KPMG

A triple threat across the Americas

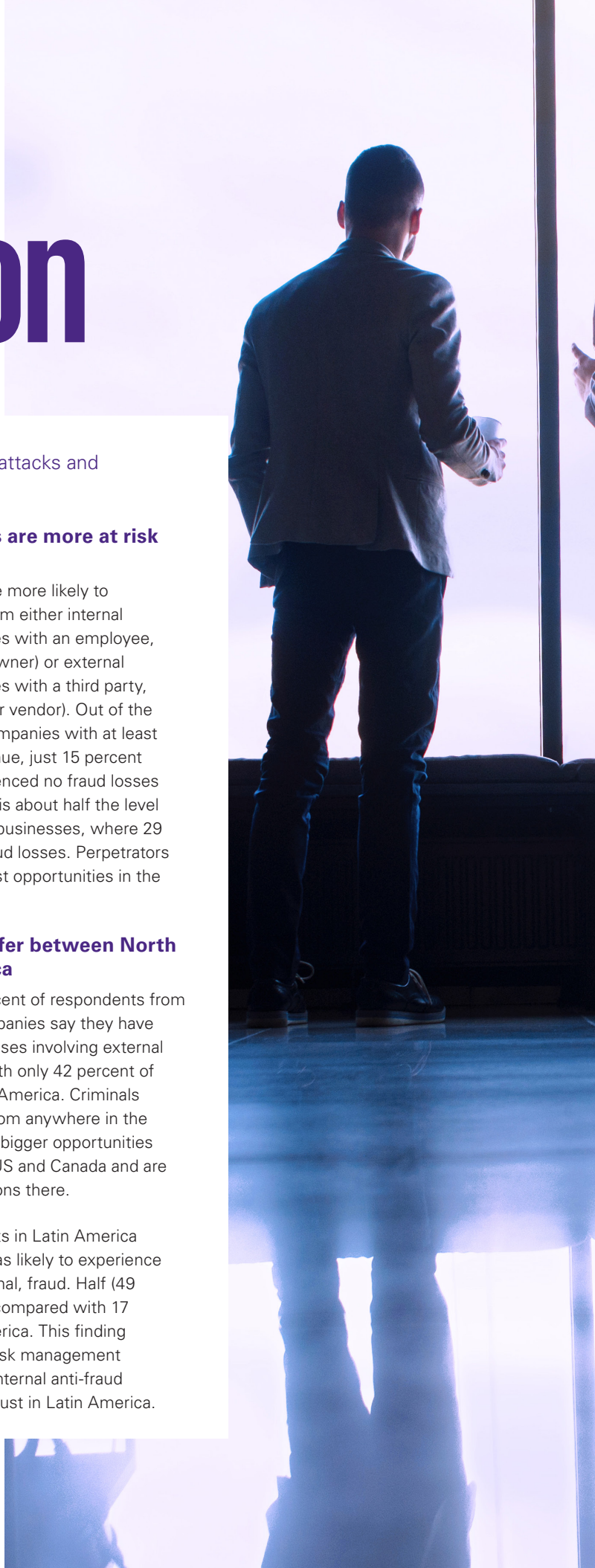
2022 KPMG Fraud Outlook

January 2022

kpmg.com

Contents

Introduction



KPMG[1] is pleased to present its 2022 outlook on fraud, cyber attacks and compliance concerns across the Americas.

Our survey of more than 600 executives across multiple industries confirms anecdotal evidence about the effects of the pandemic on these three interconnected threats: it reveals that fraud, compliance concerns and cyber attacks are common, have increased in severity — and are expected to become more frequent.

Are companies in the Americas managing to fend off this triple threat? This research suggests that many have limited defenses in place, and the shift to hybrid or remote working is making existing controls less effective.

The majority of companies across North and Latin America reported that they have suffered losses from fraud, compliance breaches, and/or cyber attacks

Eighty-three percent of survey respondents say their companies have suffered at least one cyber attack over the past 12 months. Seventy-one percent of respondents say their companies have experienced fraud. And more than half of respondents say their companies have paid regulatory fines or suffered financially due to unmitigated compliance risks.

This all adds up to significant costs. Respondents report an average loss of 1 percent of profits from fraud and compliance-related fines in the last year.

[1]Any reference to KPMG in this report refers to a collaboration among the KPMG member firms across Latin America, the US, and Canada, to produce our research insights.

