@kroll.com

FIGURE 19
CHARTING A COMPLEX
CHOREOGRAPHY



- 1** Trusty LLP, a limited liability partnership, is established in Country A. Country A has few, if any, requirements regarding transparency of beneficial ownership. The registered address for Trusty is shared by hundreds of companies, yet no active business operates from the premises. The nature of Trusty's business is broadly stated as "international trade and investment."
- 2** Once Trusty is established, its registration is transferred to individuals in Country B, a country that also has limited beneficial ownership regulations. This transfer further obscures control of the company.
- 3** Although Country A has few requirements for transparency of ownership when forming LLPs, it has stringent regulations requiring banks to know their customers and monitor transactions for signs of money laundering. To bypass these regulations, Trusty establishes an account at a bank in Country C, a developing nation that does not yet have a sophisticated infrastructure for preventing financial crime; that deficiency makes it difficult for authorities elsewhere to obtain information on account holders if suspicions arise.
- 4** A second company, E-Lec SRL, purporting to be a wholesaler/distributor of electrical fittings, is established in Country D. In reality, E-Lec is inactive and conducts no business.
- 5** A sales and purchase agreement is generated, calling for E-Lec to purchase €10 million worth of electrical fittings from Trusty.
- 6** Ostensibly to purchase those electrical fittings for resale, E-Lec requests trade financing from a commercial bank, also in Country D. The company secures the financing with collateral in the form of a letter of credit, supported by falsified bank statements, from a fictitious E-Lec investor.
- 7** The commercial bank lends €10 million to E-Lec.
- 8** E-Lec wires the €10 million to Trusty's bank account.
- 9** Those funds are immediately transferred to secondary bank accounts held in multiple offshore tax havens to further obscure the flow of the illicit funds.
- 10** Eventually the funds are used to purchase properties in several countries, including a villa at a beach resort. The loan is in default but cannot be collected, as the individuals behind both Trusty and E-Lec have disappeared.



FERNANDA BARROSO

Managing Director, Brazil Head
Business Intelligence and
Investigations
São Paulo, Brazil
fernanda.barroso@kroll.com



TARUN BHATIA

Managing Director,
South Asia Head
Business Intelligence and
Investigations
Mumbai, India
tarun.bhatia@kroll.com



HOWARD COOPER

Managing Director
Business Intelligence and
Investigations
London, UK
hcooper@kroll.com



ZOË NEWMAN

Managing Director
Business Intelligence and
Investigations
London, UK
znewman@kroll.com

Corruption at Scale: Managing Risk with Governments and State-Owned Enterprises

Understanding the factors that can make government corruption so persistent helps companies and investors navigate these challenges.

In today's global economy, the regional silos that once separated corporations, investors, and lenders have largely disappeared, creating a dynamic marketplace and bringing together new combinations of companies, lenders, investors and suppliers. Importantly, governments and state-owned enterprises (SOEs) have also entered the mix in full force. Governments of rapidly growing countries are seeking low-cost capital with less onerous terms and conditions in order to engage contractors for large-scale infrastructure projects, while state-owned enterprises are looking for suppliers, investors and acquirers in a similar manner to privately held companies.

Governments and SOEs can be highly desirable business partners, but such ventures carry certain risks; governments and their officials are uniquely susceptible to corruption due to the powers wielded by the state. The same holds true of SOEs, by virtue of the blurred line between the enterprise and the government. Furthermore, the increased opportunity to do business with governments and SOEs comes at a time when the fight against corruption is high on the agenda of many governments, leading to increased collaboration between regulators and law enforcement agencies of different jurisdictions. Also, non-governmental sources of primary funding, such as international organizations and global NGOs, increasingly make due diligence of corruption risk a condition of their involvement. Augmenting past anti-corruption efforts, which typically involved scrutinizing corporations involved with governments or SOEs, these organizations are incorporating forensic oversight into their funding of government projects.

THE OIL THAT LUBRICATES THE SYSTEM

The governments of many countries where corruption has been an issue are actively working to combat the problem, aware that doing so is a prerequisite for foreign direct investment. However, just as governments and SOEs are uniquely vulnerable to corruption, there are also particular forces that can make corruption difficult to dislodge once it has taken hold. Understanding those forces is critical for any enterprise that is considering doing business in a market where government corruption is part of the landscape.

Corruption in government goes beyond the misdirection of funds or the payment of bribes. It spreads through routine transactions, becoming the oil that lubricates the system. It

affects how projects get awarded and how business gets done. The launch of an anti-corruption campaign—or even intensified media scrutiny of the problem—can thus significantly disrupt a country's business culture. Companies competing for government contracts now need to define a different set of ethics and behavior for their managers and employees and to develop a culture that supports those changes. But that is only part of the solution. Enterprises also need to adjust to competing on the basis of performance, which has implications across the organization, from strategic decision making to hiring and compensation. Not surprisingly, undertaking this culture shift throughout a company's economy is a process that takes years of dedicated effort.

STRADDLING GOVERNMENT AND PRIVATE ENTERPRISE

Fighting corruption in SOEs brings its own challenges, precisely because these institutions straddle the line between government and private enterprise. This hybrid structure makes it easier for dishonest officials to use SOEs to expatriate and launder government funds, for example, or to steer contracts to private-sector bidders in exchange for bribes.

Ironically, a government's anti-corruption efforts can actually exacerbate an SOE's corruption problem. Strong anti-corruption measures often involve putting SOEs under additional regulatory scrutiny and implementing whistleblowing procedures. Yet this level of examination can paralyze some SOE managers. The tendency is exacerbated in SOEs where executives tend to stay for only two or three years, making it difficult to achieve long-term systemic changes in the organization.

Even where corruption is not an issue, doing business with an SOE requires a heightened level of due diligence. The management and boards of SOEs are more likely to include politically exposed persons, increasing the risk of violating sanctions, bribery and corruption regulations, or similar restrictions. This concern is magnified in jurisdictions where it is difficult to determine ultimate beneficial ownership. In many cases, SOEs lack the infrastructure to rigorously screen for potential conflicts. Therefore, when investors perform due diligence as part of potential SOE privatizations, they are well advised to identify those conflicts at the beginning and to implement compliance mechanisms going forward.

Governments and SOEs are powerful economic players in the global economy and represent compelling markets for business and investment. However, enterprises that enter those markets need to ensure that they maintain the higher level of awareness and diligence that these environments demand.

When Business and Geopolitics Converge

With protectionism on the rise and countries moving to safeguard their technology and citizens' data as a matter of national security, companies are incorporating geopolitics into their risk calculations.



STEVE CORNMELL

Managing Director

Disputes

London, UK

steve.cornmell@duffandphelps.com



VIOLET HO

Managing Director, Greater China Head

Business Intelligence and
Investigations

Hong Kong, China

vho@kroll.com



NICOLE Y. LAMB-HALE

Managing Director

Business Intelligence and
Investigations

Washington, DC, US

nicole.lamb-hale@kroll.com

Globalization is often discussed as if it were an irrepressible force of nature or an inevitable consequence of digitalization and a growing consumer class. In fact, globalization is the result of numerous conscious policy choices by countries working individually and collectively to create an environment favorable to free trade. However, the long expansion of globalization has given way to a rise in protectionism: the levying of tariffs, the use of sanctions, the unraveling of established trade alliances, and the expansion of restrictions on foreign investment. Each of these developments has dramatically increased the geopolitical risks that organizations face when doing business abroad. Our survey findings confirm that enterprises are navigating through a growing minefield of regulatory considerations and that they must also anticipate future geopolitical shifts that could disrupt market access, contracts and assumptions underlying their cross-border business strategies (see Figure 20 on page 71).

MOVING BEYOND FINANCIAL FORECASTING

Financial forecasting has long been an essential part of strategic planning; entire departments are built around it. Today's more complex and more dynamic international environment obligates enterprises to expand their geopolitical forecasting capabilities. At first glance, this task may seem daunting, but there are practical steps that companies can take, especially in the due diligence of cross-border transactions.

As part of that process, an organization must go beyond assessing its own prospects in a potential cross-border relationship and step back to look at the situation from the counterparty's perspective. This involves taking the time to understand all the forces—including economic and political ones—to which that counterparty is subjected. Our survey shows that many organizations are factoring these issues into their due diligence (see Figure 21 on page 72).

The extent to which geopolitical due diligence is effective, however, depends on an organization's sensitivity to forces that may not be readily apparent to foreign observers. Western companies doing business in China, for example, can make the mistake of assuming that a Chinese counterparty with a solid track record of fulfilling its contracts poses little risk of non-performance. However, if the Chinese government later implements a new trade policy that effectively prohibits the company from continuing to fulfill the contract, the company has little recourse in the face of what is essentially a *force majeure*.

Assessing these risks requires on-the-ground intelligence, starting with a thorough understanding of the counterparty and its context and relationships. Does the counterparty play a role in its regional or national economy that puts it under special scrutiny? To what local regulatory guidelines is it subject? What are the priorities of those regulatory agencies, and how much

latitude do they have in establishing new rules? What are the trends in enforcement? Although geopolitical shifts can seem unexpected, governments often signal their intentions prior to making their moves. Mapping the counterparty's environment in this way allows one to spot the potential ripple effects of future changes in government policy.

Geopolitical concerns can arise in domestic mergers and acquisitions as well. Even if both parties are headquartered in the same country, an acquiring company must thoroughly vet the target's operations, its value chain, and the business dealings and relationships of the target's owners and management, including other entities in which they may have an interest. It is quite possible that any of these elements will expand the geopolitical exposure of the acquirer. In the urgency to get the deal done, details such as this cannot be overlooked; doing so can plant the seeds for increased sanctions risk and other problems later.



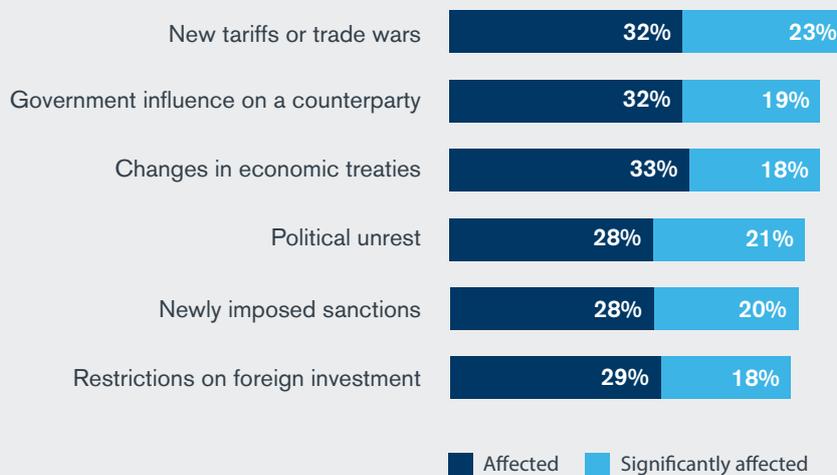
“NATIONAL SECURITY” BECOMES A COMMON REFRAIN

Given the recent overall increase in geopolitical tensions and greater sensitivity to protecting a country's technology and its citizens' data, many ripple effects are likely to emanate from the broadening of national security concerns. One vivid example of the expanded role of national security concerns in trade policy involves the Committee on Foreign Investment in the United States (CFIUS), which vets foreign investments in the United States from a national security perspective. (While CFIUS is a high-profile example of a national security regulatory body, many other countries have similar regulatory bodies.) In 2018, the statute authorizing CFIUS was amended; it now instructs the U.S. government to actively work with its allies in aligning foreign investment regulations among countries. Organizations should therefore expect such regulations to play a larger role in global trade. The convergence of anti-money laundering and anti-corruption regulations across jurisdictions illustrates how such an alignment may evolve.

Now more than ever, businesses need to consider national security concerns as a business risk. In performing their due diligence, they should assess national security issues with the same focus that they give to concerns such as antitrust compliance. This entails assessing how a potential business transaction or investment will look from the perspective of the counterparties' governments, and possibly that of other governments as well. A transaction involving a foreign investor may seem innocuous on the surface, but how regulators choose to categorize a business or its industry, technologies, and data and those of its counterparty can result in heightened scrutiny.

The best response to such scrutiny is to meet it head-on, structuring the deal to mitigate the issues that are likely to raise objections. For example, a U.S. company with a division that has clearance to work with the U.S. Department of Defense might choose to exclude that division from the

FIGURE 20
WHICH GEOPOLITICAL RISKS HAVE AFFECTED ORGANIZATIONS IN THE PAST YEAR?



company's sale to a foreign buyer. Further, when presenting the deal for CFIUS approval, the company should proactively disclose the potential national security concern, propose mitigating solutions and express its readiness to submit to independent auditing or monitoring to ensure compliance. This level of proactivity requires both a sophisticated understanding of the regulatory environment and a broader view of what constitutes risk.

Heightened tensions among nations require that companies sharpen their statecraft—in other words, that they work to understand situations from the perspectives of a broader group of stakeholders, including regulators. Incorporating those points of view into due diligence and ongoing situational intelligence can be an effective way for an organization to deftly navigate geopolitical risk.

Now more than ever, businesses need to consider national security concerns as a business risk, including those issues in due diligence just as they do antitrust compliance.

FIGURE 21
HOW DO ORGANIZATIONS INCORPORATE GEOPOLITICAL RISKS INTO DUE DILIGENCE?



Global Risk Map

■ Most common incident ■ Top risk priority ■ Top future concern



North America

Latin America



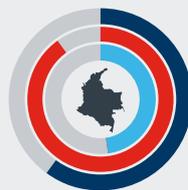
- 1 CANADA**
- 38% Adversarial social media activity
- Fraud by external parties
- 69% Data theft
- 58% Market manipulation through fake news
- Large-scale, coordinated cyberattacks



- 2 U.S.**
- 30% Disruption due to sanctions, tariffs, changes in trade agreements, etc.
- 73% Data theft
- 72% A significant financial crisis



- 3 MEXICO**
- 46% Leaks of internal information
- 89% Data theft
- Large-scale, coordinated cyberattacks
- 71% Breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.



- 4 COLOMBIA***
- 50% Leaks of internal information
- Adversarial social media activity
- 90% Reputational damage due to third-party relationship
- Disruptions caused by artificial intelligence or other technologies
- 60% Breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.

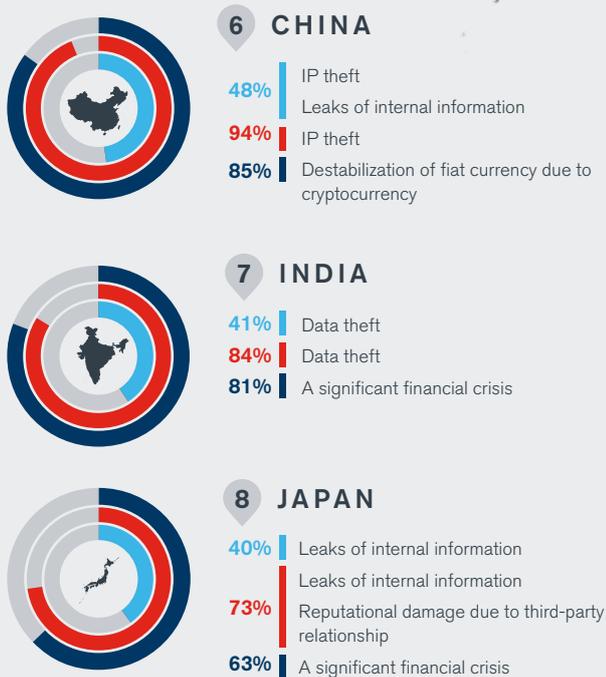


- 5 BRAZIL**
- 55% Leaks of internal information
- 84% Data theft
- 77% Large-scale, coordinated cyberattacks

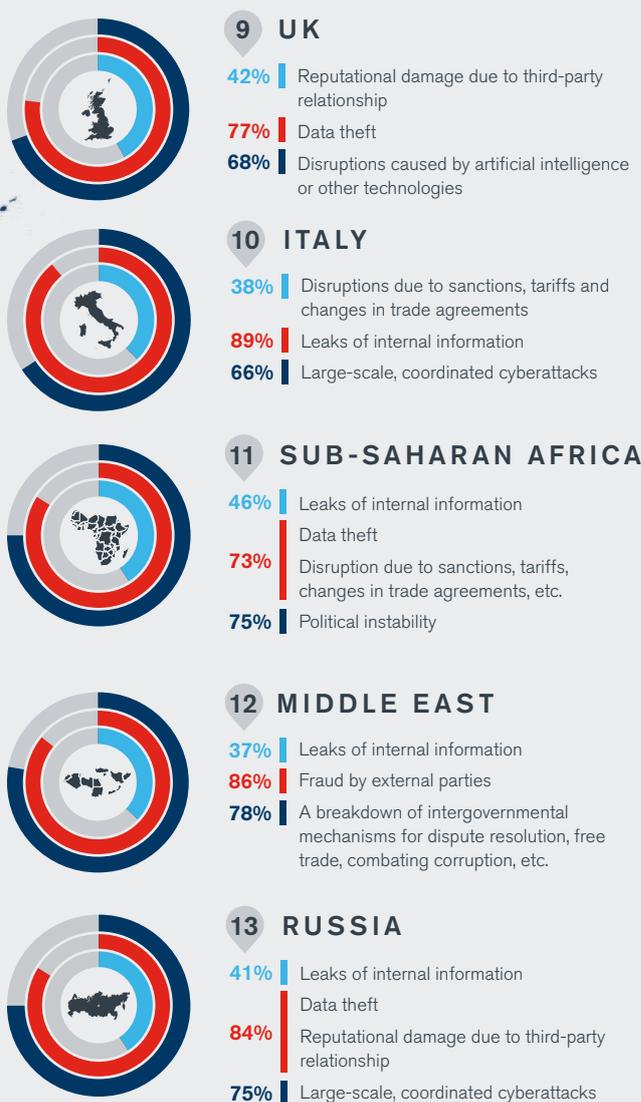
*Due to low sample size, percentages are directional only.



Asia Pacific

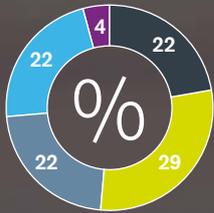


Europe, Middle East and Africa



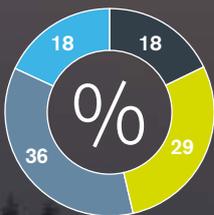


USE OF BRAND "INFLUENCERS"



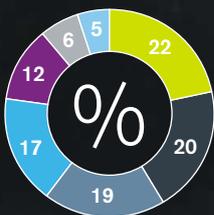
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Third parties (e.g., joint venture partners, suppliers/vendors)
- Employees
- Customers
- Contractors
- Competitors
- Unknown/random actor
- Politically motivated actors
- Politically motivated actors

Canada

Following a 2016 arbitration ruling that held companies responsible in certain circumstances for protecting their workers against social media attacks, Canadians are well aware of the risks of **adversarial social media activity**. Canadian respondents are more likely than those everywhere but in China to report that they have been a target of this type of threat (38 percent vs. 27 percent globally). Canadian respondents also report an above-average level of **IP theft** (33 percent vs. 24 percent globally), a finding that reinforces the argument for strengthening the country's IP protections.

Canadian organizations are skeptical about the efficacy of many internal detection mechanisms. Only 58 percent of respondents consider their **anti-money laundering controls** effective in detecting incidents (vs. 69 percent globally); the same percentage call their **whistleblowing** function effective (vs. 66 percent globally); and 60 percent deem their **anti-bribery and corruption controls** effective (vs. 69 percent globally). Perhaps not surprisingly, a greater percentage of incidents were uncovered by **external audit** in Canada (26 percent) than anywhere else.

While Canadian respondents are likely to say that their organizations follow some cultural practices promoting transparency and accountability, the perception of **a clear message from the top supporting integrity and accountability** is significantly lower than the average (67 percent vs. 78 percent globally), as is the belief that their companies **respond to risk management incidents in consistent ways** (67 percent vs. 75 percent globally). These findings reflect an ongoing discussion within the country about strengthening regulations and developing a business culture that promotes consistent transparency, accountability and anti-corruption efforts.

In light of the various threats reported by Canadian respondents and the apparent below-average confidence in controls and key aspects of culture, it is surprising that a relatively low share of Canadian organizations in our survey consider mitigating risks to be a priority across all risk types. However, this apparently relaxed attitude toward risk does align with the relatively low percentage of Canadians who say there is clear messaging from the top of their organizations regarding the importance of integrity, compliance and accountability (as discussed above). This lower level of concern about risk extends to emerging threats as well. For example, only 49 percent of Canadian respondents are concerned about the possibility of a **significant financial crisis** (vs. 69 percent globally), while just 44 percent express concern about the possibility of a **breakdown of intergovernmental mechanisms** for issues such as dispute resolution and free trade (vs. 61 percent globally). Canadian corporate leaders may wish to assess whether their organizations are assigning the appropriate level of importance to risk management.

Cryptocurrency in Canada is facing increasingly aggressive regulation, having experienced major upheaval when the country's largest crypto exchange went defunct following the CEO's unexpected death in 2018. It makes sense, then, that Canadian organizations are cautious about adopting cryptocurrency. While above-average percentages of Canadian respondents report investigating adoption of cryptocurrency (29 percent vs. 22 percent globally) or having a pilot program (36 percent vs. 31 percent globally), only 18 percent of Canadian organizations actively use it (vs. 28 percent globally).

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Adversarial social media activity	38%	27%	▲ 11%
Fraud by external parties	38%	28%	▲ 10%
Leaks of internal information	33%	39%	▼ -6%
IP theft (e.g., trade secrets)	33%	24%	▲ 9%
Reputational damage due to third-party relationship	31%	29%	▲ 2%
Data theft (e.g., customer records)	29%	29%	■ 0%
Fraud by internal parties	29%	27%	▲ 2%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	27%	27%	■ 0%
Bribery and corruption	22%	23%	▼ -1%
Counterfeiting or gray market activity	20%	17%	▲ 3%
Money laundering	20%	16%	▲ 4%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Changes in economic treaties between countries	49%	51%	▼ -2%
Restrictions on foreign investment	49%	47%	▲ 2%
New tariffs or trade wars	44%	54%	▼ -10%
Government influence on a vendor, partner, customer or other entity with which your company does business	44%	51%	▼ -7%
Political unrest	42%	49%	▼ -7%
Newly imposed sanctions against doing business with a government, entity or person	36%	47%	▼ -11%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Data theft (e.g., customer records)	69%	76%	▼ -7%
IP theft (e.g., trade secrets)	64%	72%	▼ -8%
Leaks of internal information	64%	73%	▼ -9%
Fraud by external parties	64%	68%	▼ -4%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	60%	62%	▼ -2%
Fraud by internal parties	58%	66%	▼ -8%
Reputational damage due to third-party relationship	58%	73%	▼ -15%
Adversarial social media activity	58%	63%	▼ -5%
Counterfeiting or gray market activity	53%	58%	▼ -5%
Money laundering	51%	62%	▼ -11%
Bribery and corruption	38%	62%	▼ -24%
LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?			
<i>(Percent "concerned" or "very concerned")</i>			
Market manipulation through fake news	58%	59%	▼ -1%
Large-scale, coordinated cyberattacks	58%	68%	▼ -10%
Political instability	51%	63%	▼ -12%
A significant financial crisis	49%	69%	▼ -20%
Climate change	47%	54%	▼ -7%
Disruptions caused by artificial intelligence or other technologies	47%	56%	▼ -9%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	44%	61%	▼ -17%
Destabilization of fiat currency due to cryptocurrency	38%	53%	▼ -15%
Military conflict	36%	51%	▼ -15%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
External audit	26%	17%	▲ 9%
Internal audit	25%	28%	▼ -3%
By management at our company	13%	16%	▼ -3%
Regulator/law enforcement	13%	13%	■ 0%
Whistleblower	12%	13%	▼ -1%
Customers/suppliers	10%	13%	▼ -3%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	87%	81%	▲ 6%
Data analytics	78%	77%	▲ 1%
Due diligence of third-party reputation and practices	71%	73%	▼ -2%
Compliance (regulatory, codes of conduct, etc.)	69%	75%	▼ -6%
Monitoring social media for adversarial activity	64%	71%	▼ -7%
Anti-bribery and anti-corruption controls	60%	69%	▼ -9%
Anti-money laundering controls	58%	69%	▼ -11%
Whistleblowing	58%	66%	▼ -8%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

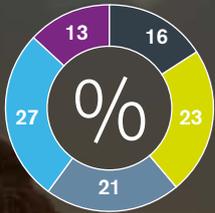
Business partners	95%	92%	▲ 3%
Potential M&A targets	95%	89%	▲ 6%
Suppliers	93%	92%	▲ 1%
Board or senior executive candidates	90%	91%	▼ -1%
Customers	88%	88%	■ 0%
Investors	86%	84%	▲ 2%
Brand ambassadors/influencers	83%	85%	▼ -2%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

Risk management programs are designed with input from those who must conform to them.	78%	74%	▲ 4%
Employees view risk management processes as being effective.	76%	76%	■ 0%
New business initiatives are regularly examined for all appropriate risk implications.	73%	74%	▼ -1%
Serious breaches of risk management processes are met with thorough internal investigations.	73%	75%	▼ -2%
Our risk management processes are adapted to local market and cultural nuances.	71%	72%	▼ -1%
Performance goals and incentives do not conflict with risk management practices.	71%	71%	■ 0%
The company responds to risk management incidents in a consistent way.	67%	75%	▼ -8%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	67%	78%	▼ -11%

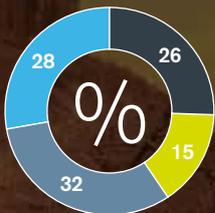


USE OF BRAND "INFLUENCERS"



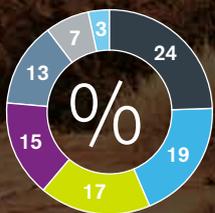
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Contractors
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Competitors
- Customers
- Unknown/random actor
- Politically motivated actors

United States

The risk landscape within the United States is somewhat more subdued than in most of the other countries and regions we surveyed, with most threats occurring at below-average levels. The few exceptions are the threat of **disruption due to sanctions, tariffs and changes in trade agreements** (30 percent vs. 27 percent globally) and some associated geopolitical risks, most notably **new tariffs or trade wars** (59 percent vs. 54 percent globally) and **restrictions on foreign investment** (51 percent vs. 47 percent globally). These findings reflect the country's more aggressive trade policy in recent years. In contrast, **bribery and corruption** were reported by only 17 percent of respondents (vs. 23 percent globally), and **leaks of internal information** were reported at a lower rate in the United States than in any other country or region (29 percent vs. 39 percent globally).