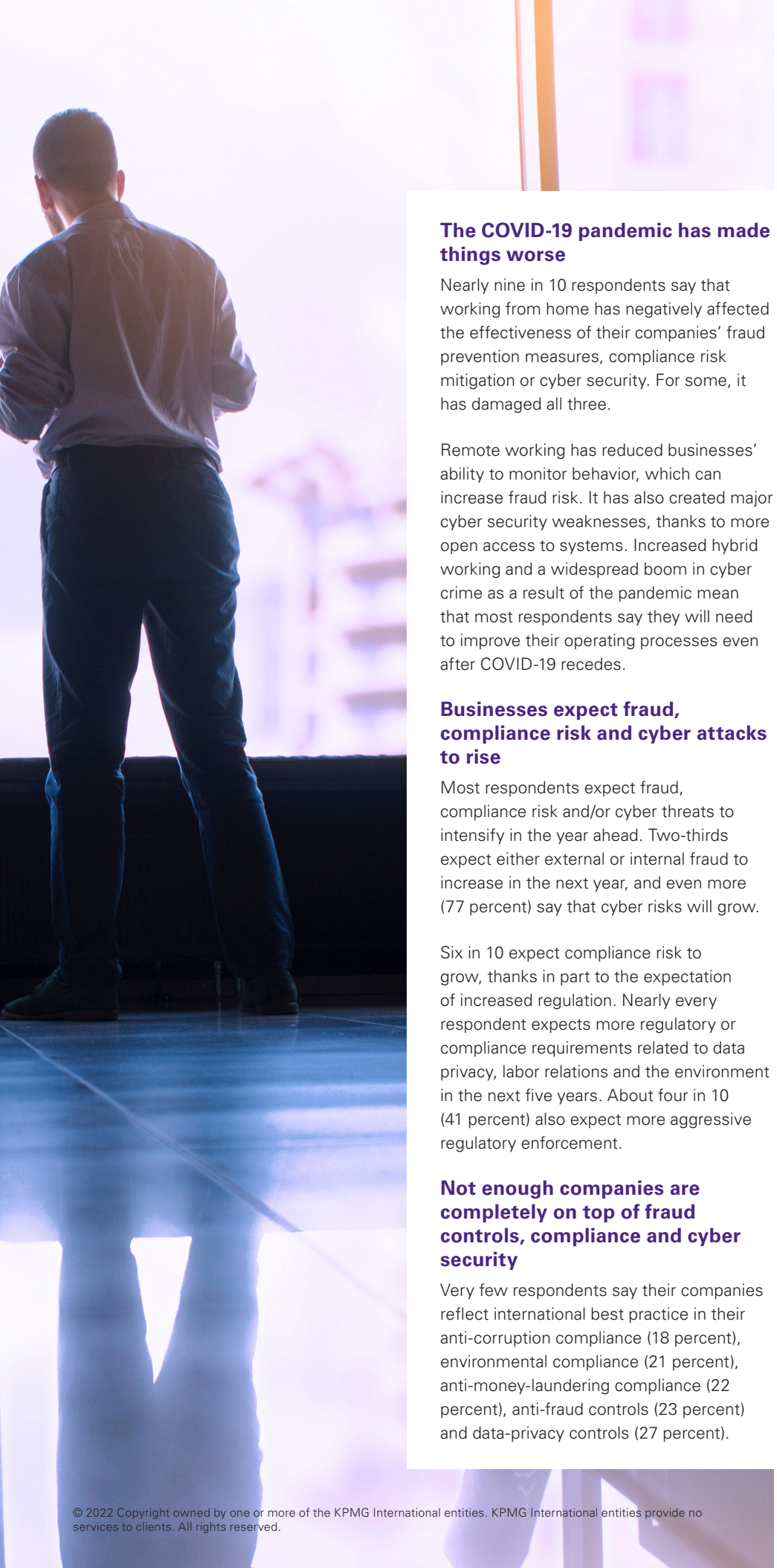
Large companies are more at risk of fraud

Bigger companies are more likely to experience losses from either internal fraud (which originates with an employee, manager, officer or owner) or external fraud (which originates with a third party, such as a customer or vendor). Out of the respondents from companies with at least US$10 billion in revenue, just 15 percent say they have experienced no fraud losses in the past year. This is about half the level seen among smaller businesses, where 29 percent report no fraud losses. Perpetrators clearly see the biggest opportunities in the largest organizations.

Fraud threats differ between North and Latin America

In the survey, 76 percent of respondents from North American companies say they have experienced fraud losses involving external parties, compared with only 42 percent of respondents in Latin America. Criminals operating remotely from anywhere in the world apparently see bigger opportunities at companies in the US and Canada and are focusing their attentions there.

However, respondents in Latin America are more than twice as likely to experience internal, or occupational, fraud. Half (49 percent) report this, compared with 17 percent in North America. This finding suggests that fraud risk management programs and other internal anti-fraud defenses are less robust in Latin America.



The COVID-19 pandemic has made things worse

Nearly nine in 10 respondents say that working from home has negatively affected the effectiveness of their companies' fraud prevention measures, compliance risk mitigation or cyber security. For some, it has damaged all three.

Remote working has reduced businesses' ability to monitor behavior, which can increase fraud risk. It has also created major cyber security weaknesses, thanks to more open access to systems. Increased hybrid working and a widespread boom in cyber crime as a result of the pandemic mean that most respondents say they will need to improve their operating processes even after COVID-19 recedes.

Businesses expect fraud, compliance risk and cyber attacks to rise

Most respondents expect fraud, compliance risk and/or cyber threats to intensify in the year ahead. Two-thirds expect either external or internal fraud to increase in the next year, and even more (77 percent) say that cyber risks will grow.

Six in 10 expect compliance risk to grow, thanks in part to the expectation of increased regulation. Nearly every respondent expects more regulatory or compliance requirements related to data privacy, labor relations and the environment in the next five years. About four in 10 (41 percent) also expect more aggressive regulatory enforcement.

Not enough companies are completely on top of fraud controls, compliance and cyber security

Very few respondents say their companies reflect international best practice in their anti-corruption compliance (18 percent), environmental compliance (21 percent), anti-money-laundering compliance (22 percent), anti-fraud controls (23 percent) and data-privacy controls (27 percent).

Looking specifically at how respondents say their companies perform across a series of measures relating to fraud control, compliance and cyber security, we found that only a small proportion report strong controls across at least half of the relevant measures (which we call the 'half-or-more' standard). Just 24 percent of respondents say their companies are strong in half or more of the relevant cyber security protections, 17 percent in controls to prevent and detect fraud, and 13 percent in addressing compliance risks. Only 4 percent say that their company excels in all three areas.

Companies have urgent priorities

Fraud:

Never discount the possibility of an inside job. A significant 31 percent of respondents say their companies have suffered from fraud perpetrated by an insider in the past year.

Compliance:

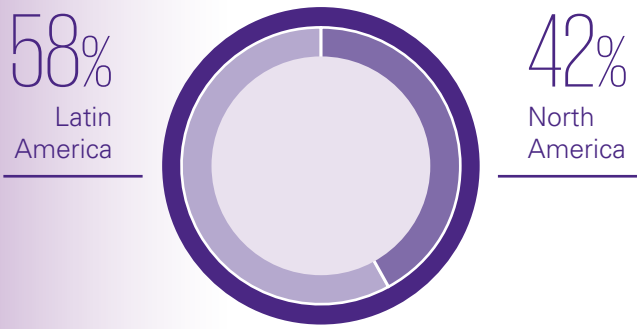
Compliance is now a reputational issue. More respondents say that reputational considerations cause their leaders to pay attention to compliance than say the same of fines and enforcement.

Cyber security:

Slow and steady will not win the cyber security race. Respondents tell us it takes about a month, on average, for a cyber attack to be fully contained, and most seem satisfied with how well their companies do in this area. This indicates that there is a potentially fatal lack of urgency.

Aboutthereserarch

This study is based on a survey of 642 executives:



They are roughly evenly divided across seven industries:

Industrial manufacturing

Consumer products and retail

Energy and natural resources

Financial services

Insurance

Life sciences and pharmaceutical

Telecoms, media and entertainment and technology

The sample is predominantly composed of senior leadership: **more than half of respondents are board members, members of the C-suite, or heads of departments**.

About the research (continued)

Their companies are a range of sizes:

have annual revenues of **less than US$1 billion**

have annual revenues of between **US$1 billion and US$10 billion**

have annual revenues of **more than US$10 billion**

We also interviewed six senior corporate leaders and experts from across the region:

José Calderón
Chief Global Auditing Officer, Grupo Bimbo

Larissa Galimberti
Partner, Pinheiro Neto Advogados

Carlos García Jiménez
Regional Director of Ethics and Compliance LATAM, Uber

Ariel Nowersztern
Cybersecurity Specialist, Inter-American Development Bank

Beth Rose
Chief Compliance, Ethics and Integrity Officer, Ford Motor Company

Pascal Saint-Amans
Director, Center for Tax Policy and Administration, Organisation for Economic Co-operation and Development

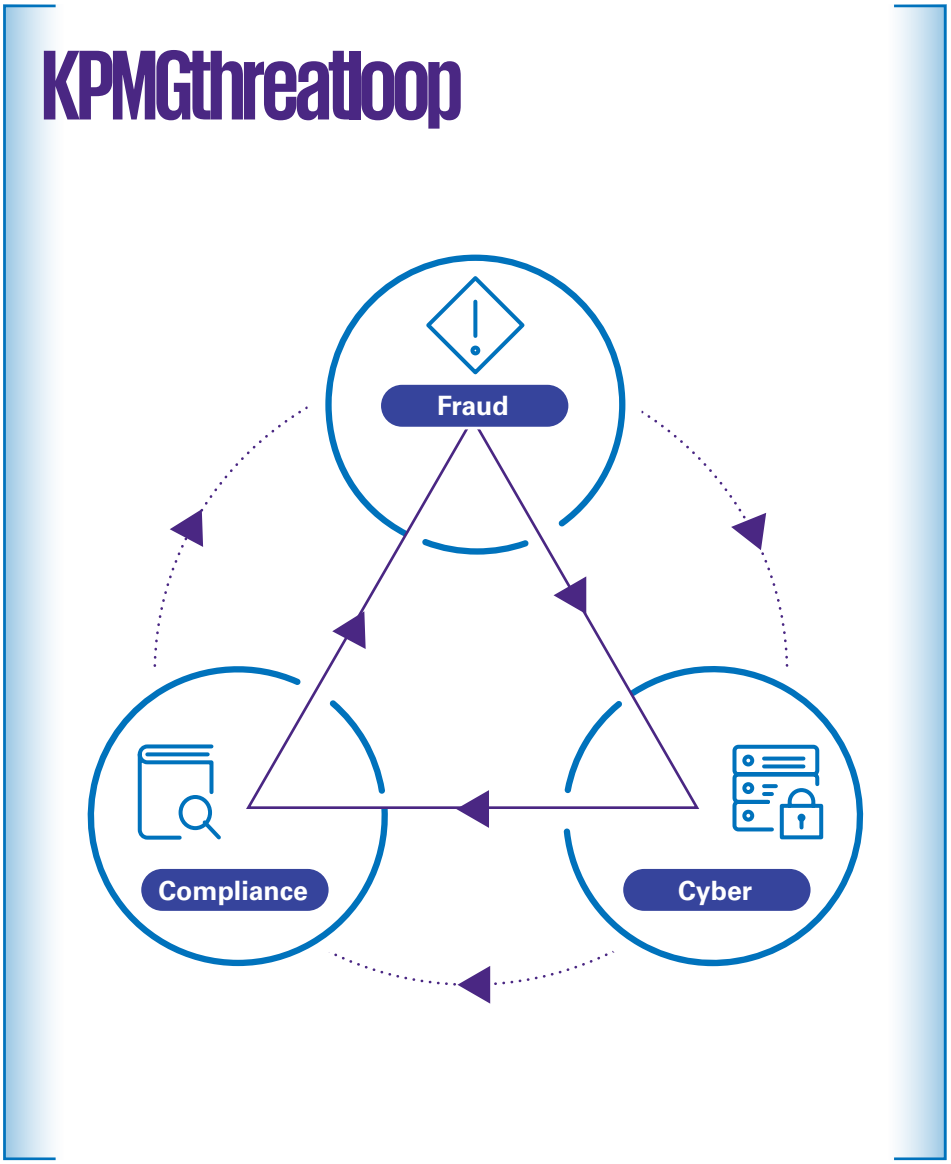
We would like to thank them for sharing their insights.

A united defense against a triple threat

Fraud, compliance risks and cyber attacks are widespread, growing dangers for companies across North and Latin America.

And these threats are intertwined. Consider, for example, the case of an employee stealing client data from their company while working from home — this raises all three threats simultaneously, and companies need to address them as one.

Companies need to mitigate what KPMG calls the 'threat loop,' which comprises the triple threat of fraud, compliance risk and a growing array of cyber security threats. Defending against this threat loop requires a collective, interconnected effort. Companies need to look at the impact created by these threats in conjunction, rather than just the risks they pose in isolation.