The effects of geopolitical risks on U.S. organizations have not served to push mitigation strategies up the agenda there, however. Countering disruption from sanctions and similar actions is a priority for only 53 percent of U.S. respondents (vs. 62 percent globally). The prevalence of U.S. concerns about **IP theft** (70 percent vs. 72 percent globally) reflects ongoing issues with China. The position of **data theft** as the top U.S. risk priority could be a result of numerous high-profile data breaches that have increased awareness among regulators, investors and board members.

U.S. respondents give high marks to their **compliance** capabilities, with 84 percent calling this function's detection capabilities effective. This confidence is mirrored in respondents' strong belief that their organizational cultures support transparency and accountability. For example, 86 percent of U.S. respondents agree that their workplaces get a **clear message from the top of their organizations that integrity, compliance and accountability are important** (vs. 78 percent globally).

Organizations in the United States, like enterprises elsewhere, report practicing reputational due diligence widely—except that those in the United States are less likely than average to apply it to **investors** (76 percent vs. 84 percent globally). This anomaly may reflect the dominant role played in the United States by large investors, whose leadership teams are under close and ongoing scrutiny by both regulators and the business media.

Looking ahead, a sizable majority of respondents in the United States express concern about the possibility of a **significant financial crisis** (72 percent vs. 69 percent globally) as well as **large-scale, coordinated cyberattacks** (70 percent vs. 68 percent globally). Acknowledging the current geopolitical situation, they are also comparatively more likely to register concern about a **breakdown of intergovernmental mechanisms** (66 percent vs. 61 percent globally).

U.S. organizations have been relatively aggressive in their use of **brand influencers**, with only 16 percent of respondents saying they never use them (vs. 22 percent globally) and 13 percent saying they always use them (vs. 9 percent globally). U.S. enterprises' adoption of **cryptocurrency**, meanwhile, is more restrained. While the share of U.S. organizations that report they are actively using cryptocurrency matches the global average (28 percent), the percentage saying they have no plans to do so (26 percent) is significantly larger than it is almost anywhere else (vs. 19 percent globally).

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	30%	27%	▲ 3%
Reputational damage due to third-party relationship	29%	29%	■ 0%
Leaks of internal information	29%	39%	▼ -10%
Fraud by external parties	27%	28%	▼ -1%
Data theft (e.g., customer records)	26%	29%	▼ -3%
Adversarial social media activity	23%	27%	▼ -4%
Fraud by internal parties	22%	27%	▼ -5%
IP theft (e.g., trade secrets)	19%	24%	▼ -5%
Bribery and corruption	17%	23%	▼ -6%
Counterfeiting or gray market activity	15%	17%	▼ -2%
Money laundering	15%	16%	▼ -1%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	59%	54%	▲ 5%
Political unrest	52%	49%	▲ 3%
Restrictions on foreign investment	51%	47%	▲ 4%
Changes in economic treaties between countries	50%	51%	▼ -1%
Government influence on a vendor, partner, customer or other entity with which your company does business	50%	51%	▼ -1%
Newly imposed sanctions against doing business with a government, entity or person	48%	47%	▲ 1%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Data theft (e.g., customer records)	73%	76%	▼ -3%
IP theft (e.g., trade secrets)	70%	72%	▼ -2%
Fraud by external parties	69%	68%	▲ 1%
Reputational damage due to third-party relationship	66%	73%	▼ -7%
Leaks of internal information	65%	73%	▼ -8%
Fraud by internal parties	64%	66%	▼ -2%
Adversarial social media activity	57%	63%	▼ -6%
Bribery and corruption	55%	62%	▼ -7%
Money laundering	54%	62%	▼ -8%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	53%	62%	▼ -9%
Counterfeiting or gray market activity	51%	58%	▼ -7%
LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?			
<i>(Percent "concerned" or "very concerned")</i>			
A significant financial crisis	72%	69%	▲ 3%
Large-scale, coordinated cyberattacks	70%	68%	▲ 2%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	66%	61%	▲ 5%
Political instability	65%	63%	▲ 2%
Disruptions caused by artificial intelligence or other technologies	60%	56%	▲ 4%
Market manipulation through fake news	59%	59%	■ 0%
Military conflict	54%	51%	▲ 3%
Destabilization of fiat currency due to cryptocurrency	50%	53%	▼ -3%
Climate change	49%	54%	▼ -5%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	30%	28%	▲ 2%
External audit	19%	17%	▲ 2%
By management at our company	17%	16%	▲ 1%
Customers/suppliers	13%	13%	■ 0%
Regulator/law enforcement	11%	13%	▼ -2%
Whistleblower	9%	13%	▼ -4%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	84%	81%	▲ 3%
Compliance (regulatory, codes of conduct, etc.)	84%	75%	▲ 9%
Data analytics	76%	77%	▼ -1%
Due diligence of third-party reputation and practices	76%	73%	▲ 3%
Monitoring social media for adversarial activity	73%	71%	▲ 2%
Anti-bribery and anti-corruption controls	67%	69%	▼ -2%
Whistleblowing	67%	66%	▲ 1%
Anti-money laundering controls	65%	69%	▼ -4%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

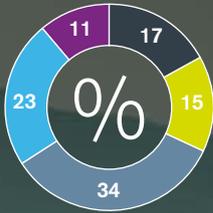
Business partners	93%	92%	▲ 1%
Board or senior executive candidates	92%	91%	▲ 1%
Suppliers	90%	92%	▼ -2%
Customers	90%	88%	▲ 2%
Potential M&A targets	87%	89%	▼ -2%
Brand ambassadors/influencers	84%	85%	▼ -1%
Investors	76%	84%	▼ -8%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	86%	78%	▲ 8%
Employees view risk management processes as being effective.	82%	76%	▲ 6%
Serious breaches of risk management processes are met with thorough internal investigations.	82%	75%	▲ 7%
Risk management programs are designed with input from those who must conform to them.	80%	74%	▲ 6%
The company responds to risk management incidents in a consistent way.	79%	75%	▲ 4%
Performance goals and incentives do not conflict with risk management practices.	78%	71%	▲ 7%
New business initiatives are regularly examined for all appropriate risk implications.	77%	74%	▲ 3%
Our risk management processes are adapted to local market and cultural nuances.	71%	72%	▼ -1%

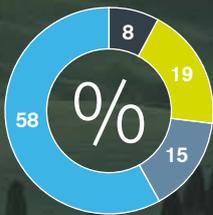


USE OF BRAND "INFLUENCERS"



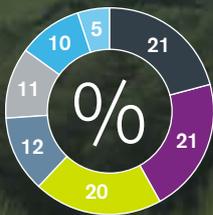
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Competitors
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Unknown/random actor
- Contractors
- Politically motivated actors
- Politically motivated actors

Italy

Recent developments have shone a bright light on the importance of international commerce to the Italian economy. It is no surprise, then, that survey respondents from Italy are more likely than those from any other country to report having been affected by **disruptions due to tariffs, sanctions and changes in trade agreements** (38 percent vs. 27 percent globally). At the same time, respondents there are less likely to report that they have been affected by specific geopolitical risks. These responses, taken together, suggest that Italian organizations are troubled by no single geopolitical issue but rather by a mix of concerns that has a particularly potent effect in that country.

Because Italy's manufacturing base focuses substantially on luxury goods, the country is a perennial target for **counterfeiting**. Italian respondents are thus more likely to report being affected by counterfeiting (23 percent vs. 17 percent globally) and to make the fight against counterfeiting a priority (70 percent vs. 58 percent globally). Notably, respondents in Italy report an above-average level of data theft (34 percent vs. 29 percent globally), even though the number of data breaches reported by Italian companies is significantly smaller than one would expect for an economy of its size. This suggests a need for more transparency regarding this category of incident.

Italian regulators seem inclined to integrate **cryptocurrency** into the larger economy. Indeed, respondents in Italy are significantly more likely than those in other countries to report that their organizations actively use cryptocurrency (58 percent vs. 28 percent globally). Only 8 percent of respondents say their organizations have no plans to do so (vs. 19 percent globally).

Italian respondents give high marks to many of their internal detection capabilities. Some of this satisfaction may reflect recent regulatory developments, such as the passing of more comprehensive legislation on **whistleblowing** and **anti-bribery and anti-corruption measures**. Eighty-nine percent of respondents in Italy say that their whistleblowing program is effective in detecting incidents (vs. 66 percent globally). Further, 81 percent of Italian respondents say their organizations are effective or highly effective in detecting corruption (vs. 69 percent globally). But the consistency with which Italian respondents consider their detection mechanisms to be effective also suggests that Italian organizations may be overestimating their capabilities and that a more objective review may be warranted.

It is worth noting that respondents in Italy are more likely than average to place priority on combating **fraud by internal parties** (74 percent vs. 66 percent globally) as well as by external parties (77 percent vs. 68 percent globally). An effective way to do so would be to strengthen the support for transparency and accountability within **corporate culture**. While **new business initiatives are regularly examined for risk implications** more often in Italy than elsewhere (85 percent vs. 74 percent globally), in other aspects, Italy hews to the global averages. Increasing transparency and accountability would help address respondents' fraud concerns.

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	38%	27%	▲ 11%
Data theft (e.g., customer records)	34%	29%	▲ 5%
Fraud by external parties	34%	28%	▲ 6%
Leaks of internal information	32%	39%	▼ -7%
Counterfeiting or gray market activity	23%	17%	▲ 6%
Fraud by internal parties	23%	27%	▼ -4%
Bribery and corruption	23%	23%	■ 0%
Reputational damage due to third-party relationship	21%	29%	▼ -8%
Adversarial social media activity	19%	27%	▼ -8%
IP theft (e.g., trade secrets)	19%	24%	▼ -5%
Money laundering	15%	16%	▼ -1%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	47%	54%	▼ -7%
Restrictions on foreign investment	40%	47%	▼ -7%
Political unrest	38%	49%	▼ -11%
Changes in economic treaties between countries	32%	51%	▼ -19%
Newly imposed sanctions against doing business with a government, entity or person	32%	47%	▼ -15%
Government influence on a vendor, partner, customer or other entity with which your company does business	30%	51%	▼ -21%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Leaks of internal information	89%	73%	▲ 16%
Reputational damage due to third-party relationship	83%	73%	▲ 10%
Data theft (e.g., customer records)	83%	76%	▲ 7%
IP theft (e.g., trade secrets)	79%	72%	▲ 7%
Fraud by external parties	77%	68%	▲ 9%
Fraud by internal parties	74%	66%	▲ 8%
Counterfeiting or gray market activity	70%	58%	▲ 12%
Bribery and corruption	68%	62%	▲ 6%
Adversarial social media activity	64%	63%	▲ 1%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	58%	62%	▼ -4%
Money laundering	55%	62%	▼ -7%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Large-scale, coordinated cyberattacks	66%	68%	▼ -2%
A significant financial crisis	64%	69%	▼ -5%
Political instability	60%	63%	▼ -3%
Market manipulation through fake news	58%	59%	▼ -1%
Disruptions caused by artificial intelligence or other technologies	57%	56%	▲ 1%
Climate change	53%	54%	▼ -1%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	51%	61%	▼ -10%
Destabilization of fiat currency due to cryptocurrency	43%	53%	▼ -10%
Military conflict	38%	51%	▼ -13%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	26%	28%	▼ -2%
By management at our company	25%	16%	▲ 9%
Regulator/law enforcement	14%	13%	▲ 1%
External audit	12%	17%	▼ -5%
Customers/suppliers	11%	13%	▼ -2%
Whistleblower	9%	13%	▼ -4%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	92%	81%	▲ 11%
Due diligence of third-party reputation and practices	91%	73%	▲ 18%
Compliance (regulatory, codes of conduct, etc.)	89%	75%	▲ 14%
Whistleblowing	89%	66%	▲ 23%
Monitoring social media for adversarial activity	87%	71%	▲ 16%
Data analytics	87%	77%	▲ 10%
Anti-bribery and anti-corruption controls	81%	69%	▲ 12%
Anti-money laundering controls	79%	69%	▲ 10%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

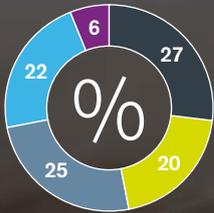
Potential M&A targets	92%	89%	▲ 3%
Board or senior executive candidates	90%	91%	▼ -1%
Investors	90%	84%	▲ 6%
Suppliers	89%	92%	▼ -3%
Business partners	85%	92%	▼ -7%
Brand ambassadors/influencers	84%	85%	▼ -1%
Customers	84%	88%	▼ -4%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

New business initiatives are regularly examined for all appropriate risk implications.	85%	74%	▲ 11%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	79%	78%	▲ 1%
The company responds to risk management incidents in a consistent way.	77%	75%	▲ 2%
Performance goals and incentives do not conflict with risk management practices.	75%	71%	▲ 4%
Serious breaches of risk management processes are met with thorough internal investigations.	75%	75%	■ 0%
Risk management programs are designed with input from those who must conform to them.	75%	74%	▲ 1%
Employees view risk management processes as being effective.	74%	76%	▼ -2%
Our risk management processes are adapted to local market and cultural nuances.	74%	72%	▲ 2%

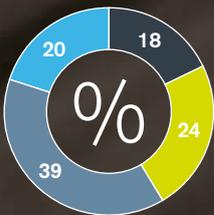


USE OF BRAND "INFLUENCERS"



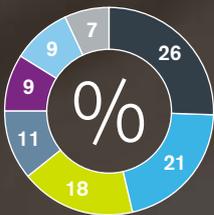
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Contractors
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Competitors
- Politically motivated actors
- Unknown/random actor

Middle East

Our survey results from the Middle East reflect the large role that **fraud, bribery and corruption** play in the region's risk profile. More than one-third of respondents there report **fraud by internal parties** within the last 12 months (35 percent vs. 27 percent globally), with almost as many having experienced **fraud by external parties** (33 percent vs. 28 percent globally); 29 percent report facing incidents of **bribery and corruption** (vs. 23 percent globally). Combating these risks is therefore a priority. For example, fighting fraud by external parties is prioritized by 86 percent of respondents in the Middle East, a higher percentage than anywhere else.

Along with addressing specific threats, some of the region's risk management priorities indicate a heightened awareness of risk generally. This awareness naturally develops as the region's enterprises work to scale their risk mitigation capabilities to match the Middle East's status as a global economic hub. Virtually every risk we asked about in our survey has a higher-than-average likelihood of being a priority for organizations in the Middle East. For example, combating **leaks of internal information** is a priority of 84 percent of respondents in the Middle East (vs. 73 percent globally) and **money laundering** is a priority of 78 percent there (vs. 62 percent globally).

The focus on money laundering can be seen in the introduction of new anti-money laundering regulations in many parts of the region and the fact that more than three-quarters of respondents in the Middle East rate their organizations' anti-money laundering detection capabilities as effective (76 percent vs. 69 percent globally). Despite geopolitical conditions that could make the area particularly vulnerable to this threat, participants there report a rate of money laundering that is in line with the global average. Organizations have also made a sustained effort to establish the **greater accountability and transparency** demanded by both local constituents and international business partners. Regarding the aspects of **company culture** that support these attributes, respondents in the Middle East give themselves ratings comparable to global averages. A higher percentage of risk incidents is uncovered by the **internal audit** function in the Middle East than almost anywhere else (36 percent vs. 28 percent globally).

Twenty percent of respondents in the Middle East report that their organizations are actively using **cryptocurrency**. While this figure is below the global average of 28 percent, it is in line with countries such as Japan (21 percent) and India (22 percent). Moreover, that figure is liable to increase, given that 39 percent of organizations in the Middle East report having pilot programs (vs. 31 percent globally) and that governments in the region are working to establish a receptive framework for digital assets.

Respondents in the Middle East are, not surprisingly, affected by **geopolitical risks** and sensitive to how those risks might develop. More than half of respondents in the Middle East report that within the last 12 months they were affected by **political unrest** (57 percent vs. 49 percent globally) and **changes in economic treaties** (59 percent vs. 51 percent globally). Looking ahead, 78 percent are concerned about a **breakdown of intergovernmental mechanisms** for collaboration (vs. 61 percent globally) and 75 percent are concerned about **political instability** (vs. 63 percent globally).

RISK LANDSCAPE

ISSUE	REGION	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	37%	39%	▼ -2%
Adversarial social media activity	35%	27%	▲ 8%
Fraud by internal parties	35%	27%	▲ 8%
Fraud by external parties	33%	28%	▲ 5%
Data theft (e.g., customer records)	31%	29%	▲ 2%
Bribery and corruption	29%	23%	▲ 6%
Reputational damage due to third-party relationship	25%	29%	▼ -4%
IP theft (e.g., trade secrets)	22%	24%	▼ -2%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	20%	27%	▼ -7%
Money laundering	18%	16%	▲ 2%
Counterfeiting or gray market activity	12%	17%	▼ -5%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Changes in economic treaties between countries	59%	51%	▲ 8%
Political unrest	57%	49%	▲ 8%
Government influence on a vendor, partner, customer or other entity with which your company does business	53%	51%	▲ 2%
Newly imposed sanctions against doing business with a government, entity or person	51%	47%	▲ 4%
Restrictions on foreign investment	51%	47%	▲ 4%
New tariffs or trade wars	49%	54%	▼ -5%

RISK STRATEGY

ISSUE	REGION	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Fraud by external parties	86%	68%	▲ 18%
Leaks of internal information	84%	73%	▲ 11%
Data theft (e.g., customer records)	78%	76%	▲ 2%
Money laundering	78%	62%	▲ 16%
Fraud by internal parties	76%	66%	▲ 10%
Reputational damage due to third-party relationship	73%	73%	■ 0%
Adversarial social media activity	71%	63%	▲ 8%
IP theft (e.g., trade secrets)	71%	72%	▼ -1%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	71%	62%	▲ 9%
Bribery and corruption	71%	62%	▲ 9%
Counterfeiting or gray market activity	65%	58%	▲ 7%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	78%	61%	▲ 17%
A significant financial crisis	76%	69%	▲ 7%
Political instability	75%	63%	▲ 12%
Large-scale, coordinated cyberattacks	75%	68%	▲ 7%
Market manipulation through fake news	71%	59%	▲ 12%
Destabilization of fiat currency due to cryptocurrency	59%	53%	▲ 6%
Climate change	57%	54%	▲ 3%
Disruptions caused by artificial intelligence or other technologies	55%	56%	▼ -1%
Military conflict	51%	51%	■ 0%

RISK MANAGEMENT IN PRACTICE

ISSUE	REGION	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	36%	28%	▲ 8%
External audit	20%	17%	▲ 3%
By management at our company	14%	16%	▼ -2%
Customers/suppliers	13%	13%	■ 0%
Whistleblower	10%	13%	▼ -3%
Regulator/law enforcement	7%	13%	▼ -6%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Data analytics	80%	77%	▲ 3%
Anti-money laundering controls	76%	69%	▲ 7%
Cybersecurity	76%	81%	▼ -5%
Compliance (regulatory, codes of conduct, etc.)	73%	75%	▼ -2%
Anti-bribery and anti-corruption controls	69%	69%	■ 0%
Monitoring social media for adversarial activity	67%	71%	▼ -4%
Due diligence of third-party reputation and practices	67%	73%	▼ -6%
Whistleblowing	57%	66%	▼ -9%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

Suppliers	98%	92%	▲ 6%
Customers	90%	88%	▲ 2%
Board or senior executive candidates	90%	91%	▼ -1%
Business partners	90%	92%	▼ -2%
Brand ambassadors/influencers	87%	85%	▲ 2%
Investors	85%	84%	▲ 1%
Potential M&A targets	82%	89%	▼ -7%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

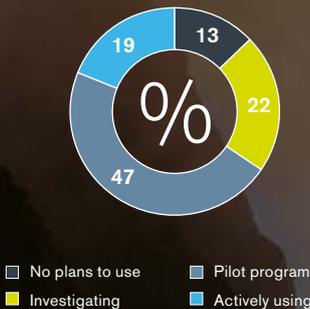
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	82%	78%	▲ 4%
Risk management programs are designed with input from those who must conform to them.	80%	74%	▲ 6%
New business initiatives are regularly examined for all appropriate risk implications.	78%	74%	▲ 4%
Employees view risk management processes as being effective.	78%	76%	▲ 2%
Our risk management processes are adapted to local market and cultural nuances.	76%	72%	▲ 4%
The company responds to risk management incidents in a consistent way.	73%	75%	▼ -2%
Serious breaches of risk management processes are met with thorough internal investigations.	71%	75%	▼ -4%
Performance goals and incentives do not conflict with risk management practices.	69%	71%	▼ -2%



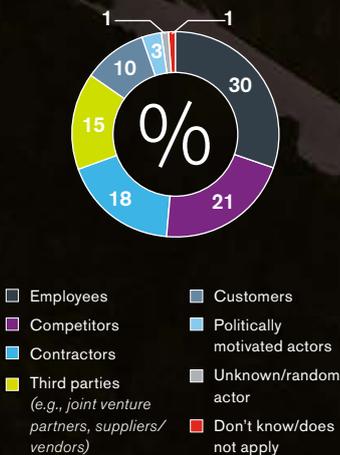
USE OF BRAND "INFLUENCERS"



ADOPTION OF CRYPTOCURRENCY



WHO WERE THE PERPETRATORS OF INCIDENTS?



Russia

Survey answers from respondents in Russia reveal how companies there are confronting risks in the context of still-emerging regulation and fluid cultural norms.

The percentage of survey respondents in Russia reporting significant effects from **bribery and corruption** is lower than in any country but Japan (16 percent vs. 23 percent globally). While bribery and corruption are commonly cited by foreign companies as a challenge when doing business in Russia, the survey findings may reflect that the Russian government's efforts to combat commercial corruption are perceived to be having an effect. In addition, given the amount of discussion there has been regarding this topic in the Russian business community, the survey results may also indicate a certain level of "corruption fatigue," in which respondents no longer see this as a new and salient issue.

It is also notable that respondents in Russia were far less likely than those anywhere else to report being victims of **adversarial social media activity** (9 percent vs. 27 percent globally). Russia is not without online concerns, however: Respondents there are more likely than those anywhere else to report that they never use **brand influencers** (41 percent vs. 22 percent globally).