Ariel Nowersztern, a Cybersecurity Specialist at the Inter-American Development Bank (IDB), says that some companies are already developing holistic defenses against these risks. "You can use any one of cyber security, internal control and auditing to improve the effectiveness of the others," he explains.

Some companies have combined the monitoring of physical and digital assets with anti-fraud and other internal controls. An alert in one area could tell you that something is wrong in another.

To find out whether companies are ready to respond to this threat loop, and how much work they need to do if they are not ready, we surveyed senior executives across North and Latin America. This report looks at what they told us and asks: Are companies in the Americas prepared?

> "You can use any one of cyber security, internal control and auditing to improve the effectiveness of the others
>
> **Ariel Nowersztern**
> Cybersecurity Specialist at the Inter-American Development Bank

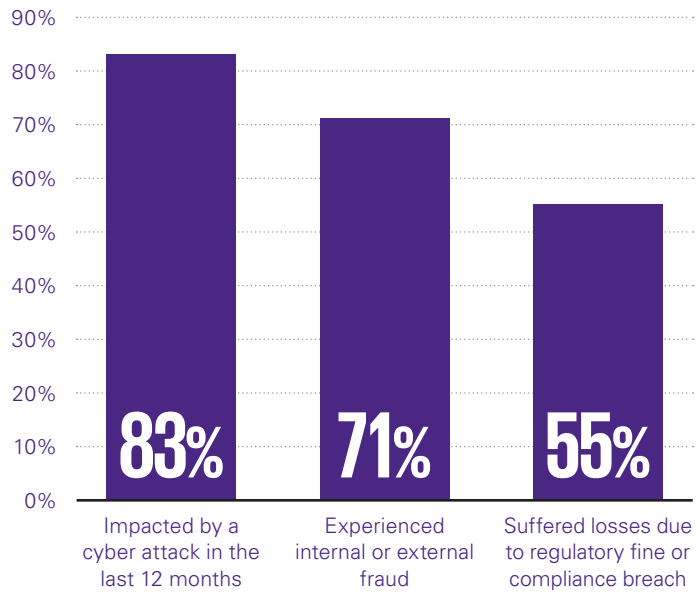
Fraud, non-compliance and cyberbreaches are the costly norm

“It is now a case of *when* a cyber attack will happen, not *if*,” says Larissa Galimberti, a Partner specializing in technology issues at Brazilian law firm Pinheiro Neto Advogados. Our survey respondents agree that, for companies in the Americas, attempted fraud and compliance gaps are inevitable.

Of the risks that we examined, respondents indicated that their companies are most likely to have experienced cyber attacks. Overall, 83 percent of those surveyed across the Americas say that their companies have suffered at least one cyber attack over the past 12 months. The survey asked respondents to comment only on incidents that had a noticeable business impact, so the overall number of cyber attacks is likely to be higher than reported.

Fraud is also cited with worrying frequency; as many as 71 percent of respondents report that their companies uncovered fraud over the past 12 months. This rises to 85 percent of companies with over $10 billion in annual revenues. Meanwhile, 55 percent of respondents also acknowledge that their businesses have paid regulatory fines or suffered financially due to compliance violations in the past year. Undiscovered instances of fraud and non-compliance mean that these numbers are likely to be unrepresentative and the underlying problem may be even larger.

The reality of the triple threat



Respondents reported that their companies had an average combined loss from fraud, compliance issues and regulatory fines of 1 percent of their profits. Moreover, 58 percent of respondents said that their companies had suffered a direct economic loss from a cyber attack.

Meanwhile, 20 percent of respondents reported that their companies had suffered reputational damage, and 32 percent reported that their companies had to deal with a compliance investigation. These incidents can pose an existential threat, Nowersztern warns, especially for smaller companies. A substantial loss of capital, a severely damaged reputation, or even the exposure of key operational information (such as client lists) can all cause a company to fold.

Costs in these areas grow with the size of the business. Respondents from large companies (defined here as those with annual revenues of over $10bn) say that, on average, their companies lost 0.7 percent of net profits to fraud last year and paid 0.8 percent of net profits as fines for non-compliance, for an aggregate of 1.5 percent.

Beth Rose, Chief Compliance, Ethics and Integrity Officer at Ford Motor Company, stresses that such figures are not the only reason why compliance, fraud prevention and cyber security are important to corporations. At good companies, reputation and probity are crucial considerations. Equally, though, costs of this magnitude will matter to companies and their stakeholders. "Executives are naturally inclined to look at the economic impact," says Rose.

Carlos García Jiménez, Regional Director of Ethics and Compliance LATAM at Uber, agrees, pointing out that effective protection against these risks "costs a fraction of" the benchmarked average losses for all companies.

Regional fraud differences and why size matters

On the surface, North and Latin American respondents report markedly different fraud incidences, as shown here.

Comparing fraud across North and Latin America

Two observations are worth noting. First, respondents indicate that fraud is a more widespread problem for North American companies. Second, the risk environment differs between regions. Latin American companies are nearly twice as likely as their North American counterparts to report insider involvement in fraud. In North America, external fraud is a much bigger issue.

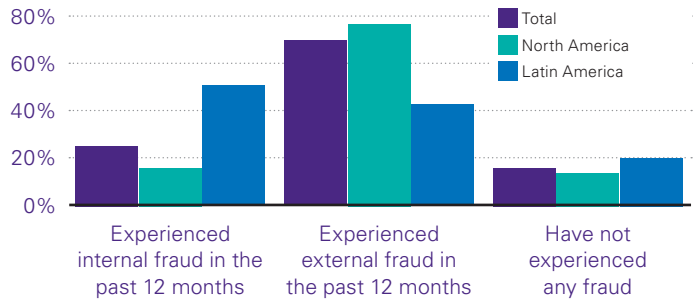
1.5 percent: the percentage of profits large companies are losing due to fraud and non-compliance

These figures, however, are likely affected by the sharp variation in average company size between the two regions. Most North American businesses that we surveyed are considerably larger, with median annual revenues of $2.9bn, compared to $846m for those in Latin America. Our survey also shows that larger, richer companies are more often targeted by external fraud.

Comparing fraud across size of company

But how much of the apparent regional differences are due to company size? An answer comes from comparing just the largest companies — those with revenues of $10bn or more — in each part of the Americas.

Comparing fraud across companies with at least $10bn in annual revenue



When comparing the respondents from big companies by region, the figures for those affected by any fraud converge. The gap between the proportion of all North American companies experiencing any fraud (77%) and the same population in Latin America (67%) is 10 percentage points. However, among respondents from larger companies, 86 percent in North America reported some fraud in the last 12 months, as compared to 80 percent in Latin America — a noticeably smaller difference.

The results for different types of fraud, however, diverge markedly. Among those surveyed at large Latin American companies, 49 percent say that at least one internal fraud had occurred in the past year, almost three times the rate in North America. This suggests that, while companies in North America are far from immune from internal fraud, Latin American companies should prioritize the implementation of internal controls to address the risk of internal fraud.

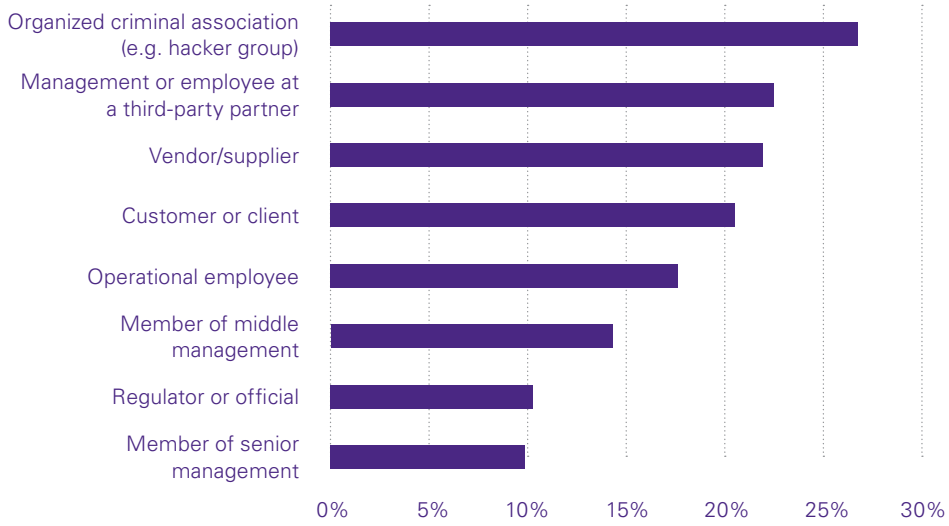
What to make, though, of the much larger percentage of North American companies that have experienced external fraud (76 percent, as compared to 42 percent in Latin America)? A likely explanation lies in the divergent experience of cyber crime. Of the respondents in large companies in Latin America, only 7 percent report a cyber attack in the past year. For North America, a staggering 43 percent of respondents experienced a cyber attack in the last year.

As well as having higher revenues, Nowersztern suggests these North American targets are more digitalized and therefore have greater exposure. Alternatively, they may be better at detecting when a cyber attack occurs, so the real rates of attempted incursion at North American and Latin American companies may be closer than reflected in the responses.

It is clear that North American companies need better cyber defenses, but Latin American companies cannot be complacent; as they grow, they will likely become bigger targets for cyber attacks.

Data Snapshot I: A flock of fraudsters

Which of the following types of individuals are known to have been involved in fraud or misconduct (either alone or in collusion) at your company during the past 12 months?

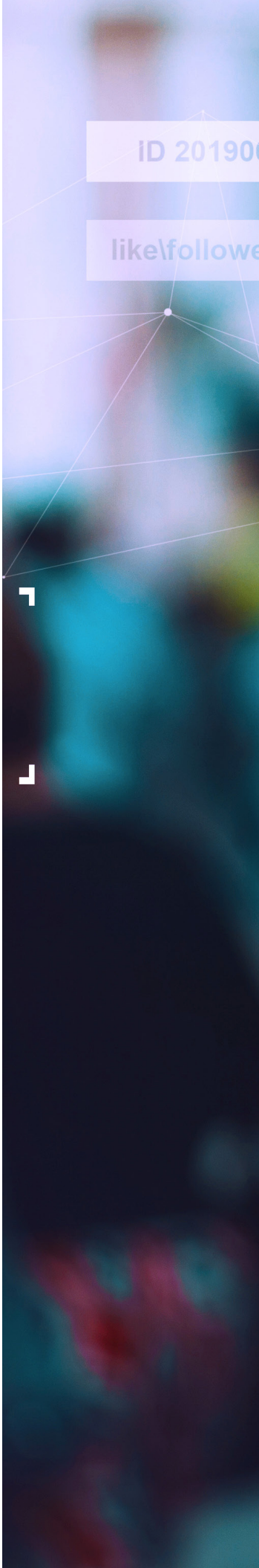


Companies are vulnerable to a wide range of fraudsters. José Calderón, Chief Global Auditing Officer at Grupo Bimbo, explains that his company has rolled out a global framework to reduce a variety of fraud risks. "All the things that can affect processes, from sourcing of raw material from many suppliers, through production, then to sales and execution," can, he suggests, create a risk of fraud. "Then you also have challenges on compliance and fraud, with internal and external associates, environmental and labor regulations, data privacy — the risk is very extensive."

According to our survey, the kind of criminal who most frequently infiltrates companies — or, at least, is most frequently uncovered — is the external thief, often digitally enabled. Close behind are partners, vendors and suppliers. In those countries where local operations of the company have few controls in place and use a large number of third-party suppliers, the potential for vendor fraud or collusion was correspondingly large.

There is also the internal threat; 31 percent of respondents report that, in the past year, internal fraud (by an employee, manager, officer or owner) had been committed at their companies.