Respondents in Russia are consistently skeptical of the effectiveness of their internal **detection mechanisms**. For example, they are less likely than average to consider their **compliance programs** effective in detecting incidents (66 percent vs. 75 percent globally). Accordingly, respondents give below-average marks to their organizations' culture of **transparency and accountability**. Only 66 percent of respondents in Russia say their **due diligence of third parties** is effective (vs. 73 percent globally). Responses from Russia also indicate that companies are less likely than average to conduct reputational due diligence—an increasingly important part of the due diligence process—on **suppliers and customers**. Even more notably, they are far less likely to perform reputational due diligence on **candidates for board director seats and senior executive positions** (77 percent vs. 91 percent globally). Although only 53 percent of Russian organizations call their **whistleblowing programs** effective (vs. 66 percent globally), incidents in Russia are detected by whistleblowers at an above-average rate (17 percent vs. 13 percent globally).

As in most other countries, **employees** were the most common source of threats (30 percent vs. 24 percent globally). But in Russia, **competitors** were the second most frequently cited perpetrator (21 percent vs. 14 percent globally). This may reflect some companies' aggressive use of lawsuits, complaints to authorities and other tactics to derail rivals.

Looking ahead, Russian respondents are no more likely than their international peers to express concern about most emerging threats—and are often significantly less likely to do so. However, Russians worry about the possibility of **large-scale, coordinated cyberattacks** at a far higher rate than respondents almost anywhere else (75 percent vs. 68 percent globally).

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	41%	39%	▲ 2%
Fraud by external parties	28%	28%	■ 0%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	25%	27%	▼ -2%
IP theft (e.g., trade secrets)	25%	24%	▲ 1%
Counterfeiting or gray market activity	19%	17%	▲ 2%
Reputational damage due to third-party relationship	16%	29%	▼ -13%
Data theft (e.g., customer records)	16%	29%	▼ -13%
Money laundering	16%	16%	■ 0%
Bribery and corruption	16%	23%	▼ -7%
Fraud by internal parties	13%	27%	▼ -14%
Adversarial social media activity	9%	27%	▼ -18%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	50%	54%	▼ -4%
Newly imposed sanctions against doing business with a government, entity or person	47%	47%	■ 0%
Political unrest	44%	49%	▼ -5%
Changes in economic treaties between countries	41%	51%	▼ -10%
Government influence on a vendor, partner, customer or other entity with which your company does business	34%	51%	▼ -17%
Restrictions on foreign investment	31%	47%	▼ -16%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Reputational damage due to third-party relationship	84%	73%	▲ 11%
Data theft (e.g., customer records)	84%	76%	▲ 8%
IP theft (e.g., trade secrets)	78%	72%	▲ 6%
Leaks of internal information	72%	73%	▼ -1%
Adversarial social media activity	66%	63%	▲ 3%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	63%	62%	▲ 1%
Bribery and corruption	63%	62%	▲ 1%
Fraud by internal parties	59%	66%	▼ -7%
Fraud by external parties	59%	68%	▼ -9%
Counterfeiting or gray market activity	56%	58%	▼ -2%
Money laundering	56%	62%	▼ -6%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Large-scale, coordinated cyberattacks	75%	68%	▲ 7%
A significant financial crisis	72%	69%	▲ 3%
Political instability	63%	63%	■ 0%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	59%	61%	▼ -2%
Military conflict	56%	51%	▲ 5%
Market manipulation through fake news	56%	59%	▼ -3%
Destabilization of fiat currency due to cryptocurrency	53%	53%	■ 0%
Climate change	44%	54%	▼ -10%
Disruptions caused by artificial intelligence or other technologies	41%	56%	▼ -15%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	25%	28%	▼ -3%
External audit	21%	17%	▲ 4%
By management at our company	18%	16%	▲ 2%
Whistleblower	17%	13%	▲ 4%
Customers/suppliers	11%	13%	▼ -2%
Regulator/law enforcement	7%	13%	▼ -6%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	88%	81%	▲ 7%
Data analytics	78%	77%	▲ 1%
Anti-money laundering controls	75%	69%	▲ 6%
Due diligence of third-party reputation and practices	66%	73%	▼ -7%
Compliance (regulatory, codes of conduct, etc.)	66%	75%	▼ -9%
Monitoring social media for adversarial activity	63%	71%	▼ -8%
Anti-bribery and anti-corruption controls	63%	69%	▼ -6%
Whistleblowing	53%	66%	▼ -13%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

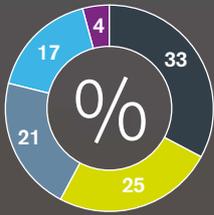
Business partners	93%	92%	▲ 1%
Brand ambassadors/influencers	90%	85%	▲ 5%
Potential M&A targets	90%	89%	▲ 1%
Suppliers	88%	92%	▼ -4%
Customers	84%	88%	▼ -4%
Investors	83%	84%	▼ -1%
Board or senior executive candidates	77%	91%	▼ -14%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	75%	78%	▼ -3%
The company responds to risk management incidents in a consistent way.	75%	75%	■ 0%
Performance goals and incentives do not conflict with risk management practices.	72%	71%	▲ 1%
New business initiatives are regularly examined for all appropriate risk implications.	72%	74%	▼ -2%
Serious breaches of risk management processes are met with thorough internal investigations.	69%	75%	▼ -6%
Risk management programs are designed with input from those who must conform to them.	69%	74%	▼ -5%
Employees view risk management processes as being effective.	69%	76%	▼ -7%
Our risk management processes are adapted to local market and cultural nuances.	63%	72%	▼ -9%

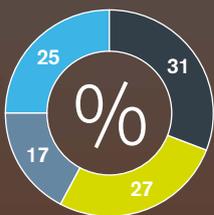


USE OF BRAND "INFLUENCERS"



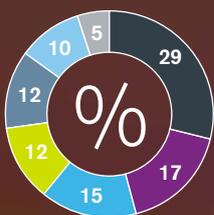
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Competitors
- Contractors
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Politically motivated actors
- Unknown/random actor

Sub-Saharan Africa

As in the Middle East, the risk profile of organizations in sub-Saharan Africa is dominated by **bribery and corruption**, reported by 33 percent of the region's respondents (vs. 23 percent globally), and **fraud**, with 44 percent reporting fraud by internal parties (vs. 27 percent globally). Not surprisingly, **employees** are more likely than average to be the source of incidents (29 percent vs. 24 percent globally). The region also reports a greater percentage of incidents (10 percent vs. 6 percent globally) caused by **politically motivated actors**, a group that includes government officials.

To meet these challenges, organizations in the area will have to realign their **risk priorities**. The 67 percent that prioritize combating fraud by internal parties is not materially higher than the global average (66 percent); fighting bribery and corruption is at the bottom of the mitigation list, with 56 percent making it a priority (vs. 62 percent globally). Further, organizations in sub-Saharan Africa place their greatest priority on **mitigating disruption due to sanctions, tariffs, and changes in trade agreements**, despite their lower overall likelihood of being affected by geopolitical risks.

Many organizations in the region have recently placed a greater emphasis on establishing a **culture of transparency and accountability** as part of their ongoing integration into global trade and investment. These developments are reflected in organizations' level of confidence in key cultural practices. For example, 87 percent of respondents in sub-Saharan Africa agree that there is a **clear message from the top of their organizations** that integrity, compliance and accountability are important (vs. 78 percent globally). These findings, together with those revealing high levels of bribery and corruption and of fraud by internal parties, suggest that the region is in a period of transition regarding these risks and that further progress is warranted.

Organizations in sub-Saharan Africa report practicing **reputational due diligence** with an above-average frequency for many categories of third parties, including **investors**: 93 percent conduct due diligence on this group (vs. 84 percent globally). However, the region lags in performing reputational due diligence on **customers** (75 percent vs. 88 percent globally).

A regional economy that is focused on natural resources and still in the process of developing infrastructure makes sub-Saharan Africa particularly vulnerable to risk from **climate change**; respondents there are more likely than those anywhere else to report concern over the future impact of this threat (67 percent vs. 54 percent globally). And while parts of sub-Saharan Africa have become more **politically stable** of late, the risk of unrest still looms large: Three-quarters of respondents in the region named that as a concern, a higher percentage than nearly anywhere else (vs. 63 percent globally).

The high percentage of Africans without access to financial institutions suggests that the region could be receptive to **cryptocurrency**. So far, however, regulators' concern about fraud and other risks has slowed the platform's adoption, with nearly one-third of respondents in the region (31 percent) reporting that their organizations have no plans to adopt cryptocurrency (vs. 19 percent globally).

RISK LANDSCAPE

ISSUE	REGION	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	46%	39%	▲ 7%
Fraud by internal parties	44%	27%	▲ 17%
Adversarial social media activity	35%	27%	▲ 8%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	33%	27%	▲ 6%
Bribery and corruption	33%	23%	▲ 10%
Reputational damage due to third-party relationship	29%	29%	■ 0%
Fraud by external parties	29%	28%	▲ 1%
IP theft (e.g., trade secrets)	21%	24%	▼ -3%
Data theft (e.g., customer records)	21%	29%	▼ -8%
Counterfeiting or gray market activity	21%	17%	▲ 4%
Money laundering	21%	16%	▲ 5%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Political unrest	52%	49%	▲ 3%
Government influence on a vendor, partner, customer or other entity with which your company does business	50%	51%	▼ -1%
New tariffs or trade wars	44%	54%	▼ -10%
Changes in economic treaties between countries	44%	51%	▼ -7%
Restrictions on foreign investment	42%	47%	▼ -5%
Newly imposed sanctions against doing business with a government, entity or person	37%	47%	▼ -10%

RISK STRATEGY

ISSUE	REGION	GLOBAL	(+/-)
-------	--------	--------	-------

WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?

(Percent responding "significant priority" or "high priority")

Disruption due to sanctions, tariffs, changes in trade agreements, etc.	73%	62%	▲ 11%
Data theft (e.g., customer records)	73%	76%	▼ -3%
IP theft (e.g., trade secrets)	71%	72%	▼ -1%
Fraud by internal parties	67%	66%	▲ 1%
Reputational damage due to third-party relationship	67%	73%	▼ -6%
Money laundering	63%	62%	▲ 1%
Leaks of internal information	62%	73%	▼ -11%
Fraud by external parties	62%	68%	▼ -6%
Adversarial social media activity	60%	63%	▼ -3%
Counterfeiting or gray market activity	56%	58%	▼ -2%
Bribery and corruption	56%	62%	▼ -6%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Political instability	75%	63%	▲ 12%
A significant financial crisis	71%	69%	▲ 2%
Large-scale, coordinated cyberattacks	67%	68%	▼ -1%
Climate change	67%	54%	▲ 13%
Market manipulation through fake news	58%	59%	▼ -1%
Disruptions caused by artificial intelligence or other technologies	58%	56%	▲ 2%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	56%	61%	▼ -5%
Military conflict	52%	51%	▲ 1%
Destabilization of fiat currency due to cryptocurrency	46%	53%	▼ -7%

RISK MANAGEMENT IN PRACTICE

ISSUE	REGION	GLOBAL	(+/-)
-------	--------	--------	-------

HOW WERE INCIDENTS DISCOVERED?

Internal audit	27%	28%	▼ -1%
By management at our company	25%	16%	▲ 9%
Customers/suppliers	16%	13%	▲ 3%
Whistleblower	12%	13%	▼ -1%
Regulator/law enforcement	12%	13%	▼ -1%
External audit	9%	17%	▼ -8%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Data analytics	81%	77%	▲ 4%
Compliance (regulatory, codes of conduct, etc.)	79%	75%	▲ 4%
Cybersecurity	77%	81%	▼ -4%
Due diligence of third-party reputation and practices	75%	73%	▲ 2%
Monitoring social media for adversarial activity	73%	71%	▲ 2%
Anti-bribery and anti-corruption controls	69%	69%	■ 0%
Whistleblowing	67%	66%	▲ 1%
Anti-money laundering controls	67%	69%	▼ -2%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

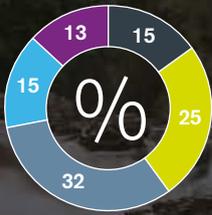
Board or senior executive candidates	96%	91%	▲ 5%
Business partners	94%	92%	▲ 2%
Suppliers	94%	92%	▲ 2%
Investors	93%	84%	▲ 9%
Potential M&A targets	86%	89%	▼ -3%
Brand ambassadors/influencers	80%	85%	▼ -5%
Customers	75%	88%	▼ -13%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	87%	78%	▲ 9%
New business initiatives are regularly examined for all appropriate risk implications.	85%	74%	▲ 11%
Serious breaches of risk management processes are met with thorough internal investigations.	83%	75%	▲ 8%
The company responds to risk management incidents in a consistent way.	83%	75%	▲ 8%
Employees view risk management processes as being effective.	79%	76%	▲ 3%
Our risk management processes are adapted to local market and cultural nuances.	75%	72%	▲ 3%
Performance goals and incentives do not conflict with risk management practices.	71%	71%	■ 0%
Risk management programs are designed with input from those who must conform to them.	71%	74%	▼ -3%

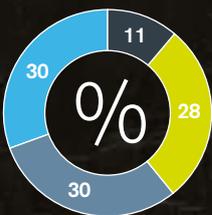


USE OF BRAND "INFLUENCERS"



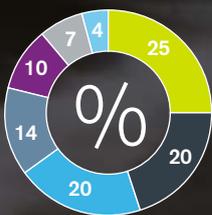
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Third parties (e.g., joint venture partners, suppliers/vendors)
- Employees
- Contractors
- Customers
- Competitors
- Unknown/random actor
- Politically motivated actors

United Kingdom

A salient feature of today's risk landscape is the variety of risks that can emanate from business networks. Respondents in the United Kingdom are acutely aware of this type of threat, with 42 percent—a larger share than in any other country—having suffered **reputational damage due to third-party relationships** (vs. 29 percent globally). Similarly, UK respondents are more likely than average to hold third parties, such as business partners and suppliers, responsible for incidents generally (25 percent vs. 19 percent globally). To that end, UK respondents are more likely than average to practice **reputational due diligence** on the full range of stakeholders, from board candidates (98 percent vs. 91 percent globally) to social media influencers (89 percent vs. 85 percent globally).

UK organizations have also been hard-hit by **internal fraud**; with 38 percent of its organizations so reporting, the United Kingdom trails only sub-Saharan Africa (44 percent). As UK organizations seek to address this issue, they may wish to examine the extent to which their **company culture** reinforces transparency and accountability. For several corporate behaviors that support such a culture, UK responses are in line with global averages, but they reveal a lag in two key areas: Only 70 percent agree there is a **clear message from the top of their organizations** that integrity, compliance and accountability are important (vs. 78 percent globally), and the same percentage says that **employees view risk management processes as being effective** (vs. 76 percent globally). That 20 percent of incidents were reported by whistleblowers—a rate 7 percentage points higher than the global average—may also necessitate more work on reinforcing key cultural norms, as whistleblowing often reflects low confidence in traditional remediation channels.

Geopolitical tensions are high on the agenda, with 60 percent of UK respondents reporting that they have been affected by **changes in economic treaties between countries** (vs. 51 percent globally). Looking ahead to future risks, UK respondents are likely to be concerned about a **breakdown of intergovernmental mechanisms for dispute resolution, free trade and combating corruption** (60 percent, in line with the global average), but they are even more likely to be concerned about disruptions caused by **artificial intelligence or other technologies** (68 percent vs. 56 percent globally). These respondents may be highly aware of AI's possibilities—for good or ill—due to the UK government's recent push to strengthen the country's AI capabilities.

UK organizations have widely adopted **social media influencers**: A mere 15 percent of respondents report their organizations never use them (vs. 22 percent globally). Current discussions about disclosing payments to influencers may have an impact on this trend. UK respondents are similarly amenable to **cryptocurrency**, with only 11 percent of surveyed firms saying they have no plans to use digital assets (vs. 19 percent globally).

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Reputational damage due to third-party relationship	42%	29%	▲ 13%
Leaks of internal information	38%	39%	▼ -1%
Fraud by internal parties	38%	27%	▲ 11%
Adversarial social media activity	32%	27%	▲ 5%
Data theft (e.g., customer records)	32%	29%	▲ 3%
Fraud by external parties	32%	28%	▲ 4%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	30%	27%	▲ 3%
IP theft (e.g., trade secrets)	26%	24%	▲ 2%
Bribery and corruption	26%	23%	▲ 3%
Counterfeiting or gray market activity	23%	17%	▲ 6%
Money laundering	17%	16%	▲ 1%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Changes in economic treaties between countries	60%	51%	▲ 9%
Government influence on a vendor, partner, customer or other entity with which your company does business	55%	51%	▲ 4%
New tariffs or trade wars	49%	54%	▼ -5%
Newly imposed sanctions against doing business with a government, entity or person	49%	47%	▲ 2%
Political unrest	47%	49%	▼ -2%
Restrictions on foreign investment	45%	47%	▼ -2%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Data theft (e.g., customer records)	77%	76%	▲ 1%
Reputational damage due to third-party relationship	75%	73%	▲ 2%
Leaks of internal information	70%	73%	▼ -3%
Adversarial social media activity	64%	63%	▲ 1%
Bribery and corruption	64%	62%	▲ 2%
Fraud by internal parties	62%	66%	▼ -4%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	62%	62%	■ 0%
IP theft (e.g., trade secrets)	62%	72%	▼ -10%
Fraud by external parties	62%	68%	▼ -6%
Money laundering	58%	62%	▼ -4%
Counterfeiting or gray market activity	51%	58%	▼ -7%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Disruptions caused by artificial intelligence or other technologies	68%	56%	▲ 12%
Large-scale, coordinated cyberattacks	66%	68%	▼ -2%
Political instability	64%	63%	▲ 1%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	60%	61%	▼ -1%
A significant financial crisis	60%	69%	▼ -9%
Destabilization of fiat currency due to cryptocurrency	57%	53%	▲ 4%
Climate change	57%	54%	▲ 3%
Market manipulation through fake news	47%	59%	▼ -12%
Military conflict	45%	51%	▼ -6%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	28%	28%	■ 0%
Whistleblower	20%	13%	▲ 7%
External audit	19%	17%	▲ 2%
Customers/suppliers	15%	13%	▲ 2%
Regulator/law enforcement	11%	13%	▼ -2%
By management at our company	8%	16%	▼ -8%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	77%	81%	▼ -4%
Data analytics	75%	77%	▼ -2%
Compliance (regulatory, codes of conduct, etc.)	75%	75%	■ 0%
Due diligence of third-party reputation and practices	74%	73%	▲ 1%
Monitoring social media for adversarial activity	72%	71%	▲ 1%
Anti-money laundering controls	64%	69%	▼ -5%
Anti-bribery and anti-corruption controls	64%	69%	▼ -5%
Whistleblowing	62%	66%	▼ -4%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

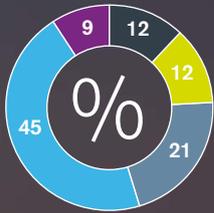
Board or senior executive candidates	98%	91%	▲ 7%
Suppliers	96%	92%	▲ 4%
Business partners	96%	92%	▲ 4%
Potential M&A targets	94%	89%	▲ 5%
Investors	92%	84%	▲ 8%
Customers	91%	88%	▲ 3%
Brand ambassadors/influencers	89%	85%	▲ 4%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

The company responds to risk management incidents in a consistent way.	77%	75%	▲ 2%
Risk management programs are designed with input from those who must conform to them.	75%	74%	▲ 1%
New business initiatives are regularly examined for all appropriate risk implications.	74%	74%	■ 0%
Performance goals and incentives do not conflict with risk management practices.	74%	71%	▲ 3%
Serious breaches of risk management processes are met with thorough internal investigations.	72%	75%	▼ -3%
Our risk management processes are adapted to local market and cultural nuances.	72%	72%	■ 0%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	70%	78%	▼ -8%
Employees view risk management processes as being effective.	70%	76%	▼ -6%

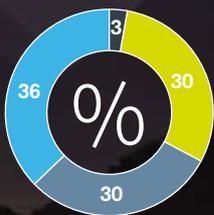


USE OF BRAND "INFLUENCERS"



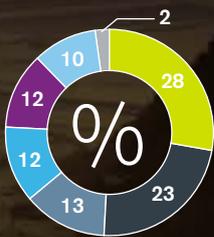
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Third parties (e.g., joint venture partners, suppliers/vendors)
- Employees
- Customers
- Contractors
- Competitors
- Politically motivated actors
- Unknown/random actor

China

China's emergence as a critical link in the global value chain has made organizations there prime targets for a variety of threats. A higher percentage of respondents in China than anywhere else have experienced **IP theft** in the past year (48 percent vs. 24 percent globally). An equal share have suffered **leaks of internal information** (vs. 39 percent globally), while 39 percent have been victims of **data theft** (vs. 29 percent globally). This threat profile has naturally informed the **risk management priorities** of China's organizations. Combating IP theft is an almost universal priority in China, named as such by 94 percent of its respondents (vs. 72 percent globally); leaks of internal information (88 percent vs. 73 percent globally) also get significant attention, although Chinese respondents are less likely than average to prioritize mitigating the risk of data theft (70 percent vs. 76 percent globally).

Chinese organizations report a comparatively lower level of **fraud by internal parties** (18 percent vs. 27 percent globally) and by **external parties** (18 percent vs. 28 percent globally). However, based on the problems we are asked to solve for our clients in China, our observation is that fraud is a significant issue. This variance could be due to the fact that fraud often goes undetected for significant periods of time. Several survey findings support the assessment that Chinese organizations could take stronger anti-fraud measures. For example, respondents in China express less-than-average confidence in the detection capabilities of their **compliance mechanisms** (70 percent vs. 75 percent globally), and **management** in China plays a much smaller role in **detecting incidents** than does management in other countries (5 percent vs. 16 percent globally).

A larger percentage of incidents in China than anywhere else are attributed to third parties such as **business partners and suppliers** (28 percent vs. 19 percent globally). A desire to mitigate this risk may explain why nearly all respondents in China report conducting reputational due diligence on their business partners (96 percent vs. 92 percent globally).

Geopolitical issues loom large in the Chinese risk landscape. Organizations in China are more likely than those elsewhere to report having been significantly affected by many types of geopolitical risk, including **tariffs, changes in economic treaties, political unrest** and **restrictions on foreign investment**. Accordingly, Chinese companies prioritize mitigating the risk of **disruption due to sanctions, tariffs and trade agreements** more widely than do enterprises in any other country or region (85 percent vs. 62 percent globally).

A greater share of organizations in China than anywhere else say they use **brand ambassadors** or social media **influencers** frequently or always (54 percent vs. 32 percent globally). But the use of social media in China, as elsewhere, is a double-edged sword: A significantly higher percentage of companies in China than elsewhere report experiencing **adversarial social media activity** (39 percent vs. 27 percent globally).

China's **cryptocurrency** environment is highly dynamic, with government regulators seeking to rein in high levels of digital asset activity. Despite the many unresolved issues, however, respondents in China are among the least likely to report that their organizations have ruled out using cryptocurrency (3 percent vs. 19 percent globally).

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	48%	39%	▲ 9%
IP theft (e.g., trade secrets)	48%	24%	▲ 24%
Adversarial social media activity	39%	27%	▲ 12%
Data theft (e.g., customer records)	39%	29%	▲ 10%
Reputational damage due to third-party relationship	30%	29%	▲ 1%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	24%	27%	▼ -3%
Counterfeiting or gray market activity	21%	17%	▲ 4%
Fraud by internal parties	18%	27%	▼ -9%
Fraud by external parties	18%	28%	▼ -10%
Bribery and corruption	18%	23%	▼ -5%
Money laundering	12%	16%	▼ -4%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	76%	54%	▲ 22%
Restrictions on foreign investment	70%	47%	▲ 23%
Changes in economic treaties between countries	67%	51%	▲ 16%
Political unrest	64%	49%	▲ 15%
Newly imposed sanctions against doing business with a government, entity or person	61%	47%	▲ 14%
Government influence on a vendor, partner, customer or other entity with which your company does business	61%	51%	▲ 10%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
IP theft (e.g., trade secrets)	94%	72%	▲ 22%
Leaks of internal information	88%	73%	▲ 15%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	85%	62%	▲ 23%
Money laundering	76%	62%	▲ 14%
Bribery and corruption	76%	62%	▲ 14%
Reputational damage due to third-party relationship	73%	73%	■ 0%
Data theft (e.g., customer records)	70%	76%	▼ -6%
Counterfeiting or gray market activity	70%	58%	▲ 12%
Fraud by internal parties	61%	66%	▼ -5%
Fraud by external parties	58%	68%	▼ -10%
Adversarial social media activity	55%	63%	▼ -8%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Destabilization of fiat currency due to cryptocurrency	85%	53%	▲ 32%
A significant financial crisis	82%	69%	▲ 13%
Large-scale, coordinated cyberattacks	67%	68%	▼ -1%
Military conflict	67%	51%	▲ 16%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	67%	61%	▲ 6%
Disruptions caused by artificial intelligence or other technologies	61%	56%	▲ 5%
Political instability	61%	63%	▼ -2%
Market manipulation through fake news	55%	59%	▼ -4%
Climate change	42%	54%	▼ -12%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	30%	28%	▼ 2%
External audit	17%	17%	■ 0%
Whistleblower	16%	13%	▲ 3%
Customers/suppliers	16%	13%	▲ 3%
Regulator/law enforcement	15%	13%	▲ 2%
By management at our company	5%	16%	▼ -11%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	85%	81%	▲ 4%
Data analytics	82%	77%	▲ 5%
Anti-money laundering controls	79%	69%	▲ 10%
Due diligence of third-party reputation and practices	76%	73%	▲ 3%
Monitoring social media for adversarial activity	70%	71%	▼ -1%
Anti-bribery and anti-corruption controls	70%	69%	▲ 1%
Compliance (regulatory, codes of conduct, etc.)	70%	75%	▼ -5%
Whistleblowing	70%	66%	▲ 4%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

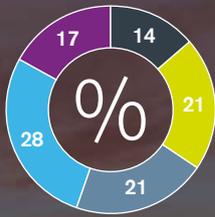
Board or senior executive candidates	97%	91%	▲ 6%
Business partners	96%	92%	▲ 4%
Suppliers	94%	92%	▲ 2%
Customers	94%	88%	▲ 6%
Brand ambassadors/influencers	90%	85%	▲ 5%
Potential M&A targets	87%	89%	▼ -2%
Investors	81%	84%	▼ -3%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

The company responds to risk management incidents in a consistent way.	82%	75%	▲ 7%
Risk management programs are designed with input from those who must conform to them.	82%	74%	▲ 8%
Our risk management processes are adapted to local market and cultural nuances.	79%	72%	▲ 7%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	76%	78%	▼ -2%
Serious breaches of risk management processes are met with thorough internal investigations.	76%	75%	▲ 1%
New business initiatives are regularly examined for all appropriate risk implications.	73%	74%	▼ -1%
Employees view risk management processes as being effective.	73%	76%	▼ -3%
Performance goals and incentives do not conflict with risk management practices.	70%	71%	▼ -1%

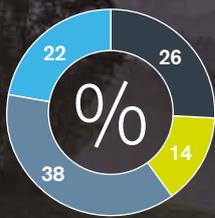


USE OF BRAND "INFLUENCERS"



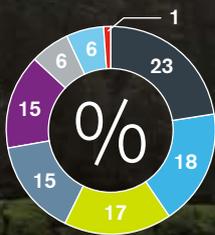
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Contractors
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Competitors
- Unknown/random actor
- Politically motivated actors
- Don't know/does not apply

India

India's role as a global IT hub, its geopolitical importance and its vast population of digital users serve to amplify the attention paid to many forms of risk there. India's corporate leaders, for example, are much more likely than respondents in other countries to prioritize the prevention of **counterfeiting** (76 percent vs. 58 percent globally) and are among the most likely to fight **money laundering** (78 percent vs. 62 percent globally). They are also acutely concerned about **adversarial social media** (81 percent vs. 63 percent globally), an apprehension that undoubtedly grew during the heated national election campaign of May 2019, in which social media played a sizable part. At the same time, a large share of respondents in India give high marks to the detection capabilities of their **social media monitoring** (84 percent vs. 71 percent globally).

The frequency of threats actually experienced by Indian organizations is broadly in line with global averages—with one notable exception: Significant **data theft** has affected 41 percent of Indian companies in the past year (vs. 29 percent globally). The country has recently been the setting for numerous high-profile data incidents, increasing organizations' awareness of and emphasis on **cybersecurity**. This may be one reason respondents in India are more likely than the global average to say that their cybersecurity systems are effective (88 percent vs. 81 percent globally).

Whistleblowing reports are on the rise in India, perhaps helped by the role of whistleblowers in bringing to light recent well-publicized corporate fraud events and by the expectation of stronger legislative protections. While respondents in India assess their whistleblowing detection mechanisms as effective or very effective significantly more often than the global average (78 percent vs. 66 percent globally), continued employee training on whistleblowing procedures and protections is needed, as potential whistleblowers can be deterred by uncertainty and fear of repercussions.

The vigorous debate in India over **cryptocurrency** may be one reason why 26 percent of respondents (vs. 19 percent globally) say they have no plans to use this new financial platform.

With China to the country's north and Pakistan to its west, India's **geopolitical risks** are very much on the minds of its corporate leaders. Indian organizations are more likely than average to report having been affected by **tariffs or trade wars** (71 percent vs. 54 percent globally), **restrictions on foreign investment** (62 percent vs. 47 percent globally) or **newly imposed sanctions** (66 percent vs. 47 percent globally).

In line with the high sensitivity of respondents in India to current threats, those respondents are also more keenly focused on risks that may occur in five years' time. A much larger percentage of respondents in India than anywhere else worry about **market manipulation through fake news** (76 percent vs. 59 percent globally); respondents there also evince more concern than those elsewhere about **military conflict** (69 percent vs. 51 percent globally), and have a high level of concern over a **breakdown of intergovernmental mechanisms for dispute resolution** (71 percent vs. 61 percent globally).

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Data theft (e.g., customer records)	41%	29%	▲ 12%
Leaks of internal information	40%	39%	▲ 1%
Reputational damage due to third-party relationship	33%	29%	▲ 4%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	33%	27%	▲ 6%
Fraud by internal parties	33%	27%	▲ 6%
Fraud by external parties	31%	28%	▲ 3%
Adversarial social media activity	29%	27%	▲ 2%
IP theft (e.g., trade secrets)	29%	24%	▲ 5%
Bribery and corruption	29%	23%	▲ 6%
Counterfeiting or gray market activity	16%	17%	▼ -1%
Money laundering	16%	16%	■ 0%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	71%	54%	▲ 17%
Government influence on a vendor, partner, customer or other entity with which your company does business	69%	51%	▲ 18%
Newly imposed sanctions against doing business with a government, entity or person	66%	47%	▲ 19%
Changes in economic treaties between countries	66%	51%	▲ 15%
Restrictions on foreign investment	62%	47%	▲ 15%
Political unrest	45%	49%	▼ -4%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
-------	---------	--------	-------

WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?

(Percent responding "significant priority" or "high priority")

Data theft (e.g., customer records)	84%	76%	▲ 8%
Reputational damage due to third-party relationship	81%	73%	▲ 8%
Adversarial social media activity	81%	63%	▲ 18%
IP theft (e.g., trade secrets)	79%	72%	▲ 7%
Money laundering	78%	62%	▲ 16%
Leaks of internal information	76%	73%	▲ 3%
Counterfeiting or gray market activity	76%	58%	▲ 18%
Fraud by external parties	76%	68%	▲ 8%
Fraud by internal parties	76%	66%	▲ 10%
Bribery and corruption	67%	62%	▲ 5%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	64%	62%	▲ 2%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A significant financial crisis	81%	69%	▲ 12%
Market manipulation through fake news	76%	59%	▲ 17%
Large-scale, coordinated cyberattacks	74%	68%	▲ 6%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	71%	61%	▲ 10%
Military conflict	69%	51%	▲ 18%
Climate change	66%	54%	▲ 12%
Disruptions caused by artificial intelligence or other technologies	66%	56%	▲ 10%
Political instability	62%	63%	▼ -1%
Destabilization of fiat currency due to cryptocurrency	62%	53%	▲ 9%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
-------	---------	--------	-------

HOW WERE INCIDENTS DISCOVERED?

Internal audit	21%	28%	▼ -7%
External audit	18%	17%	▲ 1%
Customers/suppliers	15%	13%	▲ 2%
By management at our company	15%	16%	▼ -1%
Whistleblower	15%	13%	▲ 2%
Regulator/law enforcement	15%	13%	▲ 2%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	88%	81%	▲ 7%
Data analytics	86%	77%	▲ 9%
Monitoring social media for adversarial activity	84%	71%	▲ 13%
Anti-money laundering controls	78%	69%	▲ 9%
Anti-bribery and anti-corruption controls	78%	69%	▲ 9%
Whistleblowing	78%	66%	▲ 12%
Compliance (regulatory, codes of conduct, etc.)	74%	75%	▼ -1%
Due diligence of third-party reputation and practices	74%	73%	▲ 1%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

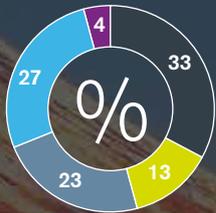
Board or senior executive candidates	95%	91%	▲ 4%
Suppliers	94%	92%	▲ 2%
Business partners	94%	92%	▲ 2%
Customers	87%	88%	▼ -1%
Potential M&A targets	85%	89%	▼ -4%
Investors	81%	84%	▼ -3%
Brand ambassadors/influencers	80%	85%	▼ -5%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	83%	78%	▲ 5%
Employees view risk management processes as being effective.	83%	76%	▲ 7%
The company responds to risk management incidents in a consistent way.	81%	75%	▲ 6%
Serious breaches of risk management processes are met with thorough internal investigations.	78%	75%	▲ 3%
Performance goals and incentives do not conflict with risk management practices.	78%	71%	▲ 7%
New business initiatives are regularly examined for all appropriate risk implications.	76%	74%	▲ 2%
Risk management programs are designed with input from those who must conform to them.	74%	74%	■ 0%
Our risk management processes are adapted to local market and cultural nuances.	72%	72%	■ 0%

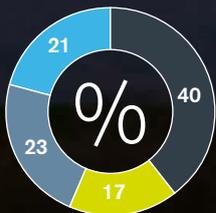


USE OF BRAND "INFLUENCERS"



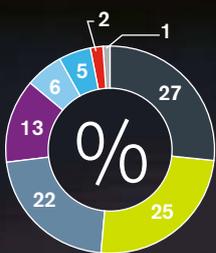
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Competitors
- Politically motivated actors
- Contractors
- Don't know/does not apply
- Unknown/random actor

Japan

In many areas, Japan's survey results depart significantly from global averages. This reflects the extent to which respondents' organizations are grappling with shortcomings in internal controls and in keeping pace with the effects of geopolitical forces on the risk landscape.

As elsewhere, respondents in Japan name **leaks of internal information, reputational damage due to third-party relationships and data theft** as the most common significant incidents in the last 12 months. Other threats, however, occur notably less often in Japan. **Bribery and corruption** are reported by only 13 percent of respondents in Japan (vs. 23 percent globally), as the large-scale reform that took place in the 1990s continues to bear fruit. **Money laundering** is reported by a scant 2 percent of respondents in Japan (vs. 16 percent globally); the extent to which this reflects systemic improvements in Japan's anti-money laundering regulations and controls will be seen after the review this year by the Financial Action Task Force.

Geopolitical issues do not receive the focus in Japan that they do elsewhere. Organizations in Japan are less likely than those in any other country to name **disruptions due to sanctions and tariffs** as a risk priority (38 percent vs. 62 percent globally) and report being less affected by **geopolitical risks** in general. Respondents in Japan are among the least likely to be concerned about the future possibility of a **breakdown of intergovernmental mechanisms for dispute resolution, free trade and combating corruption** (44 percent vs. 61 percent globally).

A series of high-profile scandals involving falsified inspections has led to national introspection regarding business culture, performance pressure and economic turbulence. The effect of these events can be seen at a number of points in the survey data. A notably lower percentage of incidents in Japan were discovered through **internal audit** than elsewhere (20 percent vs. 28 percent globally), with a greater reliance on **regulators** (20 percent vs. 13 percent globally) and **whistleblowers** (17 percent vs. 13 percent globally). In the same vein, respondents in Japan are much less likely to rate their internal detection capabilities, such as **cybersecurity** (56 percent vs. 81 percent globally), **reputational due diligence** (50 percent vs. 73 percent globally) and **data analytics** (50 percent vs. 77 percent globally), as effective or highly effective. Similarly, respondents in Japan are much less likely to agree that their organizations follow many of the practices that promote **transparency and accountability**.

A year ago, Japan stood out in the global arena for its welcoming attitude toward **cryptocurrency**. Multiple thefts at cryptocurrency exchanges, however, have resulted in greater skepticism toward digital financial platforms: The percentage of Japanese organizations reporting that they do not plan to use cryptocurrency is more than double the global average (40 percent vs. 19 percent overall).

Respondents in Japan are notably less likely than those in other countries to be concerned about the array of **future risks** presented in the survey. Interestingly, Japanese respondents are furthest from the global average when considering risks that can be addressed through government intervention, such as **destabilization of fiat currency due to cryptocurrency** (35 percent vs. 53 percent globally) and a **breakdown of intergovernmental dispute resolution** (44 percent vs. 61 percent globally).

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	40%	39%	▲ 1%
Reputational damage due to third-party relationship	29%	29%	■ 0%
Data theft (e.g., customer records)	27%	29%	▼ -2%
Adversarial social media activity	21%	27%	▼ -6%
IP theft (e.g., trade secrets)	21%	24%	▼ -3%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	17%	27%	▼ -10%
Fraud by internal parties	17%	27%	▼ -10%
Fraud by external parties	17%	28%	▼ -11%
Counterfeiting or gray market activity	15%	17%	▼ -2%
Bribery and corruption	13%	23%	▼ -10%
Money laundering	2%	16%	▼ -14%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Political unrest	52%	49%	▲ 3%
Government influence on a vendor, partner, customer or other entity with which your company does business	46%	51%	▼ -5%
New tariffs or trade wars	46%	54%	▼ -8%
Changes in economic treaties between countries	40%	51%	▼ -11%
Newly imposed sanctions against doing business with a government, entity or person	40%	47%	▼ -7%
Restrictions on foreign investment	31%	47%	▼ -16%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Reputational damage due to third-party relationship	73%	73%	■ 0%
Leaks of internal information	73%	73%	■ 0%
IP theft (e.g., trade secrets)	65%	72%	▼ -7%
Data theft (e.g., customer records)	65%	76%	▼ -11%
Fraud by external parties	58%	68%	▼ -10%
Bribery and corruption	58%	62%	▼ -4%
Fraud by internal parties	56%	66%	▼ -10%
Money laundering	52%	62%	▼ -10%
Adversarial social media activity	46%	63%	▼ -17%
Counterfeiting or gray market activity	40%	58%	▼ -18%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	38%	62%	▼ -24%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A significant financial crisis	63%	69%	▼ -6%
Large-scale, coordinated cyberattacks	56%	68%	▼ -12%
Political instability	54%	63%	▼ -9%
Climate change	54%	54%	■ 0%
Market manipulation through fake news	52%	59%	▼ -7%
Disruptions caused by artificial intelligence or other technologies	44%	56%	▼ -12%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	44%	61%	▼ -17%
Military conflict	42%	51%	▼ -9%
Destabilization of fiat currency due to cryptocurrency	35%	53%	▼ -18%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	20%	28%	▼ -8%
Regulator/law enforcement	20%	13%	▲ 7%
Whistleblower	17%	13%	▲ 4%
Customers/suppliers	14%	13%	▲ 1%
External audit	13%	17%	▼ -4%
By management at our company	13%	16%	▼ -3%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Anti-bribery and anti-corruption controls	58%	69%	▼ -11%
Cybersecurity	56%	81%	▼ -25%
Compliance (regulatory, codes of conduct, etc.)	54%	75%	▼ -21%
Monitoring social media for adversarial activity	52%	71%	▼ -19%
Due diligence of third-party reputation and practices	50%	73%	▼ -23%
Data analytics	50%	77%	▼ -27%
Anti-money laundering controls	50%	69%	▼ -19%
Whistleblowing	50%	66%	▼ -16%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

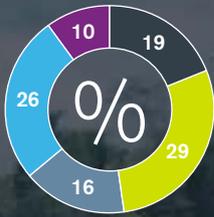
Customers	87%	88%	▼ -1%
Business partners	86%	92%	▼ -6%
Potential M&A targets	81%	89%	▼ -8%
Brand ambassadors/influencers	81%	85%	▼ -4%
Suppliers	79%	92%	▼ -13%
Board or senior executive candidates	76%	91%	▼ -15%
Investors	66%	84%	▼ -18%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

Employees view risk management processes as being effective.	73%	76%	▼ -3%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	69%	78%	▼ -9%
Serious breaches of risk management processes are met with thorough internal investigations.	65%	75%	▼ -10%
Our risk management processes are adapted to local market and cultural nuances.	65%	72%	▼ -7%
Risk management programs are designed with input from those who must conform to them.	63%	74%	▼ -11%
The company responds to risk management incidents in a consistent way.	56%	75%	▼ -19%
New business initiatives are regularly examined for all appropriate risk implications.	56%	74%	▼ -18%
Performance goals and incentives do not conflict with risk management practices.	52%	71%	▼ -19%

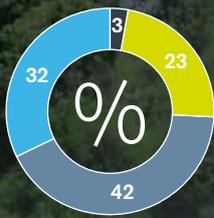


USE OF BRAND "INFLUENCERS"



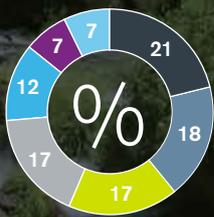
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF THOSE INCIDENTS?



- Employees
- Customers
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Unknown/random actor
- Contractors
- Competitors
- Politically motivated actors

Brazil

Brazil's survey responses reflect the extent to which the country is grappling with a number of broad, systemic challenges. First, fighting **bribery and corruption** has dominated the national conversation in Brazil since the *Lava Jato* scandal broke in 2014. The share of organizations in Brazil that report having experienced bribery and corruption exceeds the global average (29 percent vs. 23 percent overall), and combating this threat is given greater importance in Brazil than in any other country in our survey: 77 percent of respondents in Brazil named it a priority. Bribery and corruption are often accompanied by money laundering, and indeed, **money laundering** incidents occur more frequently in Brazil than in any other country in the survey (23 percent vs. 16 percent globally).

In addition to confronting bribery and corruption, Brazil is in the process of developing an anti-cybercrime regulatory and enforcement infrastructure that matches the size and increasing maturity of its economy. Respondents in Brazil are more likely than participants from any other country in the survey to report **leaks of internal information**, which often occur via computer networks (55 percent vs. 39 percent globally); they also name **data theft** as their top risk priority (84 percent vs. 76 percent globally).

When evaluating the various mechanisms used to detect intrusions, respondents in Brazil express the least confidence in their compliance systems, with only 74 percent finding them effective. The efficacy of **compliance** measures depends greatly on the degree to which a **company's culture** supports transparency and accountability. Respondents in Brazil give their organizations above-average marks for several of these components but indicate that other aspects have room for improvement—perhaps most importantly, the assurance that **performance goals and incentives do not conflict with risk management practices** (65 percent vs. 71 percent globally).

Respondents in Brazil report that they are affected by **geopolitical risks**. Fifty-eight percent of respondents say their organizations have felt the effect of **newly imposed sanctions** against business dealings with a government, entity or person; this percentage is higher in Brazil than it is anywhere else aside from India and China. Sixty-one percent of respondents in Brazil report that their organizations have been affected by **government influence on a vendor, partner or customer** (vs. 51 percent globally).

Like China, Brazil seems ambivalent about **cryptocurrency**. Ninety-seven percent of respondents in Brazil say their organizations are at least investigating cryptocurrency, if not actively using it. Paradoxically, though, when looking five years into the future, 74 percent of respondents in Brazil (vs. 53 percent globally) worry that cryptocurrency could lead to a **destabilization of fiat currency**.

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	55%	39%	▲ 16%
Reputational damage due to third-party relationship	32%	29%	▲ 3%
Bribery and corruption	29%	23%	▲ 6%
Fraud by external parties	23%	28%	▼ -5%
IP theft (e.g., trade secrets)	23%	24%	▼ -1%
Money laundering	23%	16%	▲ 7%
Data theft (e.g., customer records)	19%	29%	▼ -10%
Fraud by internal parties	19%	27%	▼ -11%
Adversarial social media activity	16%	27%	▼ -11%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	16%	27%	▼ -11%
Counterfeiting or gray market activity	10%	17%	▼ -7%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Government influence on a vendor, partner, customer or other entity with which your company does business	61%	51%	▲ 10%
New tariffs or trade wars	58%	54%	▲ 4%
Newly imposed sanctions against doing business with a government, entity or person	58%	47%	▲ 11%
Political unrest	58%	49%	▲ 9%
Changes in economic treaties between countries	52%	51%	▲ 1%
Restrictions on foreign investment	42%	47%	▼ -5%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Data theft (e.g., customer records)	84%	76%	▲ 8%
IP theft (e.g., trade secrets)	81%	72%	▲ 9%
Bribery and corruption	77%	62%	▲ 15%
Reputational damage due to third-party relationship	74%	73%	▲ 1%
Leaks of internal information	71%	73%	▼ -2%
Adversarial social media activity	71%	63%	▲ 8%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	71%	62%	▲ 9%
Fraud by external parties	71%	68%	▲ 3%
Counterfeiting or gray market activity	61%	58%	▲ 3%
Money laundering	61%	62%	▼ -1%
Fraud by internal parties	61%	66%	▼ -5%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Large-scale, coordinated cyberattacks	77%	68%	▲ 9%
A significant financial crisis	74%	69%	▲ 5%
Destabilization of fiat currency due to cryptocurrency	74%	53%	▲ 21%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combatting corruption, etc.	68%	61%	▲ 7%
Market manipulation through fake news	68%	59%	▲ 9%
Military conflict	65%	51%	▲ 14%
Disruptions caused by artificial intelligence or other technologies	61%	56%	▲ 5%
Political instability	61%	63%	▼ -2%
Climate change	58%	54%	▲ 4%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	32%	28%	▲ 4%
By management at our company	21%	16%	▲ 5%
Regulator/law enforcement	18%	13%	▲ 5%
External audit	12%	17%	▼ -5%
Whistleblower	9%	13%	▼ -4%
Customers/suppliers	9%	13%	▼ -4%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	94%	81%	▲ 13%
Due diligence of third-party reputation and practices	87%	73%	▲ 14%
Anti-money laundering controls	84%	69%	▲ 15%
Whistleblowing	84%	66%	▲ 18%
Data analytics	81%	77%	▲ 4%
Monitoring social media for adversarial activity	81%	71%	▲ 10%
Anti-bribery and anti-corruption controls	77%	69%	▲ 8%
Compliance (regulatory, codes of conduct, etc.)	74%	75%	▼ -1%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

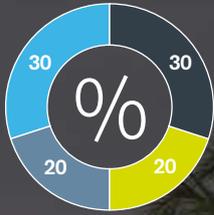
Customers	97%	88%	▲ 9%
Potential M&A targets	96%	89%	▲ 7%
Board or senior executive candidates	93%	91%	▲ 2%
Brand ambassadors/influencers	92%	85%	▲ 7%
Business partners	90%	92%	▼ -2%
Suppliers	86%	92%	▼ -6%
Investors	83%	84%	▼ -1%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	84%	78%	▲ 6%
Employees view risk management processes as being effective.	81%	76%	▲ 5%
The company responds to risk management incidents in a consistent way.	77%	75%	▲ 2%
Serious breaches of risk management processes are met with thorough internal investigations.	74%	75%	▼ -1%
Risk management programs are designed with input from those who must conform to them.	68%	74%	▼ -6%
Performance goals and incentives do not conflict with risk management practices.	65%	71%	▼ -6%
New business initiatives are regularly examined for all appropriate risk implications.	65%	74%	▼ -9%
Our risk management processes are adapted to local market and cultural nuances.	58%	72%	▼ -14%

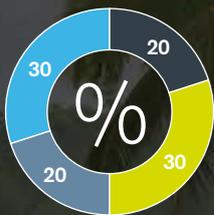


USE OF BRAND "INFLUENCERS"*



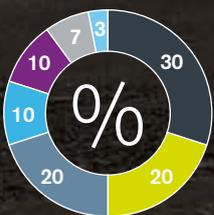
- Never
- Occasionally
- Sometimes
- Frequently

ADOPTION OF CRYPTOCURRENCY*



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?*



- Employees
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Contractors
- Competitors
- Unknown/random actor
- Politically motivated actors
- Politically motivated actors

Colombia

Given the survey's limited number of participants in Colombia, their responses provide only directional guidance on the country's risk profile and its organizations' priorities. Even so, some general insights emerge from the data. The two types of incidents most commonly experienced within the last 12 months are **leaks of internal information** (reported by half of respondents) and **fraud by external parties** (four of ten respondents); the frequency of most other threat incidents was lower (two or three of ten). Among risk priorities, however, the distinctions are more marked. Nine of ten respondents said combating **adversarial social media activity** and guarding against **reputational damage due to third-party relationships** are priorities; only four of ten make it a priority to crack down on **counterfeiting**. Respondents' emphasis on social media may reflect Colombia's steadily growing online population and the widespread use of social media there.