The culprits also vary by region. Among North American respondents, 43 percent cite occurrences of fraud perpetrated by an outside criminal organization (such as a hacker group), compared to just 14 percent in Latin America — consistent with the higher levels of cyber crime in North America. Conversely, 36 percent of Latin American respondents say that their companies experienced internal fraud, compared to just 23 percent of North American respondents.



How the pandemic changed thepicture

The COVID-19 pandemic and resulting lockdowns have complicated the threat environment.

In every area, the risk environment has worsened, while increased remote working has undermined existing defenses. Overall, 86 percent of respondents say that remote working has negatively affected at least one element of fraud prevention, compliance and cyber security programs at their company.

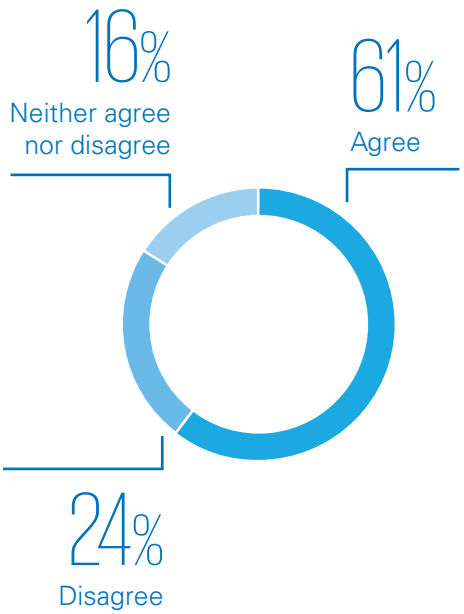
86 percent: proportion of respondents who say that working remotely has negatively affected at least one element of their company's fraud prevention, compliance, or cyber security programs

Fraud prevention

Fraud opportunities within a business are the product of its operations. For example, says Grupo Bimbo's José Calderón, a need to obtain raw materials and spare parts expeditiously creates substantial risks.

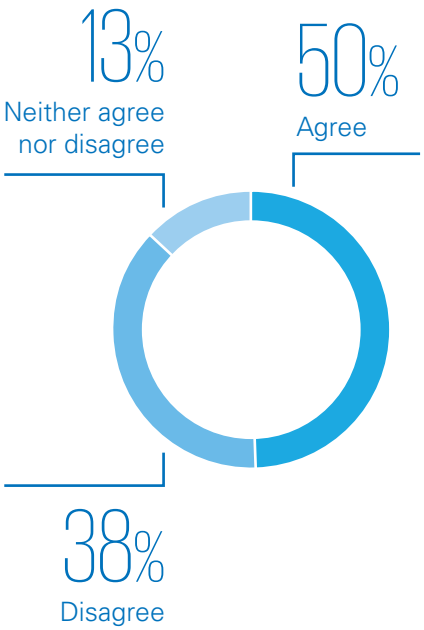
This is because companies are more likely to circumvent existing controls (such as due diligence on third parties) to get access to those materials as quickly as possible. This was a particular risk for many businesses both at the low point of the pandemic and amid supply-chain problems in much of the world in late 2021.

The shift to remote working has increased our risk of fraud due to a reduced ability to monitor and control for fraudulent behavior[2]



[2]Amounts in chart do not total 100 percent due to rounding

Working from home has negatively impacted our ability to respond appropriately to fraud in our business[2]

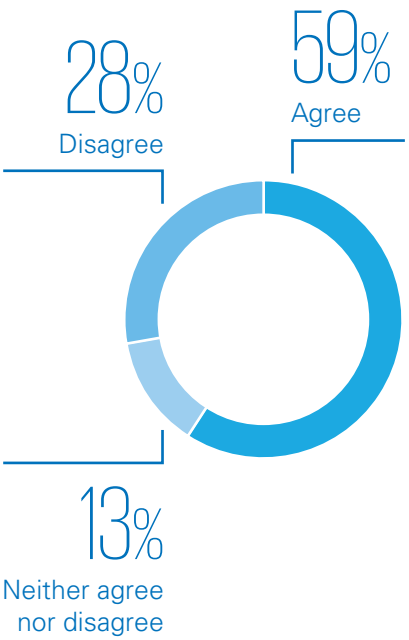


Meanwhile, the rapid increase in remote working also brings challenges for fraud prevention, especially for oversight and investigation; 61 percent of those surveyed indicated increased risk of fraud due to a lowered ability to monitor employee behavior. This is not related to operational employees alone; 28 percent of respondents report that remote work has impeded management controls and supervision. The issue goes beyond employees having a new remote workplace. For example, says Garcia Jiménez, many employees are millennials who share apartments with others not associated with the company. Because of this, ensuring that non-employees are unable to obtain access to company systems became more challenging.

Similarly, half of respondents tell us that working from home has negatively impacted their companies' ability to respond to fraud. Garcia Jiménez notes that even basic fraud controls have had to change. Outside of a normal office environment, investigators no longer have the same level of physical control of a situation. "It's a huge challenge to collect information or retrieve files and emails. Even conducting an interview [is harder]. From a logistical perspective, you need to develop different arrangements than in the past, [not just] reserving a room." Some employees may even be working remotely from another state or country.

These challenges are not likely to recede, with hybrid working expected to be increasingly common. A majority of companies in the Americas remain unready to respond to these risks.