Colombian organizations express a high level of confidence in the ability of their **compliance mechanisms** to detect threats and generally agree that their companies' behavior supports a **culture of integrity**. However, only six of ten respondents report that their **risk management programs are designed with input from those who must comply with them**—an area for possible improvement.

In four of ten cases, the threat incidents experienced by our respondents in Colombia were uncovered by the **internal audit** function, evidently much more important than other detection methods. Colombia does have legislation dictating that internal mechanisms be established to prevent workplace harassment, but there is no formal **whistleblowing** law; survey results bear out the significance of this omission, as only 3 percent of incidents are uncovered through whistleblowing.

Respondents in Colombia have been strongly affected by **geopolitical risks**. Eight of ten, for example, report that **a government has exerted influence on a vendor, business partner or other entity** in a way that altered their organizations' relationship with that third party. Although the high-profile trade conflicts in the headlines have not involved Colombia itself, seven of ten respondents there have been affected by **new tariffs and trade wars**, illustrating how easily enterprises in bystander countries can be disrupted. This issue extends into the future: Six of ten respondents in Colombia expressed concern about **breakdowns of intergovernmental mechanisms** for dispute resolution, free trade, combating corruption and similar issues. Other future risks, however, are of less concern: Only three of ten respondents in Colombia are concerned about the possibility of a **significant financial crisis** five years from now, and only four of ten cite concern over future **political instability**.

The Colombian government has welcomed the use of blockchain-based platforms to help fight corruption. Three of ten respondents now report actively using **cryptocurrency**, and fully half of respondents are either investigating cryptocurrency or have a pilot program underway, ensuring increased adoption in years to come.

* Due to low sample size, percentages are directional only.

RISK LANDSCAPE*

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	50%	39%	▲ 11%
Fraud by external parties	40%	28%	▲ 12%
Reputational damage due to third-party relationship	30%	29%	▲ 1%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	30%	27%	▲ 3%
Counterfeiting or gray market activity	30%	17%	▲ 13%
Fraud by internal parties	30%	27%	▲ 3%
Adversarial social media activity	20%	27%	▼ -7%
IP theft (e.g., trade secrets)	20%	24%	▼ -4%
Data theft (e.g., customer records)	20%	29%	▼ -9%
Bribery and corruption	20%	23%	▼ -3%
Money laundering	10%	16%	▼ -6%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Government influence on a vendor, partner, customer or other entity with which your company does business	80%	51%	▲ 29%
New tariffs or trade wars	70%	54%	▲ 16%
Political unrest	60%	49%	▲ 11%
Restrictions on foreign investment	60%	47%	▲ 13%
Newly imposed sanctions against doing business with a government, entity or person	50%	47%	▲ 3%
Changes in economic treaties between countries	40%	51%	▼ -11%

RISK STRATEGY*

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Adversarial social media activity	90%	63%	▲ 27%
Reputational damage due to third-party relationship	90%	73%	▲ 17%
Leaks of internal information	80%	73%	▲ 7%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	80%	62%	▲ 18%
Fraud by external parties	80%	68%	▲ 12%
IP theft (e.g., trade secrets)	70%	72%	▼ -2%
Fraud by internal parties	70%	66%	▲ 4%
Money laundering	60%	62%	▼ -2%
Data theft (e.g., customer records)	50%	76%	▼ -26%
Bribery and corruption	50%	62%	▼ -12%
Counterfeiting or gray market activity	40%	58%	▼ -18%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Disruptions caused by artificial intelligence or other technologies	60%	56%	▲ 4%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	60%	61%	▼ -1%
Large-scale, coordinated cyberattacks	50%	68%	▼ -18%
Destabilization of fiat currency due to cryptocurrency	50%	53%	▼ -3%
Military conflict	50%	51%	▼ -1%
Market manipulation through fake news	50%	59%	▼ -9%
Climate change	40%	54%	▼ -14%
Political instability	40%	63%	▼ -23%
A significant financial crisis	30%	69%	▼ -39%

RISK MANAGEMENT IN PRACTICE*

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	43%	28%	▲ 15%
Customers/suppliers	17%	13%	▲ 4%
By management at our company	17%	16%	▲ 1%
Regulator/law enforcement	13%	13%	■ 0%
External audit	7%	17%	▼ -10%
Whistleblower	3%	13%	▼ -10%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Compliance (regulatory, codes of conduct, etc.)	90%	75%	▲ 15%
Monitoring social media for adversarial activity	80%	71%	▲ 9%
Anti-money laundering controls	60%	69%	▼ -9%
Cybersecurity	60%	81%	▼ -21%
Due diligence of third-party reputation and practices	60%	73%	▼ -13%
Data analytics	50%	77%	▼ -27%
Anti-bribery and anti-corruption controls	50%	69%	▼ -19%
Whistleblowing	40%	66%	▼ -26%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

Suppliers	100%	92%	▲ 8%
Customers	100%	88%	▲ 12%
Business partners	90%	92%	▼ -2%
Investors	89%	84%	▲ 5%
Board or senior executive candidates	80%	91%	▼ -11%
Potential M&A targets	75%	89%	▼ -14%
Brand ambassadors/influencers	63%	85%	▼ -22%

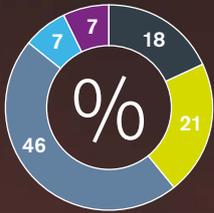
HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	80%	78%	▲ 2%
The company responds to risk management incidents in a consistent way.	80%	75%	▲ 5%
New business initiatives are regularly examined for all appropriate risk implications.	80%	74%	▲ 6%
Serious breaches of risk management processes are met with thorough internal investigations.	70%	75%	▼ -5%
Performance goals and incentives do not conflict with risk management practices.	70%	71%	▼ -1%
Employees view risk management processes as being effective.	70%	76%	▼ -6%
Our risk management processes are adapted to local market and cultural nuances.	70%	72%	▼ -2%
Risk management programs are designed with input from those who must conform to them.	60%	74%	▼ -14%

*Due to low sample size, percentages are directional only.

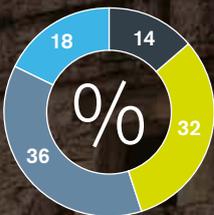


USE OF BRAND "INFLUENCERS"



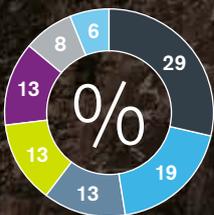
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Contractors
- Customers
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Competitors
- Unknown/random actor
- Politically motivated actors

Mexico

In 2016, the Mexican government integrated **anti-bribery and anti-corruption** frameworks among local, state and national jurisdictions, but it has not as yet aggressively prosecuted corruption allegations. Respondents' organizations in the region have thus taken it upon themselves to increase the effectiveness of their own **anti-bribery and anti-corruption** controls, with 79 percent saying they are efficient or very efficient (vs. 69 percent globally). However, in the wake of high-profile cyberattacks on the national financial system and elsewhere, respondents in Mexico are less confident than most in their **cybersecurity** (68 percent vs. 81 percent globally) and have almost universally prioritized mitigating against **data theft** (89 percent vs. 76 percent globally). Mexican organizations are also still grappling with **monitoring social media for adversarial attacks**, with only half of respondents there calling those detection mechanisms effective or very effective (vs. 71 percent globally).

Respondents in Mexico give their organizations relatively low marks for reinforcing **transparency and accountability**. They are more likely than average to agree or strongly agree that they **adapt their risk management processes to local market and cultural nuances** (82 percent vs. 72 percent globally), but are much less likely to have the same opinion about other key components of company culture, from having the right **message from the top of the organization** (68 percent vs. 78 percent globally) to **responding consistently to risk management incidents** (57 percent vs. 75 percent globally). These results indicate a clear opportunity for Mexican enterprises to improve their risk mitigation measures.

Mexico has recently enacted a new regulatory regime for financial technologies. As part of this initiative, the Bank of Mexico has imposed stricter restrictions on **cryptocurrency** exchanges. Not surprisingly, respondents in Mexico report a somewhat conservative approach to digital assets: Only 18 percent report that their organizations have actively embraced cryptocurrency platforms (vs. 28 percent globally) but an above-average percentage are in the investigation phase (32 percent vs. 22 percent globally).

Looking ahead, respondents in Mexico are less concerned than decision makers elsewhere about many of the **future risks** in our survey. For example, only 46 percent are concerned or very concerned about possible **disruptions due to artificial intelligence** (vs. 56 percent globally). However, the prospects for ongoing stability of **intergovernmental mechanisms** such as free trade agreements and dispute resolution elicit considerable apprehension in Mexico (71 percent vs. 61 percent globally). This unease contrasts sharply with the far lower share (14 percent vs. 27 percent globally) who report having been affected by **disruptions due to tariffs, sanctions and free trade agreements** in the 12 months before the survey was taken in April 2019. The disconnect between recent experience and worries about the future reflects respondents' acute awareness of how quickly conditions have changed in the current geopolitical environment.

RISK LANDSCAPE

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	46%	39%	▲ 7%
Reputational damage due to third-party relationship	32%	29%	▲ 3%
Data theft (e.g., customer records)	32%	29%	▲ 3%
Bribery and corruption	21%	23%	▼ -2%
Money laundering	18%	16%	▲ 2%
Adversarial social media activity	14%	27%	▼ -13%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	14%	27%	▼ -13%
Fraud by internal parties	14%	27%	▼ -13%
Fraud by external parties	14%	28%	▼ -14%
Counterfeiting or gray market activity	11%	17%	▼ -6%
IP theft (e.g., trade secrets)	7%	24%	▼ -17%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	61%	54%	▲ 7%
Changes in economic treaties between countries	61%	51%	▲ 10%
Newly imposed sanctions against doing business with a government, entity or person	50%	47%	▲ 3%
Government influence on a vendor, partner, customer or other entity with which your company does business	50%	51%	▼ -1%
Restrictions on foreign investment	46%	47%	▼ -1%
Political unrest	39%	49%	▼ -10%

RISK STRATEGY

ISSUE	COUNTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
<i>(Percent responding "significant priority" or "high priority")</i>			
Data theft (e.g., customer records)	89%	76%	▲ 13%
Leaks of internal information	75%	73%	▲ 2%
Reputational damage due to third-party relationship	71%	73%	▼ -2%
Bribery and corruption	71%	62%	▲ 9%
Adversarial social media activity	68%	63%	▲ 5%
Fraud by internal parties	68%	66%	▲ 2%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	64%	62%	▲ 2%
Counterfeiting or gray market activity	64%	58%	▲ 6%
IP theft (e.g., trade secrets)	64%	72%	▼ -8%
Fraud by external parties	64%	68%	▼ -4%
Money laundering	61%	62%	▼ -1%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	71%	61%	▲ 10%
Large-scale, coordinated cyberattacks	71%	68%	▲ 3%
A significant financial crisis	68%	69%	▼ -1%
Political instability	61%	63%	▼ -2%
Market manipulation through fake news	54%	59%	▼ -5%
Military conflict	46%	51%	▼ -5%
Disruptions caused by artificial intelligence or other technologies	46%	56%	▼ -10%
Destabilization of fiat currency due to cryptocurrency	46%	53%	▼ -7%
Climate change	46%	54%	▼ -8%

RISK MANAGEMENT IN PRACTICE

ISSUE	COUNTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	30%	28%	▲ 2%
By management at our company	21%	16%	▲ 5%
Regulator/law enforcement	19%	13%	▲ 6%
Customers/suppliers	13%	13%	■ 0%
External audit	10%	17%	▼ -7%
Whistleblower	8%	13%	▼ -5%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Anti-bribery and anti-corruption controls	79%	69%	▲ 10%
Data analytics	79%	77%	▲ 2%
Compliance (regulatory, codes of conduct, etc.)	75%	75%	■ 0%
Anti-money laundering controls	68%	69%	▼ -1%
Cybersecurity	68%	81%	▼ -13%
Due diligence of third-party reputation and practices	64%	73%	▼ -9%
Whistleblowing	57%	66%	▼ -9%
Monitoring social media for adversarial activity	50%	71%	▼ -21%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

Potential M&A targets	100%	89%	▲ 11%
Suppliers	96%	92%	▲ 4%
Investors	96%	84%	▲ 12%
Customers	93%	88%	▲ 5%
Business partners	92%	92%	■ 0%
Board or senior executive candidates	88%	91%	▼ -3%
Brand ambassadors/influencers	87%	85%	▲ 2%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

Our risk management processes are adapted to local market and cultural nuances.	82%	72%	▲ 10%
Performance goals and incentives do not conflict with risk management practices.	75%	71%	▲ 4%
Serious breaches of risk management processes are met with thorough internal investigations.	71%	75%	▼ -4%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	68%	78%	▼ -10%
Risk management programs are designed with input from those who must conform to them.	64%	74%	▼ -10%
Employees view risk management processes as being effective.	61%	76%	▼ -15%
The company responds to risk management incidents in a consistent way.	57%	75%	▼ -18%
New business initiatives are regularly examined for all appropriate risk implications.	57%	74%	▼ -17%

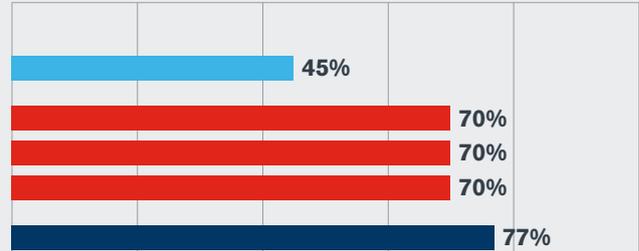
Industry Risk Map

■ Most common incident ■ Top risk priority ■ Top future concern

CONSTRUCTION, ENGINEERING AND INFRASTRUCTURE



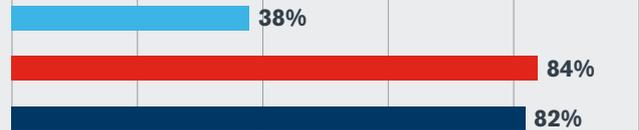
- Leaks of internal information
- Reputational damage due to third-party relationship
- Leaks of internal information
- Bribery and corruption
- A significant financial crisis



CONSUMER GOODS



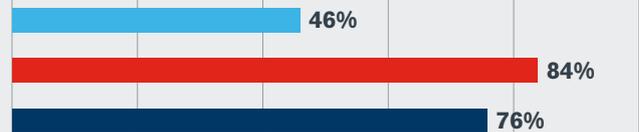
- Leaks of internal information
- Reputational damage due to third-party relationship
- Large-scale, coordinated cyberattacks



EXTRACTIVES



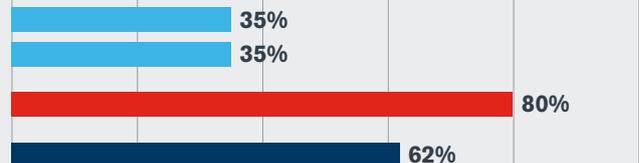
- Leaks of internal information
- IP theft
- A significant financial crisis



FINANCIAL SERVICES



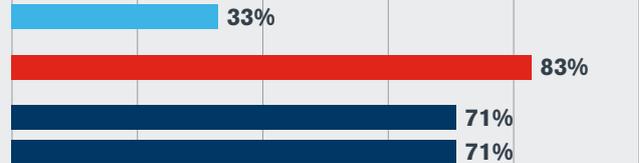
- Adversarial social media activity
- Fraud by external parties
- Leaks of internal information
- Large-scale, coordinated cyberattacks



LIFE SCIENCES

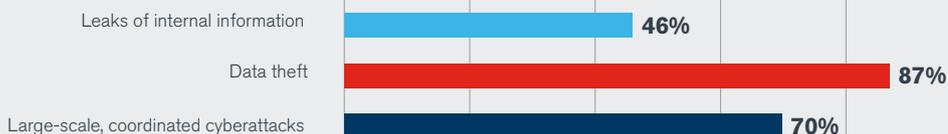


- Leaks of internal information
- Data theft
- Large-scale, coordinated cyberattacks
- A significant financial crisis

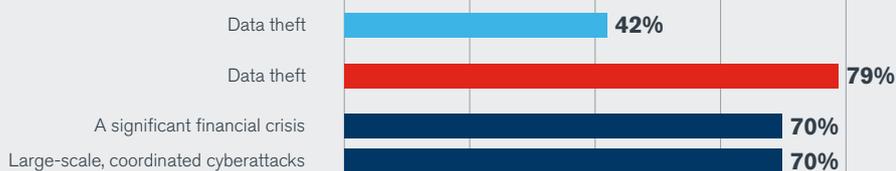


0 100

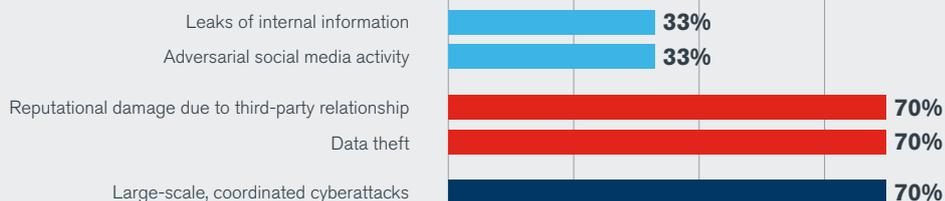
MANUFACTURING



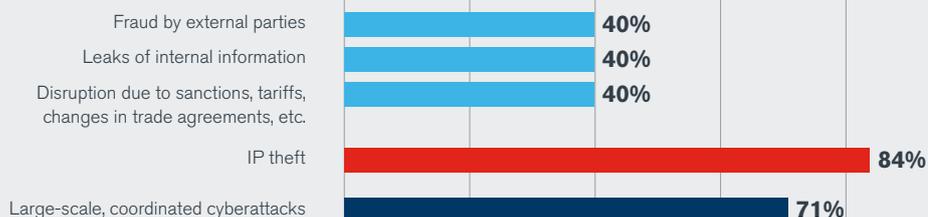
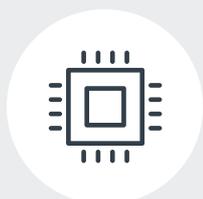
PROFESSIONAL SERVICES



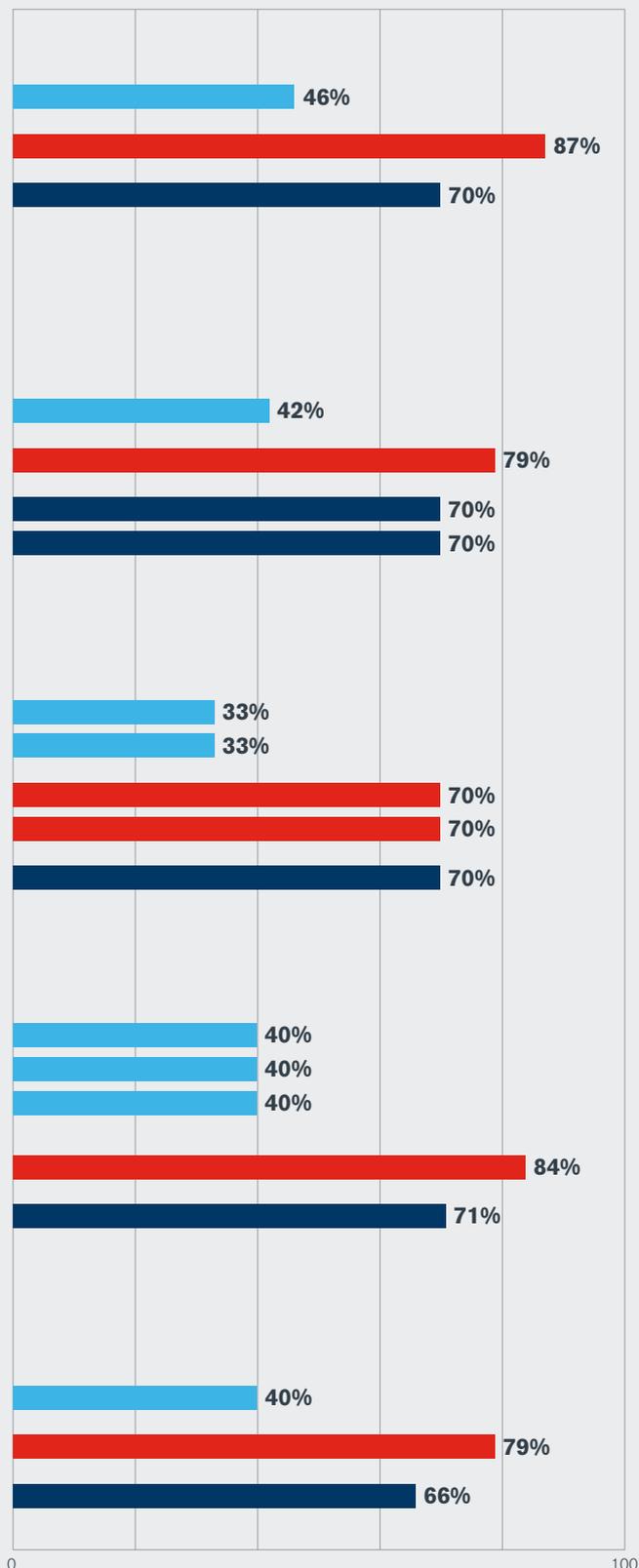
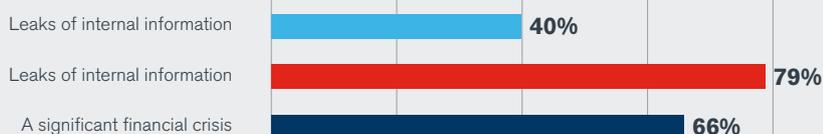
RETAIL, WHOLESALE AND DISTRIBUTION



TECHNOLOGY, MEDIA AND TELECOMS

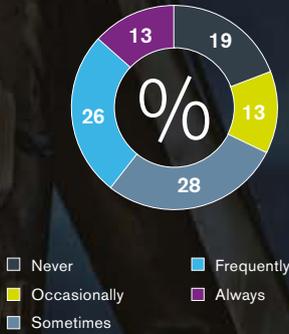


TRANSPORTATION, LEISURE AND TOURISM

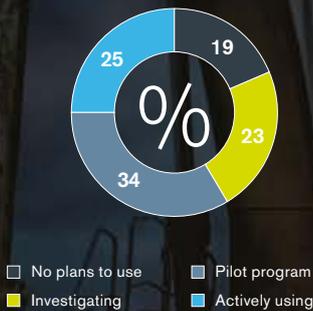


Construction, Engineering and Infrastructure

USE OF BRAND "INFLUENCERS"



ADOPTION OF CRYPTOCURRENCY



WHO WERE THE PERPETRATORS OF INCIDENTS?



The global boom in construction has been heavily affected by current trade wars, which have included tariffs on both raw materials, like steel, and heavy equipment, such as cranes. So it is that within the construction sector (a group that also includes engineering and infrastructure), 38 percent of survey respondents say they have been affected by **disruptions due to sanctions, tariffs and changes in trade agreements**, second only to the share of respondents in the technology industry. Construction also has the highest percentage of respondents indicating they have been affected by **political unrest** (60 percent vs. 49 percent for all industries). Sensitivity to this risk is hardly surprising, given the sizable role that government contracts play in this sector.

The construction industry has also been hard-hit by **leaks of internal information**, with 45 percent of firms reporting significant effects within the last year (vs. 39 percent for all industries).

Bribery and corruption have been a perennial risk management challenge for the industry. The share of construction firms (30 percent) affected by these threats is comparatively high, exceeded only by that of the transportation sector. Tellingly, construction has less confidence in its **anti-bribery and anti-corruption controls** than does any other industry surveyed (51 percent vs. 69 percent for all industries) but is addressing this vulnerability by designating the fight against bribery and corruption a top industry priority (70 percent vs. 62 percent for all industries). Fortunately, our survey results suggest a possible path forward. The percentage of construction industry respondents with confidence in their organization's **data analytics** as an effective risk detection method is lower than that of any other industry (66 percent vs. 77 percent for all industries). Further, for all types of incidents, the construction industry's **internal audit** function was less likely than average to have uncovered the threat (24 percent vs. 28 percent for all industries). Investing in data analytics to identify patterns of corruption early on could help firms control this risk and strengthen internal audit.

While construction industry respondents believe their anti-bribery and anti-corruption controls to be their least reliable risk mitigation measures, they exhibit skepticism about the efficacy of virtually all such mechanisms, including **reputational due diligence of third parties** (66 percent vs. 73 percent for all industries) and **anti-money laundering controls** (62 percent vs. 69 percent for all industries). Collectively, this data reveals that the construction industry has a considerable opportunity to strengthen its risk management controls. In doing so, construction companies should consider involving personnel throughout their organizations; only 64 percent of construction respondents—a smaller share than in virtually any other industry—agree that **risk management programs are designed with input from those who must conform to them** (vs. 74 percent for all industries).

Looking to the future, the construction industry is greatly concerned about events that could upend economic and political stability, including possible **military conflict** (64 percent vs. 51 percent for all industries) and a **significant financial crisis** (77 percent vs. 69 percent for all industries). Meanwhile, the industry is also paying closer-than-average attention to technology-driven disruptions, including **market manipulations through fake news** (70 percent vs. 59 percent for all industries) and disruptions caused by **artificial intelligence** (66 percent vs. 56 percent for all industries).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	45%	39%	▲ 6%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	38%	27%	▲ 11%
Reputational damage due to third-party relationship	30%	29%	▲ 1%
Adversarial social media activity	30%	27%	▲ 3%
Bribery and corruption	30%	23%	▲ 7%
IP theft (e.g., trade secrets)	26%	24%	▲ 2%
Fraud by external parties	25%	28%	▼ -3%
Fraud by internal parties	23%	27%	▼ -4%
Money laundering	21%	16%	▲ 5%
Data theft (e.g., customer records)	19%	29%	▼ -10%
Counterfeiting or gray market activity	9%	17%	▼ -8%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	62%	54%	▲ 8%
Political unrest	60%	49%	▲ 11%
Government influence on a vendor, partner, customer or other entity with which your company does business	58%	51%	▲ 7%
Newly imposed sanctions against doing business with a government, entity or person	47%	47%	■ 0%
Changes in economic treaties between countries	47%	51%	▼ -4%
Restrictions on foreign investment	43%	47%	▼ -4%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
Reputational damage due to third-party relationship	70%	73%	▼ -3%
Leaks of internal information	70%	73%	▼ -3%
Bribery and corruption	70%	62%	▲ 8%
Data theft (e.g., customer records)	68%	76%	▼ -8%
IP theft (e.g., trade secrets)	66%	72%	▼ -6%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	64%	62%	▲ 2%
Fraud by external parties	62%	68%	▼ -6%
Fraud by internal parties	58%	66%	▼ -8%
Adversarial social media activity	58%	63%	▼ -5%
Counterfeiting or gray market activity	49%	58%	▼ -9%
Money laundering	45%	62%	▼ -17%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A significant financial crisis	77%	69%	▲ 8%
Market manipulation through fake news	70%	59%	▲ 11%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	68%	61%	▲ 7%
Disruptions caused by artificial intelligence or other technologies	66%	56%	▲ 10%
Political instability	66%	63%	▲ 3%
Military conflict	64%	51%	▲ 13%
Large-scale, coordinated cyberattacks	60%	68%	▼ -8%
Destabilization of fiat currency due to cryptocurrency	55%	53%	▲ 2%
Climate change	55%	54%	▲ 1%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	24%	28%	▼ -4%
External audit	18%	17%	▲ 1%
By management at our company	18%	16%	▲ 2%
Customers/suppliers	16%	13%	▲ 3%
Regulator/law enforcement	13%	13%	■ 0%
Whistleblower	11%	13%	▼ -2%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	77%	81%	▼ -4%
Compliance (regulatory, codes of conduct, etc.)	72%	75%	▼ -3%
Due diligence of third-party reputation and practices	66%	73%	▼ -7%
Data analytics	66%	77%	▼ -11%
Whistleblowing	66%	66%	■ 0%
Monitoring social media for adversarial activity	64%	71%	▼ -7%
Anti-money laundering controls	62%	69%	▼ -7%
Anti-bribery and anti-corruption controls	51%	69%	▼ -18%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

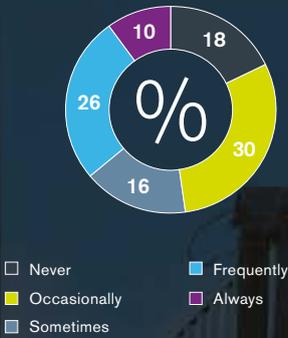
Business partners	94%	92%	▲ 2%
Potential M&A targets	92%	89%	▲ 3%
Customers	90%	88%	▲ 2%
Board or senior executive candidates	90%	91%	▼ -1%
Suppliers	88%	92%	▼ -4%
Brand ambassadors/influencers	80%	85%	▼ -5%
Investors	79%	84%	▼ -5%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

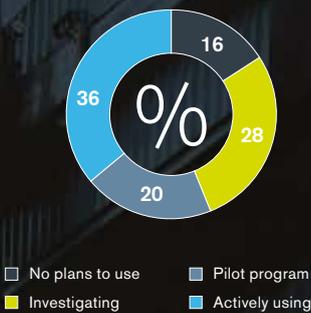
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	77%	78%	▼ -1%
Performance goals and incentives do not conflict with risk management practices.	77%	71%	▲ 6%
The company responds to risk management incidents in a consistent way.	77%	75%	▲ 2%
New business initiatives are regularly examined for all appropriate risk implications.	77%	74%	▲ 3%
Employees view risk management processes as being effective.	77%	76%	▲ 1%
Serious breaches of risk management processes are met with thorough internal investigations.	70%	75%	▼ -5%
Our risk management processes are adapted to local market and cultural nuances.	68%	72%	▼ -4%
Risk management programs are designed with input from those who must conform to them.	64%	74%	▼ -10%



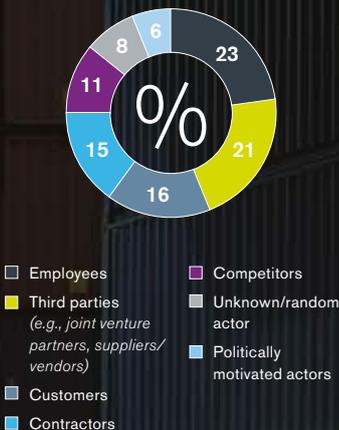
USE OF BRAND "INFLUENCERS"



ADOPTION OF CRYPTOCURRENCY



WHO WERE THE PERPETRATORS OF INCIDENTS?



Consumer Goods

Respondents in the consumer goods industry experience a notable level of incidents in two key areas of the value chain. The first is **reputational damage caused by third-party relationships** (34 percent vs. 29 percent for all industries). The second is **counterfeiting and gray market activity** (26 percent vs. 17 percent for all industries).

Adverse incidents caused by third-party relationships are most often due to issues in the supply chain. Consumers now place a much greater emphasis on the integrity of the supply chain and the ethical standards of the brands whose products they buy. So it is that consumer goods organizations are more likely than those in any other industry to prioritize mitigating against reputational damage caused by third parties (84 percent vs. 73 percent for all industries). However, this concern is not always manifest in practice. While consumer goods companies are more likely than the average of all industries to conduct reputational due diligence on some stakeholders, they are slightly less likely to do so on **business partners and suppliers**. Given the industry's branding concerns, reputational due diligence on these two groups should be standard practice.

Counterfeiting and gray market activity remain persistent problems. In our survey, 26 percent of consumer goods companies report experiencing significant counterfeiting incidents within the last 12 months (vs. 17 percent for all industries). Counterfeiting infringements are so frequent that many businesses find they have to be selective in the cases they choose to pursue.

Respondents in the consumer goods industry acknowledge that their companies instill a strong culture of transparency and accountability. A significant majority of respondents say they get a **clear message from the top of their organizations** that a culture of integrity is important (88 percent vs. 78 percent for all industries), and the proportion who agree that their companies **respond to risk management incidents in consistent ways** is higher than in any industry besides life sciences (84 percent vs. 75 percent for all industries).

Thirty-six percent of consumer goods respondents—a higher percentage than in any other industry—indicate that their organizations are actively using **cryptocurrency** (vs. 28 percent for all industries). The industry is expected to continue to be a bellwether for broader crypto adoption.

At a higher rate than any other industry, consumer goods organizations express concern about three possible future risks: **large-scale, coordinated cyberattacks** (82 percent vs. 68 percent for all industries), **a significant financial crisis** (78 percent vs. 69 percent for all industries) and **political instability** (70 percent vs. 63 percent for all industries).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	38%	39%	▼ -1%
Reputational damage due to third-party relationship	34%	29%	▲ 5%
Data theft (e.g., customer records)	30%	29%	▲ 1%
Fraud by internal parties	30%	27%	▲ 3%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	26%	27%	▼ -1%
Counterfeiting or gray market activity	26%	17%	▲ 9%
Bribery and corruption	26%	23%	▲ 3%
Fraud by external parties	24%	28%	▼ -4%
Adversarial social media activity	20%	27%	▼ -7%
IP theft (e.g., trade secrets)	20%	24%	▼ -4%
Money laundering	8%	16%	▼ -8%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Government influence on a vendor, partner, customer or other entity with which your company does business	54%	51%	▲ 3%
Political unrest	52%	49%	▲ 3%
New tariffs or trade wars	48%	54%	▼ -6%
Restrictions on foreign investment	48%	47%	▲ 1%
Changes in economic treaties between countries	46%	51%	▼ -5%
Newly imposed sanctions against doing business with a government, entity or person	44%	47%	▼ -3%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION? (Percent responding "significant priority" or "high priority")			
Reputational damage due to third-party relationship	84%	73%	▲ 11%
Leaks of internal information	78%	73%	▲ 5%
Data theft (e.g., customer records)	72%	76%	▼ -4%
IP theft (e.g., trade secrets)	70%	72%	▼ -2%
Fraud by internal parties	68%	66%	▲ 2%
Bribery and corruption	66%	62%	▲ 4%
Adversarial social media activity	66%	63%	▲ 3%
Fraud by external parties	66%	68%	▼ -2%
Counterfeiting or gray market activity	64%	58%	▲ 6%
Money laundering	64%	62%	▲ 2%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	58%	62%	▼ -4%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Large-scale, coordinated cyberattacks	82%	68%	▲ 14%
A significant financial crisis	78%	69%	▲ 9%
Political instability	70%	63%	▲ 7%
Market manipulation through fake news	66%	59%	▲ 7%
Destabilization of fiat currency due to cryptocurrency	62%	53%	▲ 9%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	58%	61%	▼ -3%
Climate change	56%	54%	▲ 2%
Military conflict	54%	51%	▲ 3%
Disruptions caused by artificial intelligence or other technologies	54%	56%	▼ -2%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	29%	28%	▲ 1%
External audit	19%	17%	▲ 2%
Customers/suppliers	16%	13%	▲ 3%
Whistleblower	13%	13%	■ 0%
Regulator/law enforcement	13%	13%	■ 0%
By management at our company	9%	16%	▼ -7%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	90%	81%	▲ 9%
Data analytics	78%	77%	▲ 1%
Anti-money laundering controls	78%	69%	▲ 9%
Compliance (regulatory, codes of conduct, etc.)	76%	75%	▲ 1%
Due diligence of third-party reputation and practices	72%	73%	▼ -1%
Monitoring social media for adversarial activity	70%	71%	▼ -1%
Anti-bribery and anti-corruption controls	70%	69%	▲ 1%
Whistleblowing	64%	66%	▼ -2%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

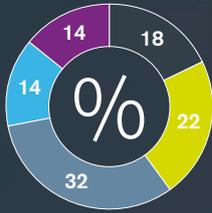
Board or senior executive candidates	96%	91%	▲ 5%
Customers	94%	88%	▲ 6%
Investors	93%	84%	▲ 9%
Business partners	91%	92%	▼ -1%
Suppliers	91%	92%	▼ -1%
Potential M&A targets	90%	89%	▲ 1%
Brand ambassadors/influencers	90%	85%	▲ 5%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	88%	78%	▲ 10%
The company responds to risk management incidents in a consistent way.	84%	75%	▲ 9%
New business initiatives are regularly examined for all appropriate risk implications.	82%	74%	▲ 8%
Our risk management processes are adapted to local market and cultural nuances.	78%	72%	▲ 6%
Employees view risk management processes as being effective.	76%	76%	■ 0%
Serious breaches of risk management processes are met with thorough internal investigations.	74%	75%	▼ -1%
Performance goals and incentives do not conflict with risk management practices.	74%	71%	▲ 3%
Risk management programs are designed with input from those who must conform to them.	72%	74%	▼ -2%

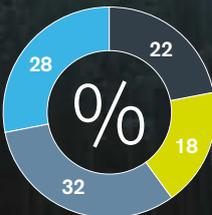


USE OF BRAND "INFLUENCERS"



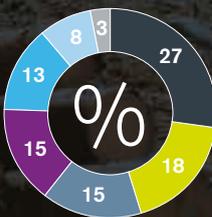
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Competitors
- Contractors
- Politically motivated actors
- Unknown/random actor

Extractives

Many countries with a wealth of natural resources are still developing anti-fraud regulatory and enforcement capabilities and building cultures of transparency. It is therefore not surprising that the extractives industry (including oil, gas and mining) experiences a comparatively high rate of **fraud by internal parties** (36 percent vs. 27 percent for all industries) and **money laundering** (22 percent vs. 16 percent for all industries). In line with these findings, across all types of incidents, the extractives sector has a larger-than-average share of perpetrators who are **politically motivated actors** (8 percent vs. 6 percent for all industries)—a category that includes government officials. In addition, along with manufacturing, extractives suffers from among the greatest incidence of **leaks of internal information** (46 percent vs. 39 percent for all industries) and **reputational damage due to third-party relationships** (34 percent vs. 29 percent for all industries). This last finding may be the result of consumers' increased attention to the environmental impact of corporate practices.

The extractives industry has aligned its **risk priorities** with the threats that it currently faces. Indeed, its respondents were more likely than those of any other industry to prioritize fighting **leaks of internal information** (82 percent vs. 73 percent for all industries) and **fraud by internal parties** (78 percent vs. 66 percent overall). And while the degree of reported **disruption due to sanctions, tariffs and trade agreements** in the extractives industry is only slightly higher than average (30 percent vs. 27 percent for all industries), this sector's respondents are most likely to make mitigating that risk a priority (70 percent vs. 62 percent for all industries).

The extractives industry is notable for how often incidents are detected by **internal audit**. Respondents in this industry say that the internal audit function identified 36 percent of incidents, a larger share than in any other (vs. 28 percent for all industries). In line with this, the extractives industry is second only to technology in agreeing that **serious breaches of risk management processes are met with thorough internal investigations** (80 percent vs. 75 percent for all industries). At the same time, there is room for improvement in the industry's culture with respect to transparency and accountability: Just 66 percent of extractives respondents assert that their companies **respond to risk management incidents in consistent ways** (vs. 75 percent for all industries). Only the manufacturing industry reports a lower rate overall.

Looking ahead, three potential risks cause significantly above-average concern among extractives respondents, and all three are tied to economic stability: the possibility of a **significant financial crisis** (76 percent vs. 69 percent for all industries), **destabilization of fiat currency due to cryptocurrency** (60 percent vs. 53 percent overall) and **disruptions due to artificial intelligence**, which could have implications for commodities trading (66 percent vs. 56 percent overall).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	46%	39%	▲ 7%
Fraud by internal parties	36%	27%	▲ 9%
Reputational damage due to third-party relationship	34%	29%	▲ 5%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	30%	27%	▲ 3%
Data theft (e.g., customer records)	28%	29%	▼ -1%
Counterfeiting or gray market activity	28%	17%	▲ 11%
Fraud by external parties	26%	28%	▼ -2%
Bribery and corruption	24%	23%	▲ 1%
Money laundering	22%	16%	▲ 6%
Adversarial social media activity	20%	27%	▼ -7%
IP theft (e.g., trade secrets)	20%	24%	▼ -4%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	60%	54%	▲ 6%
Government influence on a vendor, partner, customer or other entity with which your company does business	54%	51%	▲ 3%
Changes in economic treaties between countries	52%	51%	▲ 1%
Restrictions on foreign investment	50%	47%	▲ 3%
Newly imposed sanctions against doing business with a government, entity or person	48%	47%	▲ 1%
Political unrest	48%	49%	▼ -1%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
IP theft (e.g., trade secrets)	84%	72%	▲ 12%
Leaks of internal information	82%	73%	▲ 9%
Counterfeiting or gray market activity	78%	58%	▲ 20%
Fraud by internal parties	78%	66%	▲ 12%
Reputational damage due to third-party relationship	74%	73%	▲ 1%
Data theft (e.g., customer records)	72%	76%	▼ -4%
Fraud by external parties	72%	68%	▲ 4%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	70%	62%	▲ 8%
Money laundering	68%	62%	▲ 6%
Adversarial social media activity	66%	63%	▲ 3%
Bribery and corruption	64%	62%	▲ 2%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A significant financial crisis	76%	69%	▲ 7%
Large-scale, coordinated cyberattacks	72%	68%	▲ 4%
Disruptions caused by artificial intelligence or other technologies	66%	56%	▲ 10%
Political instability	64%	63%	▲ 1%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	62%	61%	▲ 1%
Destabilization of fiat currency due to cryptocurrency	60%	53%	▲ 7%
Market manipulation through fake news	58%	59%	▼ -1%
Climate change	56%	54%	▲ 2%
Military conflict	50%	51%	▼ -1%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	36%	28%	▲ 8%
External audit	14%	17%	▼ -3%
Whistleblower	14%	13%	▲ 1%
Customers/suppliers	13%	13%	■ 0%
Regulator/law enforcement	13%	13%	■ 0%
By management at our company	10%	16%	▼ -6%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Data analytics	82%	77%	▲ 5%
Monitoring social media for adversarial activity	78%	71%	▲ 7%
Cybersecurity	78%	81%	▼ -3%
Compliance (regulatory, codes of conduct, etc.)	76%	75%	▲ 1%
Anti-money laundering controls	74%	69%	▲ 5%
Whistleblowing	72%	66%	▲ 6%
Due diligence of third-party reputation and practices	70%	73%	▼ -3%
Anti-bribery and anti-corruption controls	66%	69%	▼ -3%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

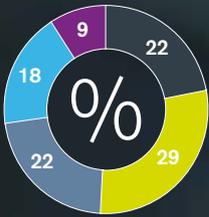
Board or senior executive candidates	94%	91%	▲ 3%
Suppliers	94%	92%	▲ 2%
Business partners	91%	92%	▼ -1%
Customers	89%	88%	▲ 1%
Brand ambassadors/influencers	85%	85%	■ 0%
Potential M&A targets	85%	89%	▼ -4%
Investors	85%	84%	▲ 1%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

Serious breaches of risk management processes are met with thorough internal investigations.	80%	75%	▲ 5%
Risk management programs are designed with input from those who must conform to them.	80%	74%	▲ 6%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	78%	78%	■ 0%
Our risk management processes are adapted to local market and cultural nuances.	78%	72%	▲ 6%
Employees view risk management processes as being effective.	72%	76%	▼ -4%
Performance goals and incentives do not conflict with risk management practices.	70%	71%	▼ -1%
New business initiatives are regularly examined for all appropriate risk implications.	70%	74%	▼ -4%
The company responds to risk management incidents in a consistent way.	66%	75%	▼ -9%

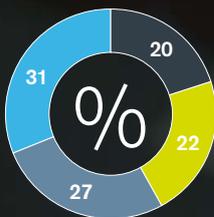


USE OF BRAND "INFLUENCERS"



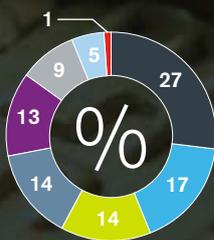
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Contractors
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Competitors
- Unknown/random actor
- Politically motivated actors
- Don't know/does not apply

Financial Services

Financial services is one of the most regulated of all sectors, a characteristic borne out by the industry's risk profile. Responses to our survey indicate a lower rate of **bribery and corruption** than any other industry (13 percent vs. 23 percent for all industries) and a likelihood of **money laundering** that is only slightly above average despite the industry's considerable inherent risk in this area (18 percent vs. 16 percent for all industries). Not surprisingly, given financial services' regulatory framework, those organizations are more likely than others to prioritize the mitigation of money laundering (73 percent vs. 62 percent for all industries).

In recent years, as the financial services industry has expanded its online presence, it has accordingly adopted a higher social media profile, thereby encountering new risks. For example, skeptical consumers can be quick to respond to actual or perceived missteps—and our survey reveals that, indeed, financial services is more likely than average to have experienced significant **adversarial social media activity** (35 percent vs. 27 percent for all industries). Ironically, it is also the industry least likely to make a priority of countering negative social media activity (56 percent vs. 63 percent for all industries), which indicates a clear opportunity for improved risk management in this area.

The survey results also point to two aspects of incident detection that warrant attention. First, financial services firms are less likely than those in any other industry to believe that their **cybersecurity** is effective at detecting incidents (73 percent vs. 81 percent for all industries). This sentiment likely stems from the high-profile cyber incidents that have recently affected the industry and from the awareness that the industry's very nature makes it a perennial high-value target.

In addition, respondents in the financial services industry are less likely than those in any industry besides professional services to hold that their **whistleblowing** program offers effective incident detection (60 percent vs. 66 percent for all industries). In line with this finding, a lower percentage of incidents are detected by internal whistleblowing programs in financial services than in any other industry (10 percent vs. 13 percent for all industries). Financial services organizations may need to strengthen their whistleblowing programs, particularly in light of regulation in several countries that increases whistleblowing protection.

Financial services organizations are less likely than average to have been affected by **geopolitical risks**—with the notable exception of **restrictions on foreign investment**, which have affected the financial services industry more than any other due to its role as an investment intermediary (55 percent vs. 47 percent for all industries).

Looking ahead five years, the financial services industry is less concerned than any other industry about either **military conflict** (38 percent vs. 51 percent for all industries) or **climate change** (47 percent vs. 54 percent for all industries). Most notably, financial services expresses the least concern of all industries regarding possible **destabilization of fiat currency due to cryptocurrency** (38 percent vs. 53 percent for all industries)—a finding that may pave the way for increased acceptance of these digital assets.