The anti-fraud controls we had in place pre-pandemic have not been effectively updated to reflect the new working reality

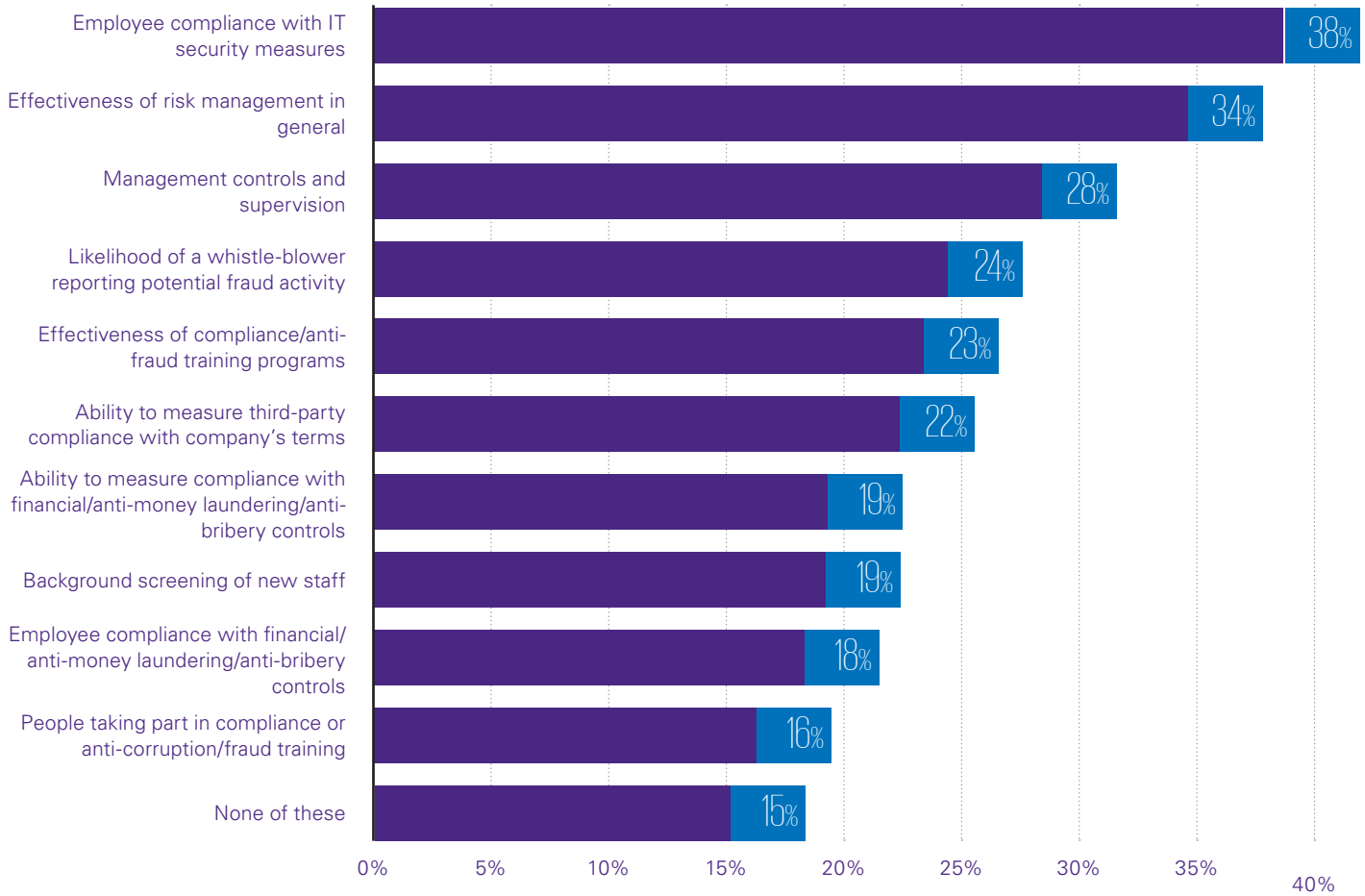


59 percent of respondents agree that the anti-fraud controls they had in place pre-pandemic have not been effectively updated to reflect the new working reality

Compliance

As many as 77 percent of those surveyed say that their companies had to develop new strategies during the pandemic to keep pace with evolving compliance demands. In some cases, this reflected the novel challenges of the situation. Ford Motor Company's Beth Rose recalls that "COVID-19 required a huge shift from every compliance department." The initial question was "How do you comply with health and safety?" Similarly, when Ford began manufacturing ventilators and respirators for the first time, it had to understand and implement compliance requirements related to these products.

Which of the following have been negatively impacted by an increase in employees working from home in the last year?



Remote-working considerations have also played a significant role in compliance. Garcia Jiménez suggests that compliance training saw the biggest impact, with in-person courses shifting online. This is more than a shift in the medium of interaction. For many companies, it required a substantial revision of training materials and development of different communication skills by those leading and learning. The time involved will have forced an extended gap in training for many.

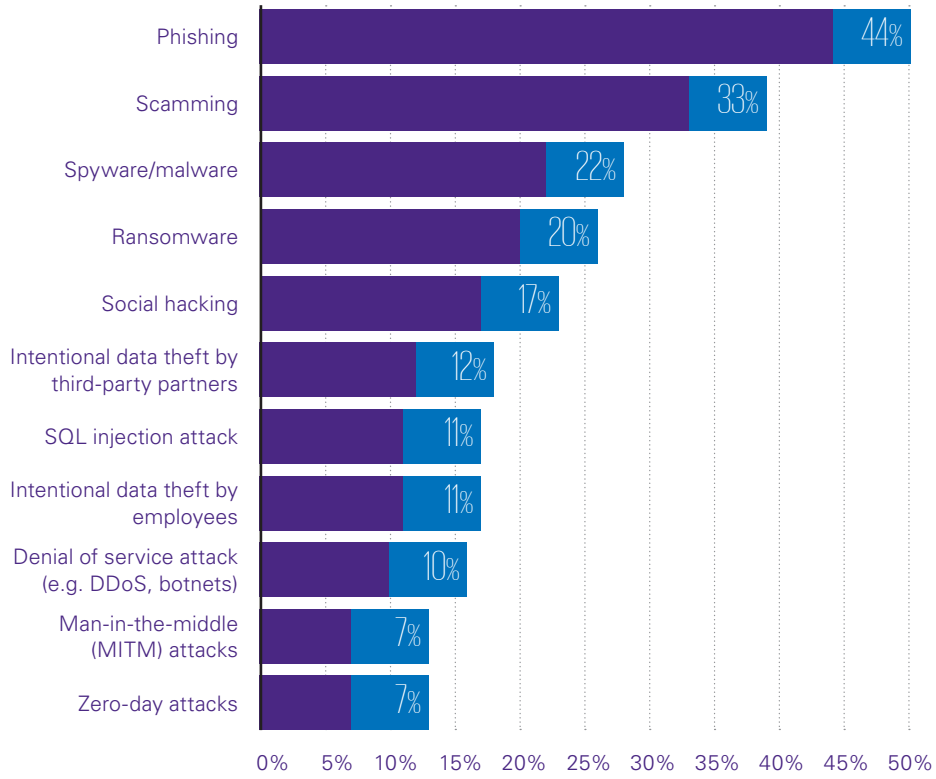
Increased remote working also demanded a substantial cultural change. "Part of compliance is seeing what is happening in order to get a sense of where there might be some risk," says Rose. "When we went virtual, that became an issue." Many respondents agree: 19 percent report that remote working made it more difficult to measure compliance with financial, anti-money laundering and anti-bribery controls.