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Adversarial social media activity	35%	27%	▲ 8%
Fraud by external parties	35%	28%	▲ 7%
Leaks of internal information	33%	39%	▼ -6%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	31%	27%	▲ 4%
Data theft (e.g., customer records)	31%	29%	▲ 2%
Reputational damage due to third-party relationship	25%	29%	▼ -4%
Fraud by internal parties	25%	27%	▼ -2%
Money laundering	18%	16%	▲ 2%
IP theft (e.g., trade secrets)	16%	24%	▼ -8%
Bribery and corruption	13%	23%	▼ -10%
Counterfeiting or gray market activity	9%	17%	▼ -8%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Restrictions on foreign investment	55%	47%	▲ 8%
Changes in economic treaties between countries	45%	51%	▼ -6%
Newly imposed sanctions against doing business with a government, entity or person	45%	47%	▼ -2%
Political unrest	44%	49%	▼ -5%
New tariffs or trade wars	42%	54%	▼ -12%
Government influence on a vendor, partner, customer or other entity with which your company does business	36%	51%	▼ -15%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
Leaks of internal information	80%	73%	▲ 7%
Data theft (e.g., customer records)	75%	76%	▼ -1%
Reputational damage due to third-party relationship	73%	73%	■ 0%
Money laundering	73%	62%	▲ 11%
Fraud by external parties	73%	68%	▲ 5%
IP theft (e.g., trade secrets)	65%	72%	▼ -7%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	64%	62%	▲ 2%
Fraud by internal parties	64%	66%	▼ -2%
Bribery and corruption	58%	62%	▼ -4%
Adversarial social media activity	56%	63%	▼ -7%
Counterfeiting or gray market activity	55%	58%	▼ -3%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Large-scale, coordinated cyberattacks	62%	68%	▼ -6%
A significant financial crisis	60%	69%	▼ -9%
Disruptions caused by artificial intelligence or other technologies	58%	56%	▲ 2%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	56%	61%	▼ -5%
Political instability	55%	63%	▼ -8%
Market manipulation through fake news	51%	59%	▼ -8%
Climate change	47%	54%	▼ -7%
Destabilization of fiat currency due to cryptocurrency	38%	53%	▼ -15%
Military conflict	38%	51%	▼ -13%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	28%	28%	■ 0%
External audit	22%	17%	▲ 5%
Customers/suppliers	15%	13%	▲ 2%
By management at our company	14%	16%	▼ -2%
Whistleblower	10%	13%	▼ -3%
Regulator/law enforcement	9%	13%	▼ -4%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Data analytics	75%	77%	▼ -2%
Due diligence of third-party reputation and practices	73%	73%	■ 0%
Cybersecurity	73%	81%	▼ -8%
Anti-bribery and anti-corruption controls	71%	69%	▲ 2%
Compliance (regulatory, codes of conduct, etc.)	71%	75%	▼ -4%
Anti-money laundering controls	69%	69%	■ 0%
Monitoring social media for adversarial activity	67%	71%	▼ -4%
Whistleblowing	60%	66%	▼ -6%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

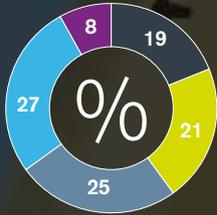
Suppliers	94%	92%	▲ 2%
Business partners	94%	92%	▲ 2%
Customers	93%	88%	▲ 5%
Potential M&A targets	90%	89%	▲ 1%
Board or senior executive candidates	88%	91%	▼ -3%
Brand ambassadors/influencers	88%	85%	▲ 3%
Investors	86%	84%	▲ 2%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	80%	78%	▲ 2%
Risk management programs are designed with input from those who must conform to them.	76%	74%	▲ 2%
Serious breaches of risk management processes are met with thorough internal investigations.	76%	75%	▲ 1%
Performance goals and incentives do not conflict with risk management practices.	73%	71%	▲ 2%
New business initiatives are regularly examined for all appropriate risk implications.	73%	74%	▼ -1%
Employees view risk management processes as being effective.	73%	76%	▼ -3%
The company responds to risk management incidents in a consistent way.	69%	75%	▼ -6%
Our risk management processes are adapted to local market and cultural nuances.	67%	72%	▼ -5%

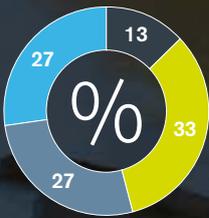


USE OF BRAND "INFLUENCERS"



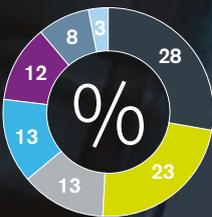
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Unknown/random actor
- Contractors
- Competitors
- Customers
- Politically motivated actors

Life Sciences

Along with financial services, life sciences (encompassing healthcare, pharmaceuticals and biotechnology) is one of the most highly regulated of all industries, and its risk profile reflects that. In our survey, life sciences respondents reported the lowest rates of **counterfeiting or gray market activity** (8 percent vs. 17 percent for all industries) and **fraud by external parties** (10 percent vs. 28 percent for all industries) and among the lowest level of significant **leaks of internal information** (33 percent vs. 39 percent for all industries).

The industry is helped in achieving these results by a strong risk management infrastructure. The **internal audit** function plays a greater role in detecting incidents in the life sciences industry than in any industry other than extractives (35 percent vs. 28 percent for all industries). The life sciences sector also has high confidence in the effectiveness of its **whistleblowing** mechanisms (73 percent vs. 66 percent for all industries) and its respondents are more likely than those in any other industry to say their organizations **respond to risk management incidents in consistent ways** (85 percent vs. 75 percent for all industries).

The life sciences industry also places significant emphasis on **reputational due diligence**. It is more likely than any other industry in our survey to conduct such due diligence on **suppliers** (100 percent vs. 92 percent for all industries), **business partners** (100 percent vs. 92 percent overall), and, along with the professional services industry, **potential M&A targets** (94 percent vs. 89 percent overall). At the same time, respondents in this sector are the least likely to conduct reputational due diligence on **investors** (71 percent vs. 84 percent for all industries). This omission might be explained by a tendency for private investors in life sciences to be large, well-established players. Still, in line with these overall findings, the life sciences industry has more confidence in the effectiveness of its reputational due diligence than any other industry (85 percent vs. 73 percent for all industries).

While the life sciences industry experiences **data theft** at a rate slightly below the average (27 percent vs. 29 percent for all industries), it is more likely than any sector besides manufacturing to make combating data theft a priority (83 percent vs. 76 percent for all industries). This is no doubt influenced by regulatory requirements and the legal, financial and reputational consequences of a breach involving personal medical records and other life sciences data.

Respondents in the life sciences industry are also most likely to express confidence that their organizations' **monitoring of social media for adversarial activity** is effective (87 percent vs. 71 percent for all industries). Effective social media monitoring is a natural consequence of the extensive regulation covering the marketing of medical products in many jurisdictions.

While life sciences respondents are less likely than those in any other industry to report **experiencing disruption due to sanctions, tariffs and changes in trade agreements** (15 percent vs. 27 percent for all industries), this does not mean the industry is immune to geopolitical concerns. Fifty-eight percent of life sciences respondents report having been affected by **changes in economic treaties** (vs. 51 percent for all industries); the same percentage has been affected by **trade wars** (vs. 54 percent overall). These figures may convey growing concern within the industry about the effects of continued geopolitical tensions on future availability of raw materials.

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	33%	39%	▼ -6%
Reputational damage due to third-party relationship	31%	29%	▲ 2%
Data theft (e.g., customer records)	27%	29%	▼ -2%
Adversarial social media activity	21%	27%	▼ -6%
Fraud by internal parties	19%	27%	▼ -8%
IP theft (e.g., trade secrets)	17%	24%	▼ -7%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	15%	27%	▼ -12%
Bribery and corruption	15%	23%	▼ -8%
Money laundering	12%	16%	▼ -4%
Fraud by external parties	10%	28%	▼ -18%
Counterfeiting or gray market activity	8%	17%	▼ -9%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	58%	54%	▲ 4%
Changes in economic treaties between countries	58%	51%	▲ 7%
Newly imposed sanctions against doing business with a government, entity or person	48%	47%	▲ 1%
Political unrest	44%	49%	▼ -5%
Government influence on a vendor, partner, customer or other entity with which your company does business	44%	51%	▼ -7%
Restrictions on foreign investment	42%	47%	▼ -5%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
Data theft (e.g., customer records)	83%	76%	▲ 7%
Reputational damage due to third-party relationship	71%	73%	▼ -2%
Leaks of internal information	71%	73%	▼ -2%
IP theft (e.g., trade secrets)	67%	72%	▼ -5%
Fraud by internal parties	63%	66%	▼ -3%
Adversarial social media activity	60%	63%	▼ -3%
Fraud by external parties	60%	68%	▼ -8%
Counterfeiting or gray market activity	56%	58%	▼ -2%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	54%	62%	▼ -8%
Money laundering	50%	62%	▼ -12%
Bribery and corruption	48%	62%	▼ -14%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A significant financial crisis	71%	69%	▲ 2%
Large-scale, coordinated cyberattacks	71%	68%	▲ 3%
Market manipulation through fake news	62%	59%	▲ 3%
Disruptions caused by artificial intelligence or other technologies	58%	56%	▲ 2%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	56%	61%	▼ -5%
Climate change	54%	54%	■ 0%
Political instability	52%	63%	▼ -11%
Destabilization of fiat currency due to cryptocurrency	50%	53%	▼ -3%
Military conflict	50%	51%	▼ -1%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	35%	28%	▲ 7%
Customers/suppliers	17%	13%	▲ 4%
External audit	14%	17%	▼ -3%
By management at our company	13%	16%	▼ -3%
Whistleblower	12%	13%	▼ -1%
Regulator/law enforcement	9%	13%	▼ -4%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Monitoring social media for adversarial activity	87%	71%	▲ 16%
Due diligence of third-party reputation and practices	85%	73%	▲ 12%
Cybersecurity	83%	81%	▲ 2%
Data analytics	79%	77%	▲ 2%
Compliance (regulatory, codes of conduct, etc.)	77%	75%	▲ 2%
Whistleblowing	73%	66%	▲ 7%
Anti-bribery and anti-corruption controls	71%	69%	▲ 2%
Anti-money laundering controls	67%	69%	▼ -2%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

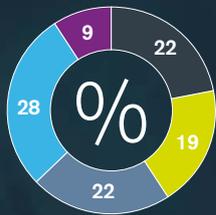
Suppliers	100%	92%	▲ 8%
Business partners	100%	92%	▲ 8%
Potential M&A targets	94%	89%	▲ 5%
Board or senior executive candidates	90%	91%	▼ -1%
Brand ambassadors/influencers	84%	85%	▼ -1%
Customers	82%	88%	▼ -6%
Investors	71%	84%	▼ -13%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

The company responds to risk management incidents in a consistent way.	85%	75%	▲ 10%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	81%	78%	▲ 3%
Risk management programs are designed with input from those who must conform to them.	77%	74%	▲ 3%
Employees view risk management processes as being effective.	77%	76%	▲ 1%
Serious breaches of risk management processes are met with thorough internal investigations.	75%	75%	■ 0%
Performance goals and incentives do not conflict with risk management practices.	75%	71%	▲ 4%
New business initiatives are regularly examined for all appropriate risk implications.	73%	74%	▼ -1%
Our risk management processes are adapted to local market and cultural nuances.	69%	72%	▼ -3%

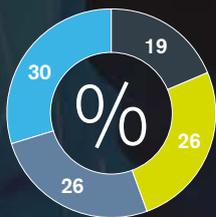


USE OF BRAND "INFLUENCERS"



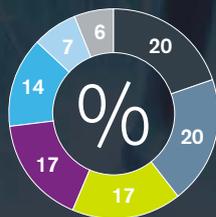
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Customers
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Competitors
- Contractors
- Politically motivated actors
- Unknown/random actor

Manufacturing

The results of our survey highlight many risks to which the manufacturing industry is particularly susceptible. A natural repository of intellectual property, manufacturing is significantly more likely than other industries to have experienced **IP theft** (43 percent vs. 24 percent for all industries); it also matches the extractives sector in experiencing the highest incidence of **leaks of internal information** (46 percent vs. 39 percent for all industries).

In addition, the industry reports significant **reputational damage due to third-party relationships** at a substantially higher rate than average (35 percent vs. 29 percent for all industries)—a clear illustration of how reputational problems can move along a supply chain. Consequently, manufacturing companies would do well to mandate **reputational due diligence for suppliers**, especially given the industry's current below-average rate for such examinations (89 percent vs. 92 percent for all industries).

Manufacturing respondents are less likely than average to say they perceive a **clear message from the top of their organizations that integrity, compliance and accountability are important** (72 percent vs. 78 percent for all industries) and are the least likely respondents from any industry to report that their companies **respond to risk management incidents in consistent ways** (65 percent vs. 75 percent overall).

While **disruptions due to sanctions, tariffs or changes in trade agreements** have affected the manufacturing industry at an average rate (28 percent vs. 27 percent for all industries), geopolitical issues have nevertheless had a significant effect on the sector. Manufacturing is the industry most likely to report having been affected by **newly imposed sanctions** (57 percent vs. 47 percent for all industries) and by **new tariffs or trade wars** (69 percent vs. 54 percent for all industries). The industry as a whole does not expect geopolitical risks to abate anytime soon—in our survey, manufacturing respondents are more likely than respondents in any other industry to express concern about a potential **breakdown in intergovernmental mechanisms for dispute resolution, free trade and combating corruption** (69 percent vs. 61 percent for all industries).

Geopolitical risks are not the only issues anticipated by the manufacturing industry. Given the immense effects that robotics and other technologies have had on manufacturing, naturally this sector is more concerned than any other about **disruptions due to artificial intelligence** (67 percent vs. 56 percent for all industries). Manufacturing respondents also report far more concern than those in any other industry about **destabilization of fiat currency due to cryptocurrency** (67 percent vs. 53 percent for all industries).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	46%	39%	▲ 7%
IP theft (e.g., trade secrets)	43%	24%	▲ 19%
Reputational damage due to third-party relationship	35%	29%	▲ 6%
Fraud by external parties	31%	28%	▲ 3%
Fraud by internal parties	30%	27%	▲ 3%
Adversarial social media activity	28%	27%	▲ 1%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	28%	27%	▲ 1%
Data theft (e.g., customer records)	28%	29%	▼ -1%
Bribery and corruption	28%	23%	▲ 5%
Money laundering	22%	16%	▲ 6%
Counterfeiting or gray market activity	17%	17%	■ 0%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	69%	54%	▲ 15%
Newly imposed sanctions against doing business with a government, entity or person	57%	47%	▲ 10%
Changes in economic treaties between countries	56%	51%	▲ 5%
Political unrest	44%	49%	▼ -5%
Government influence on a vendor, partner, customer or other entity with which your company does business	44%	51%	▼ -7%
Restrictions on foreign investment	43%	47%	▼ -4%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
Data theft (e.g., customer records)	87%	76%	▲ 11%
IP theft (e.g., trade secrets)	83%	72%	▲ 11%
Leaks of internal information	78%	73%	▲ 5%
Fraud by internal parties	76%	66%	▲ 10%
Bribery and corruption	76%	62%	▲ 14%
Reputational damage due to third-party relationship	74%	73%	▲ 1%
Fraud by external parties	70%	68%	▲ 2%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	69%	62%	▲ 7%
Counterfeiting or gray market activity	67%	58%	▲ 9%
Adversarial social media activity	65%	63%	▲ 2%
Money laundering	63%	62%	▲ 1%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Large-scale, coordinated cyberattacks	70%	68%	▲ 2%
A significant financial crisis	69%	69%	■ 0%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	69%	61%	▲ 8%
Destabilization of fiat currency due to cryptocurrency	67%	53%	▲ 14%
Disruptions caused by artificial intelligence or other technologies	67%	56%	▲ 11%
Market manipulation through fake news	65%	59%	▲ 6%
Political instability	63%	63%	■ 0%
Military conflict	54%	51%	▲ 3%
Climate change	52%	54%	▼ -2%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
By management at our company	25%	16%	▲ 9%
Internal audit	21%	28%	▼ -7%
Regulator/law enforcement	19%	13%	▲ 6%
External audit	13%	17%	▼ -4%
Whistleblower	13%	13%	■ 0%
Customers/suppliers	10%	13%	▼ -3%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	81%	81%	■ 0%
Compliance (regulatory, codes of conduct, etc.)	80%	75%	▲ 5%
Data analytics	78%	77%	▲ 1%
Due diligence of third-party reputation and practices	78%	73%	▲ 5%
Anti-bribery and anti-corruption controls	72%	69%	▲ 3%
Anti-money laundering controls	70%	69%	▲ 1%
Monitoring social media for adversarial activity	65%	71%	▼ -6%
Whistleblowing	61%	66%	▼ -5%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

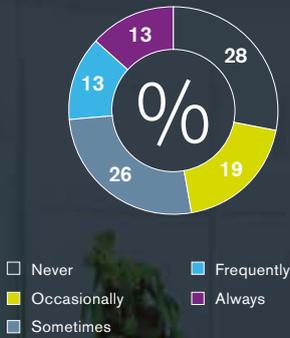
Business partners	92%	92%	■ 0%
Board or senior executive candidates	90%	91%	▼ -1%
Suppliers	89%	92%	▼ -3%
Potential M&A targets	86%	89%	▼ -3%
Customers	85%	88%	▼ -3%
Investors	84%	84%	■ 0%
Brand ambassadors/influencers	82%	85%	▼ -3%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

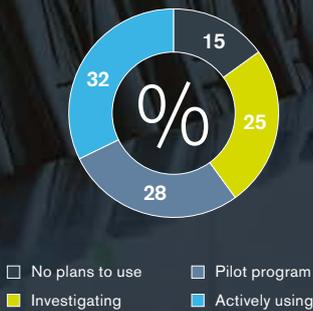
New business initiatives are regularly examined for all appropriate risk implications.	74%	74%	■ 0%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	72%	78%	▼ -6%
Employees view risk management processes as being effective.	72%	76%	▼ -4%
Serious breaches of risk management processes are met with thorough internal investigations.	70%	75%	▼ -5%
Performance goals and incentives do not conflict with risk management practices.	70%	71%	▼ -1%
Risk management programs are designed with input from those who must conform to them.	70%	74%	▼ -4%
Our risk management processes are adapted to local market and cultural nuances.	67%	72%	▼ -5%
The company responds to risk management incidents in a consistent way.	65%	75%	▼ -10%



USE OF BRAND "INFLUENCERS"



ADOPTION OF CRYPTOCURRENCY



WHO WERE THE PERPETRATORS OF INCIDENTS?



Professional Services

Because professional services—law firms, accounting firms, consulting firms and the like—often have access to clients' sensitive and confidential information, these organizations constitute high-value targets for bad actors seeking inside knowledge on the business strategy and dealings of other entities. So it is that, according to our survey, the rate at which professional services firms experienced significant **data theft** in the past year far outstrips that of any other industry (42 percent vs. 29 percent for all industries). And while the likelihood is comparatively small that the professional services industry has experienced **disruption due to sanctions, tariffs or changes in trade agreements** (17 percent vs. 27 percent for all industries), these firms have felt the effect of two geopolitical factors: **restrictions on foreign investment** (53 percent vs. 47 percent for all industries) and **government influence on a vendor, partner, customer or other entity with which the firm does business** (57 percent vs. 51 percent for all industries).

The professional services industry is unique in that even very large firms are essentially aggregations of individual practitioners. This can make it challenging to establish a firm-wide culture. Perhaps that explains why a relatively small share of professional services respondents believe that their firm's behavior promote a culture of transparency and accountability. A lower percentage of respondents in professional services than in any other industry report that they get a **clear message from the top of their organizations that integrity, compliance and accountability are important** (68 percent vs. 78 percent for all industries), that **employees view risk management processes as being effective** (68 percent vs. 76 percent for all industries) and, along with the construction industry, that **risk management programs are designed with input from those who must conform to them** (64 percent vs. 74 percent for all industries).

Professional services firms have begun to incorporate social media into their communications strategies, and these firms are more likely than average to say they always use **social media influencers** (13 percent vs. 9 percent for all industries). However, skeptics remain: A larger-than-average percentage also say they never use them (28 percent vs. 22 percent for all industries). And when the professional services industry uses influencers or brand ambassadors, it is more likely than any other industry to conduct **reputational due diligence** on them (95 percent vs. 85 percent for all industries).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Data theft (e.g., customer records)	42%	29%	▲ 13%
Leaks of internal information	40%	39%	▲ 1%
Fraud by internal parties	32%	27%	▲ 5%
Reputational damage due to third-party relationship	30%	29%	▲ 1%
Counterfeiting or gray market activity	30%	17%	▲ 13%
Fraud by external parties	26%	28%	▼ -2%
Bribery and corruption	26%	23%	▲ 3%
Adversarial social media activity	25%	27%	▼ -2%
IP theft (e.g., trade secrets)	19%	24%	▼ -5%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	17%	27%	▼ -10%
Money laundering	13%	16%	▼ -3%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Government influence on a vendor, partner, customer or other entity with which your company does business	57%	51%	▲ 6%
New tariffs or trade wars	53%	54%	▼ -1%
Restrictions on foreign investment	53%	47%	▲ 6%
Newly imposed sanctions against doing business with a government, entity or person	45%	47%	▼ -2%
Changes in economic treaties between countries	40%	51%	▼ -11%
Political unrest	38%	49%	▼ -11%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
Data theft (e.g., customer records)	79%	76%	▲ 3%
Adversarial social media activity	72%	63%	▲ 9%
Reputational damage due to third-party relationship	68%	73%	▼ -5%
Leaks of internal information	64%	73%	▼ -9%
Fraud by internal parties	62%	66%	▼ -4%
Fraud by external parties	62%	68%	▼ -6%
IP theft (e.g., trade secrets)	62%	72%	▼ -10%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	60%	62%	▼ -2%
Bribery and corruption	60%	62%	▼ -2%
Money laundering	53%	62%	▼ -9%
Counterfeiting or gray market activity	51%	58%	▼ -7%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A significant financial crisis	70%	69%	▲ 1%
Large-scale, coordinated cyberattacks	70%	68%	▲ 2%
Political instability	62%	63%	▼ -1%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	58%	61%	▼ -3%
Market manipulation through fake news	57%	59%	▼ -2%
Disruptions caused by artificial intelligence or other technologies	55%	56%	▼ -1%
Destabilization of fiat currency due to cryptocurrency	53%	53%	■ 0%
Climate change	51%	54%	▼ -3%
Military conflict	47%	51%	▼ -4%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	28%	28%	■ 0%
By management at our company	24%	16%	▲ 8%
Whistleblower	13%	13%	■ 0%
Regulator/law enforcement	13%	13%	■ 0%
External audit	11%	17%	▼ -6%
Customers/suppliers	11%	13%	▼ -2%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Compliance (regulatory, codes of conduct, etc.)	75%	75%	■ 0%
Cybersecurity	75%	81%	▼ -6%
Data analytics	74%	77%	▼ -3%
Anti-money laundering controls	72%	69%	▲ 3%
Due diligence of third-party reputation and practices	68%	73%	▼ -5%
Anti-bribery and anti-corruption controls	62%	69%	▼ -7%
Monitoring social media for adversarial activity	60%	71%	▼ -11%
Whistleblowing	57%	66%	▼ -9%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

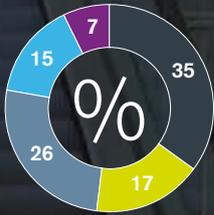
Investors	98%	84%	▲ 14%
Brand ambassadors/influencers	95%	85%	▲ 10%
Suppliers	94%	92%	▲ 2%
Potential M&A targets	94%	89%	▲ 5%
Customers	88%	88%	■ 0%
Board or senior executive candidates	88%	91%	▼ -3%
Business partners	86%	92%	▼ -6%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

Our risk management processes are adapted to local market and cultural nuances.	75%	72%	▲ 3%
Serious breaches of risk management processes are met with thorough internal investigations.	74%	75%	▼ -1%
New business initiatives are regularly examined for all appropriate risk implications.	72%	74%	▼ -2%
The company responds to risk management incidents in a consistent way.	70%	75%	▼ -5%
There is a clear message from the top of the organization that integrity, compliance and accountability are important.	68%	78%	▼ -10%
Employees view risk management processes as being effective.	68%	76%	▼ -8%
Performance goals and incentives do not conflict with risk management practices.	66%	71%	▼ -5%
Risk management programs are designed with input from those who must conform to them.	64%	74%	▼ -10%

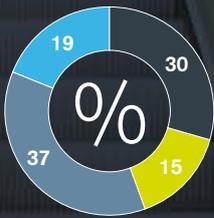


USE OF BRAND "INFLUENCERS"



- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Contractors
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Customers
- Competitors
- Unknown/random actor
- Politically motivated actors
- Don't know/does not apply

Retail, Wholesale and Distribution

Respondents in the retail industry, incorporating both wholesale and distribution, express a lower-than-average level of confidence in almost all of the incident detection mechanisms mentioned in the survey. For example, only 74 percent express confidence in the **effectiveness of their organizations' cybersecurity capabilities** (vs. 81 percent for all industries). The lower-than-average level of confidence expressed by retail respondents here is significant. While only 22 percent of retail organizations (vs. 29 percent for all industries) reported significant **data theft**, the type and scale of customer data held by these companies make them an attractive target for cyber criminals.

A similar trend is found in retail respondents' confidence in the threat detection capabilities of their companies' **data analytics** (69 percent vs. 77 percent for all industries). Strengthening this detection mechanism could help address the industry's concerns regarding loss prevention. The sector may also benefit from paying closer attention to screening of personnel; when considering all categories of threats collectively, the retail industry is more likely than any other to find that the perpetrators are **employees** (30 percent vs. 24 percent for all industries) and **contractors** (22 percent vs. 16 percent for all industries). More than half of all retail risk incidents, in other words, are caused by people inside the organization.

The industry could also redouble its efforts to foster a **culture of transparency and accountability**. Fewer respondents from retail than from any other industry assert that in their organizations **serious breaches of risk management processes are met with thorough internal investigations** (67 percent vs. 75 percent for all industries) or that **risk management processes are adapted to local market and cultural nuances** (65 percent vs. 72 percent for all industries).

In the area of **due diligence**, retail is the least likely of all sectors to conduct reputational due diligence on **candidates for board seats or senior executive positions** (85 percent vs. 91 percent for all industries) or **suppliers** (84 percent vs. 92 percent overall). Given increased public scrutiny of the integrity of both corporate leadership and the supply chain, the retail industry should embrace the use of due diligence as a mechanism for reducing risk in this area.

The retail industry takes a conservative view toward the use of **social media influencers**. Retail respondents are more likely than those from any other industry to report that they never use this type of spokesperson (35 percent vs. 22 percent for all industries). Retail holds a similarly skeptical view of **cryptocurrency**; of all industries, it has the lowest percentage actively using crypto (19 percent vs. 28 percent overall) and the highest percentage with no plans in place to use it (30 percent vs. 19 percent for all industries).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	33%	39%	▼ -6%
Adversarial social media activity	33%	27%	▲ 6%
Fraud by external parties	31%	28%	▲ 3%
Reputational damage due to third-party relationship	26%	29%	▼ -3%
IP theft (e.g., trade secrets)	26%	24%	▲ 2%
Data theft (e.g., customer records)	22%	29%	▼ -7%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	20%	27%	▼ -7%
Counterfeiting or gray market activity	20%	17%	▲ 3%
Fraud by internal parties	19%	27%	▼ -8%
Bribery and corruption	19%	23%	▼ -4%
Money laundering	15%	16%	▼ -1%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

New tariffs or trade wars	59%	54%	▲ 5%
Changes in economic treaties between countries	56%	51%	▲ 5%
Political unrest	56%	49%	▲ 7%
Government influence on a vendor, partner, customer or other entity with which your company does business	48%	51%	▼ -3%
Newly imposed sanctions against doing business with a government, entity or person	46%	47%	▼ -1%
Restrictions on foreign investment	44%	47%	▼ -3%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
Reputational damage due to third-party relationship	70%	73%	▼ -3%
Data theft (e.g., customer records)	70%	76%	▼ -6%
Leaks of internal information	67%	73%	▼ -6%
IP theft (e.g., trade secrets)	67%	72%	▼ -5%
Fraud by external parties	65%	68%	▼ -3%
Adversarial social media activity	63%	63%	■ 0%
Fraud by internal parties	63%	66%	▼ -3%
Money laundering	59%	62%	▼ -3%
Bribery and corruption	57%	62%	▼ -5%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	54%	62%	▼ -8%
Counterfeiting or gray market activity	52%	58%	▼ -6%
LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?			
(Percent "concerned" or "very concerned")			
Large-scale, coordinated cyberattacks	70%	68%	▲ 2%
Political instability	69%	63%	▲ 6%
A significant financial crisis	67%	69%	▼ -2%
Military conflict	61%	51%	▲ 10%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	61%	61%	■ 0%
Market manipulation through fake news	61%	59%	▲ 2%
Climate change	54%	54%	■ 0%
Destabilization of fiat currency due to cryptocurrency	46%	53%	▼ -7%
Disruptions caused by artificial intelligence or other technologies	46%	56%	▼ -10%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	22%	28%	▼ -6%
By management at our company	22%	16%	▲ 6%
External audit	15%	17%	▼ -2%
Regulator/law enforcement	14%	13%	▲ 1%
Customers/suppliers	12%	13%	▼ -1%
Whistleblower	11%	13%	▼ -2%
Don't know/does not apply	3%	1%	▲ 2%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

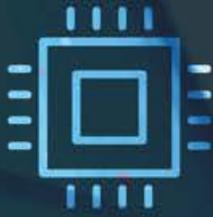
Cybersecurity	74%	81%	▼ -7%
Monitoring social media for adversarial activity	70%	71%	▼ -1%
Data analytics	69%	77%	▼ -8%
Anti-bribery and anti-corruption controls	69%	69%	■ 0%
Compliance (regulatory, codes of conduct, etc.)	69%	75%	▼ -6%
Due diligence of third-party reputation and practices	67%	73%	▼ -6%
Whistleblowing	63%	66%	▼ -3%
Anti-money laundering controls	56%	69%	▼ -13%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

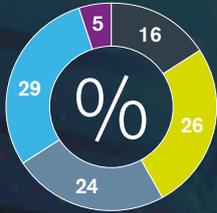
Business partners	91%	92%	▼ -1%
Potential M&A targets	88%	89%	▼ -1%
Board or senior executive candidates	85%	91%	▼ -6%
Suppliers	84%	92%	▼ -8%
Brand ambassadors/influencers	83%	85%	▼ -2%
Customers	83%	88%	▼ -5%
Investors	75%	84%	▼ -9%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	76%	78%	▲ -2%
Employees view risk management processes as being effective.	76%	76%	■ 0%
Risk management programs are designed with input from those who must conform to them.	74%	74%	■ 0%
The company responds to risk management incidents in a consistent way.	72%	75%	▼ -3%
New business initiatives are regularly examined for all appropriate risk implications.	69%	74%	▼ -5%
Performance goals and incentives do not conflict with risk management practices.	67%	71%	▼ -4%
Serious breaches of risk management processes are met with thorough internal investigations.	67%	75%	▼ -8%
Our risk management processes are adapted to local market and cultural nuances.	65%	72%	▼ -7%

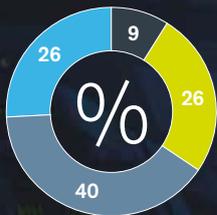


USE OF BRAND "INFLUENCERS"



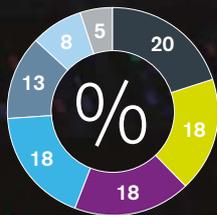
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Employees
- Third parties (e.g., joint venture partners, suppliers/vendors)
- Competitors
- Contractors
- Customers
- Politically motivated actors
- Unknown/random actor

Technology, Media and Telecoms

Our survey results show that geopolitical issues loom large for the technology, media and telecommunications (TMT) industry. Companies in the TMT sector are more likely to have been affected by **sanctions, tariffs or changes in trade agreements** than those in any other industry (40 percent vs. 27 percent for all industries). The TMT industry is also most likely to have been affected by **government influence on a vendor, partner, customer or other entity with which the company does business** (62 percent vs. 51 percent for all industries).

The TMT industry is more likely than any other to have experienced significant **fraud by external parties** (40 percent vs. 28 percent for all industries). Appropriately, TMT respondents are more likely than those in any other industry to make combating this threat a priority (76 percent vs. 68 percent for all industries).

Meanwhile, the TMT industry is least likely to experience **fraud by internal parties** (17 percent vs. 27 percent for all industries). This may be due in part to corporate cultures that strongly emphasize integrity; in our survey, TMT respondents are among the most likely to agree that their company strives for **corporate transparency and accountability**. For example, 86 percent of TMT respondents report that **serious breaches of risk management processes are met with thorough internal investigations** (vs. 75 percent for all industries) and 88 percent assert that **employees at their organizations view risk management processes as being effective** (vs. 76 percent for all industries).

TMT companies are not at the forefront in the adoption of **brand ambassadors and social media influencers**—only 5 percent of those organizations say they always use them, vs. 9 percent in all industries—but neither has the industry ruled them out; the TMT industry is the least likely of all industries to say it never uses influencers (16 percent vs. 22 percent for all industries).

The TMT sector has been more aggressive, however, in its adoption of **cryptocurrency**. This industry is less likely than any other to report having no plans to use crypto (9 percent vs. 19 percent for all industries). And while the share of TMT companies actively using cryptocurrency is roughly average (26 percent vs. 28 percent for all industries), the percentage of them that have established cryptocurrency pilot programs is larger than in any other industry (40 percent vs. 31 percent).

In considering the future, the TMT industry's outlook is notable for the threats about which it has a lower-than-average level of concern. TMT companies are less likely than those in any other industry to be concerned about the possibility of a **significant financial crisis** (57 percent vs. 69 percent for all industries). They are also notably less likely than average to be concerned about the effects of either **military conflict** (41 percent vs. 51 percent for all industries) or **disruptions caused by artificial intelligence or other technologies** (47 percent vs. 56 percent for all industries).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	40%	39%	▲ 1%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	40%	27%	▲ 13%
Fraud by external parties	40%	28%	▲ 12%
Data theft (e.g., customer records)	31%	29%	▲ 2%
Adversarial social media activity	26%	27%	▼ -1%
IP theft (e.g., trade secrets)	26%	24%	▲ 2%
Reputational damage due to third-party relationship	17%	29%	▼ -12%
Fraud by internal parties	17%	27%	▼ -10%
Bribery and corruption	16%	23%	▼ -7%
Money laundering	14%	16%	▼ -2%
Counterfeiting or gray market activity	9%	17%	▼ -8%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Government influence on a vendor, partner, customer or other entity with which your company does business	62%	51%	▲ 11%
New tariffs or trade wars	55%	54%	▲ 1%
Changes in economic treaties between countries	55%	51%	▲ 4%
Political unrest	55%	49%	▲ 6%
Restrictions on foreign investment	48%	47%	▲ 1%
Newly imposed sanctions against doing business with a government, entity or person	45%	47%	▼ -2%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
IP theft (e.g., trade secrets)	84%	72%	▲ 12%
Data theft (e.g., customer records)	81%	76%	▲ 5%
Reputational damage due to third-party relationship	78%	73%	▲ 5%
Fraud by external parties	76%	68%	▲ 8%
Leaks of internal information	74%	73%	▲ 1%
Money laundering	72%	62%	▲ 10%
Fraud by internal parties	69%	66%	▲ 3%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	67%	62%	▲ 5%
Adversarial social media activity	67%	63%	▲ 4%
Counterfeiting or gray market activity	62%	58%	▲ 4%
Bribery and corruption	57%	62%	▼ -5%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

Large-scale, coordinated cyberattacks	71%	68%	▲ 3%
Political instability	60%	63%	▼ -3%
A significant financial crisis	57%	69%	▼ -12%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	57%	61%	▼ -4%
Market manipulation through fake news	57%	59%	▼ -2%
Climate change	52%	54%	▼ -2%
Disruptions caused by artificial intelligence or other technologies	47%	56%	▼ -9%
Destabilization of fiat currency due to cryptocurrency	47%	53%	▼ -6%
Military conflict	41%	51%	▼ -10%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	31%	28%	▲ 3%
Customers/suppliers	16%	13%	▲ 3%
External audit	14%	17%	▼ -3%
Regulator/law enforcement	14%	13%	▲ 1%
By management at our company	13%	16%	▼ -3%
Whistleblower	11%	13%	▼ -2%
Don't know/does not apply	0%	1%	▼ -1%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	88%	81%	▲ 7%
Data analytics	86%	77%	▲ 9%
Compliance (regulatory, codes of conduct, etc.)	81%	75%	▲ 6%
Anti-money laundering controls	79%	69%	▲ 10%
Whistleblowing	78%	66%	▲ 12%
Due diligence of third-party reputation and practices	74%	73%	▲ 1%
Monitoring social media for adversarial activity	74%	71%	▲ 3%
Anti-bribery and anti-corruption controls	72%	69%	▲ 3%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

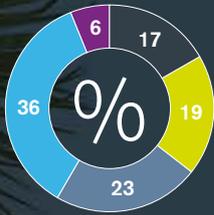
Customers	98%	88%	▲ 10%
Business partners	93%	92%	▲ 1%
Suppliers	91%	92%	▼ -1%
Board or senior executive candidates	91%	91%	■ 0%
Investors	91%	84%	▲ 7%
Potential M&A targets	88%	89%	▼ -1%
Brand ambassadors/influencers	84%	85%	▼ -1%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	88%	78%	▲ 10%
Employees view risk management processes as being effective.	88%	76%	▲ 12%
Serious breaches of risk management processes are met with thorough internal investigations.	86%	75%	▲ 11%
Our risk management processes are adapted to local market and cultural nuances.	86%	72%	▲ 14%
Risk management programs are designed with input from those who must conform to them.	84%	74%	▲ 10%
New business initiatives are regularly examined for all appropriate risk implications.	84%	74%	▲ 10%
The company responds to risk management incidents in a consistent way.	81%	75%	▲ 6%
Performance goals and incentives do not conflict with risk management practices.	76%	71%	▲ 5%

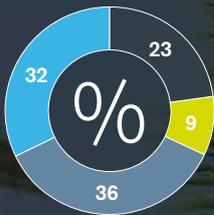


USE OF BRAND "INFLUENCERS"



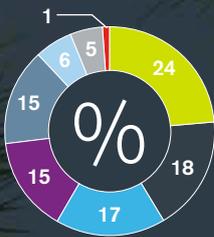
- Never
- Occasionally
- Sometimes
- Frequently
- Always

ADOPTION OF CRYPTOCURRENCY



- No plans to use
- Investigating
- Pilot program
- Actively using

WHO WERE THE PERPETRATORS OF INCIDENTS?



- Third parties (e.g., joint venture partners, suppliers/vendors)
- Employees
- Contractors
- Competitors
- Customers
- Politically motivated actors
- Unknown/random actor
- Don't know/does not apply

Transportation, Leisure and Tourism

Our survey suggests that the transportation industry has a heightened susceptibility to **bribery and corruption**. Within this industry (which in our survey also includes leisure and tourism), 36 percent of respondents report that their organizations have experienced significant incidents of bribery and corruption in the past year—a far higher percentage than in any other industry and one that substantially exceeds the 23 percent average across all industries. However, only 64 percent of industry respondents say they have prioritized combating it (vs. 62 percent for all industries). Perhaps this is because transportation industry respondents are currently more likely than average to view their **anti-bribery and anti-corruption controls** as effective (74 percent vs. 69 percent for all industries).

One way in which the industry can attempt to mitigate bribery and corruption is through its corporate culture. Transportation is on par with other industries in agreeing that there is a clear **message from the top of their organizations that integrity, compliance and accountability are important** (79 percent vs. 78 percent for all industries). However, transportation respondents are far less likely than those from any other industry to assert that, in their organizations, **performance goals and incentives do not conflict with risk management practices** (58 percent vs. 71 percent for all industries). Respondents from this industry are also the least likely to concur that **new business initiatives are regularly examined for appropriate risk implications** (62 percent vs. 74 percent for all industries). The combination of these two findings—personal performance pressure that can supersede internal controls combined with insufficient attention to risk at the strategic level—can easily create an environment hospitable to bribery and corruption. This situation can be expected to be even worse in regions that have a high baseline level of corrupt behavior along with insufficient regulation and enforcement.

The industry's need for more robust internal controls can also be seen in how its incidents are detected. In no other industry are risk incidents more likely to be revealed by **external audit** (22 percent, matching the financial services industry, vs. 17 percent for all industries) or by **whistleblowers** (16 percent vs. 13 percent overall). Having a strong framework to encourage and protect whistleblowers is important, but it is also crucial to note that employees usually resort to whistleblowing when they have little confidence that they will get results through less disruptive channels.

The transportation industry—presumably led in this case by its leisure and tourism components—has actively embraced the use of **brand ambassadors and social media influencers**. Transportation respondents are more likely than people in any other industry to say their organizations frequently follow this communications strategy (36 percent vs. 23 percent for all industries). But the double-edged nature of social media is also evident: 34 percent of transportation respondents report having faced **adversarial social media activity** within the past year (vs. 27 percent for all industries).

RISK LANDSCAPE

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH INCIDENTS HAVE SIGNIFICANTLY AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?			
Leaks of internal information	40%	39%	▲ 1%
Bribery and corruption	36%	23%	▲ 13%
Reputational damage due to third-party relationship	34%	29%	▲ 5%
Adversarial social media activity	34%	27%	▲ 7%
Data theft (e.g., customer records)	34%	29%	▲ 5%
Fraud by external parties	34%	28%	▲ 6%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	32%	27%	▲ 5%
Fraud by internal parties	30%	27%	▲ 3%
IP theft (e.g., trade secrets)	28%	24%	▲ 4%
Counterfeiting or gray market activity	21%	17%	▲ 4%
Money laundering	15%	16%	▼ -1%

WHICH GEOPOLITICAL RISKS HAVE AFFECTED YOUR ORGANIZATION IN THE LAST YEAR?

(Percent responding "affected" or "very affected")

Government influence on a vendor, partner, customer or other entity with which your company does business	58%	51%	▲ 7%
New tariffs or trade wars	53%	54%	▼ -1%
Political unrest	53%	49%	▲ 4%
Changes in economic treaties between countries	51%	51%	■ 0%
Restrictions on foreign investment	49%	47%	▲ 2%
Newly imposed sanctions against doing business with a government, entity or person	49%	47%	▲ 2%

RISK STRATEGY

ISSUE	INDUSTRY	GLOBAL	(+/-)
WHICH RISKS ARE PRIORITIES FOR YOUR ORGANIZATION?			
(Percent responding "significant priority" or "high priority")			
Leaks of internal information	79%	73%	▲ 6%
IP theft (e.g., trade secrets)	77%	72%	▲ 5%
Data theft (e.g., customer records)	77%	76%	▲ 1%
Fraud by external parties	75%	68%	▲ 7%
Fraud by internal parties	74%	66%	▲ 8%
Reputational damage due to third-party relationship	72%	73%	▼ -1%
Bribery and corruption	64%	62%	▲ 2%
Disruption due to sanctions, tariffs, changes in trade agreements, etc.	62%	62%	■ 0%
Money laundering	62%	62%	■ 0%
Adversarial social media activity	60%	63%	▼ -3%
Counterfeiting or gray market activity	57%	58%	▼ -1%

LOOKING AHEAD FIVE YEARS, WHAT RISKS CONCERN YOU?

(Percent "concerned" or "very concerned")

A significant financial crisis	66%	69%	▼ -3%
A breakdown of intergovernmental mechanisms for dispute resolution, free trade, combating corruption, etc.	64%	61%	▲ 3%
Political instability	62%	63%	▼ -1%
Market manipulation through fake news	58%	59%	▼ -1%
Climate change	57%	54%	▲ 3%
Large-scale, coordinated cyberattacks	55%	68%	▼ -13%
Destabilization of fiat currency due to cryptocurrency	53%	53%	■ 0%
Military conflict	53%	51%	▲ 2%
Disruptions caused by artificial intelligence or other technologies	45%	56%	▼ -11%

RISK MANAGEMENT IN PRACTICE

ISSUE	INDUSTRY	GLOBAL	(+/-)
HOW WERE INCIDENTS DISCOVERED?			
Internal audit	25%	28%	▼ -3%
External audit	22%	17%	▲ 5%
Whistleblower	16%	13%	▲ 3%
By management at our company	15%	16%	▼ -1%
Regulator/law enforcement	11%	13%	▼ -2%
Customers/suppliers	11%	13%	▼ -2%
Don't know/does not apply	1%	1%	■ 0%

HOW EFFECTIVE WERE THE FOLLOWING IN DETECTING INCIDENTS? (Percent responding "effective" or "very effective")

Cybersecurity	85%	81%	▲ 4%
Monitoring social media for adversarial activity	79%	71%	▲ 8%
Data analytics	74%	77%	▼ -3%
Anti-bribery and anti-corruption controls	74%	69%	▲ 5%
Compliance (regulatory, codes of conduct, etc.)	72%	75%	▼ -3%
Anti-money laundering controls	70%	69%	▲ 1%
Whistleblowing	70%	66%	▲ 4%
Due diligence of third-party reputation and practices	68%	73%	▼ -5%

ON WHOM DO YOU CONDUCT REPUTATIONAL DUE DILIGENCE?

Board or senior executive candidates	94%	91%	▲ 3%
Suppliers	90%	92%	▼ -2%
Business partners	90%	92%	▼ -2%
Customers	87%	88%	▼ -1%
Potential M&A targets	85%	89%	▼ -4%
Brand ambassadors/influencers	84%	85%	▼ -1%
Investors	82%	84%	▼ -2%

HOW DOES YOUR ORGANIZATION SUPPORT A CULTURE OF INTEGRITY? (Percent agreeing or strongly agreeing)

There is a clear message from the top of the organization that integrity, compliance and accountability are important.	79%	78%	▲ 1%
Risk management programs are designed with input from those who must conform to them.	79%	74%	▲ 5%
Employees view risk management processes as being effective.	77%	76%	▲ 1%
Serious breaches of risk management processes are met with thorough internal investigations.	75%	75%	■ 0%
The company responds to risk management incidents in a consistent way.	72%	75%	▼ -3%
Our risk management processes are adapted to local market and cultural nuances.	66%	72%	▼ -6%
New business initiatives are regularly examined for all appropriate risk implications.	62%	74%	▼ -12%
Performance goals and incentives do not conflict with risk management practices.	58%	71%	▼ -13%

Contact

NORTH AMERICA

BOSTON

Daniel Linskey
+1 617 210 7471
daniel.linskey@kroll.com

CHICAGO

Baltazar Vallenilla
+1 312 415 1579
bvallenilla@kroll.com

DALLAS

Terry Orr
+1 469 547 3906
terry.orr@kroll.com

HOUSTON

Mike Schwartz
+1 713 392 8761
michael.schwartz@kroll.com

LOS ANGELES

Jason Smolanoff
+1 213 443 6055
jason.smolanoff@kroll.com

NASHVILLE

Brian Lapidus
+1 615 577 6770
blapidus@kroll.com

NEW YORK

Rich Plansky
+1 212 523 0590
richard.plansky@kroll.com

PHILADELPHIA

Mark Ehlers
+1 215 568 8305
mehlers@kroll.com

RESTON

Mari Davies-DeMarco
+1 703 860 0190
mdavies-demarco@kroll.com

SAN FRANCISCO

Betsy Blumenthal
+1 415 693 5360
bblument@kroll.com

TORONTO

Peter McFarlane
+1 416 813 4401
pmcfarlane@kroll.com

WASHINGTON, DC

Nicole Lamb-Hale
+1 20 2649 1272
nicole.lamb-hale@kroll.com

LATIN AMERICA

BOGOTÁ

Pablo Iragorri
+57 1 742 5556
pablo.iragorri@kroll.com

BUENOS AIRES

Juan Cruz Amirante
+54 11 4706 6024
jcamirante@kroll.com

GRENADA

Glen Harloff
+1 473 439 7999
gharloff@kroll.com

MEXICO CITY

Brian Weihs
+52 55 5279 7250
bweihs@kroll.com

MIAMI

James Faulkner
+1 305 789 7130
jfaulkner@kroll.com

SÃO PAULO

Fernanda Barroso
+55 11 3897 0900
fernanda.barroso@kroll.com

EMEA

AMSTERDAM

Rens Rozekrans
+31 208 515 108
rens.rozekrans@kroll.com

DUBAI

Amine Antari
+971 4 449 6720
amine.antari@kroll.com

DUBLIN

Kevin Hart
+353 1 472 0801
kevin.hart@kroll.com

LONDON

Neil Kirton
+44 20 70 29 5204
nkirton@kroll.com

MADRID

Marcelo Correia
+34 910 389 051
marcelo.correia@kroll.com

MILAN

Marianna Vintiadis
+39 02 0066 7901
mvintiadis@kroll.com

MOSCOW

Alex Volcic
+7 495 969 2898
avolcic@kroll.com

PARIS

Béchr Mana
+33 1 4267 8146
bmana@kroll.com

RIYADH

Sultana El Sayed
+966 11 2118 148
sel-sayed@kroll.com

ZURICH

Louis-David Magnien
+44 207 029 8527
louis-david.magnien@kroll.com

APAC

BEIJING

Calvin Dong
+86 10 5964 7656
cdong@kroll.com

HONG KONG

Violet Ho
+852 2884 7777
vho@kroll.com

TOKYO

Hiroki Katayama
+81 33509 7127
hiroki.katayama@kroll.com

MELBOURNE

Mark Jones
+61 416 058 297
mark.jones@kroll.com

MUMBAI

Tarun Bhatia
+91 22 6294 8166
tarun.bhatia@kroll.com

SINGAPORE

Reshmi Khurana
+65 6645 4527
rkhurana@kroll.com

SHANGHAI

Sarah Zheng
+86 21 6156 1713
sarah.zheng@kroll.com

SYDNEY

Cem Ozturk
+61 434 005 518
cozturk@kroll.com





ABOUT KROLL, A DIVISION OF DUFF & PHELPS

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cybersecurity, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cybersecurity, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com