Adjusting to the new compliance environment remains a work in progress. Rose reports that Ford is planning to continue with its current hybrid-working model. Figuring out the implications for compliance is "the million-dollar question. We have to think differently about training, awareness, teams and risk assessment", she confirms. Different industries will have distinct needs.

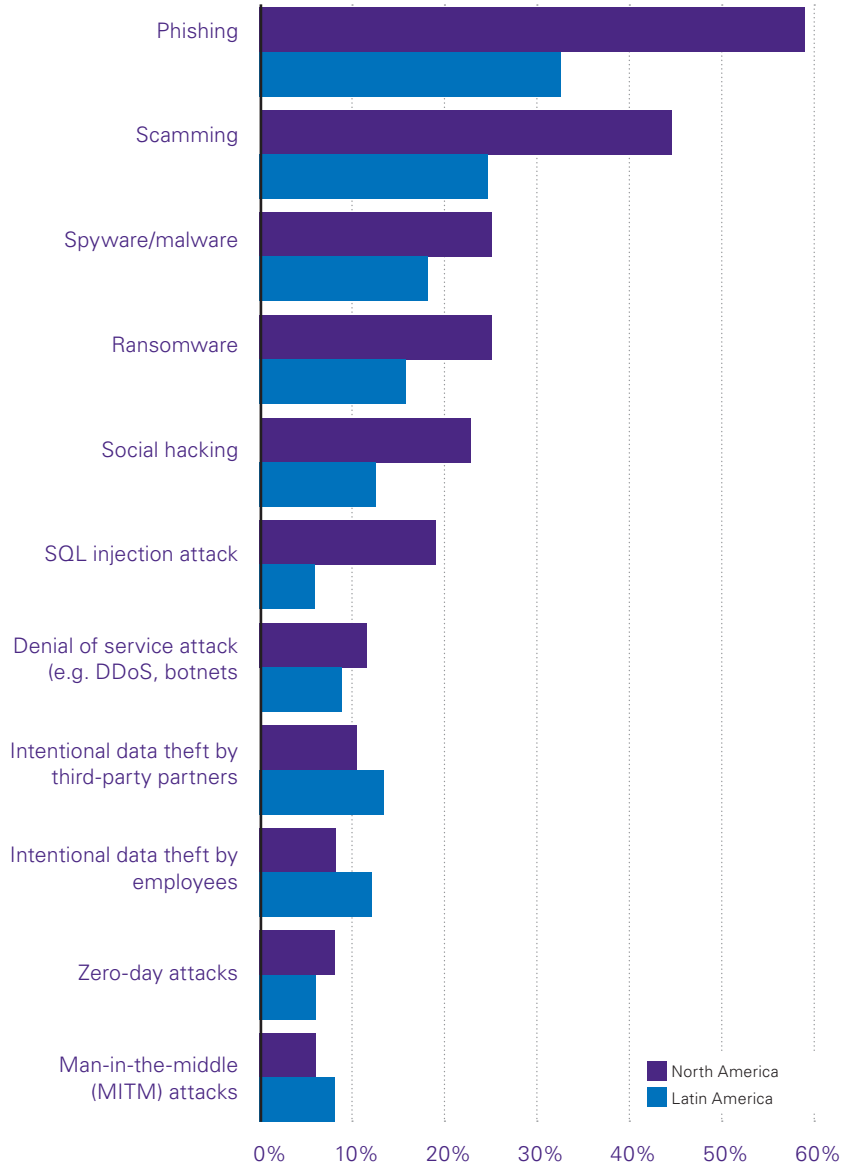
Cyber security

Cyber crime increased in volume during the pandemic and has not abated. As the chart shows, companies surveyed for this report are reporting rises in frequency of various kinds of attacks, with phishing (cited by 44%), scamming (33%), malware (22%), and ransomware (20%), growing challenges for many. Overall, 79 percent of respondents saw growth in at least one of the types of attacks covered in the survey.

For which of the following types of cyber attacks has your company experienced an increase in the last 12 months (if any)?



Comparison by region: of which of the following have you seen an increase in the last year?



Even individual incidents can have a huge impact. As one example, a ransomware attack on a pipeline in May 2021 led to oil shortages in several southern US states. As another example with a substantial effect, Galimberti cites a major data theft that took place in Brazil in early 2021: "Files on 220 million Brazilians were put on the dark web with all kinds of information," she says.

Nowersztern points out that several trends that pre-dated, but were accelerated by, the pandemic helped drive this growth in criminal activity. For example, phishing messages took on topical COVID-19 themes to lure in anxious consumers. Moreover, as companies and society have grown more reliant on digital assets and equipment, he warns, "we are now even more vulnerable than we used to be. Criminals have taken note."

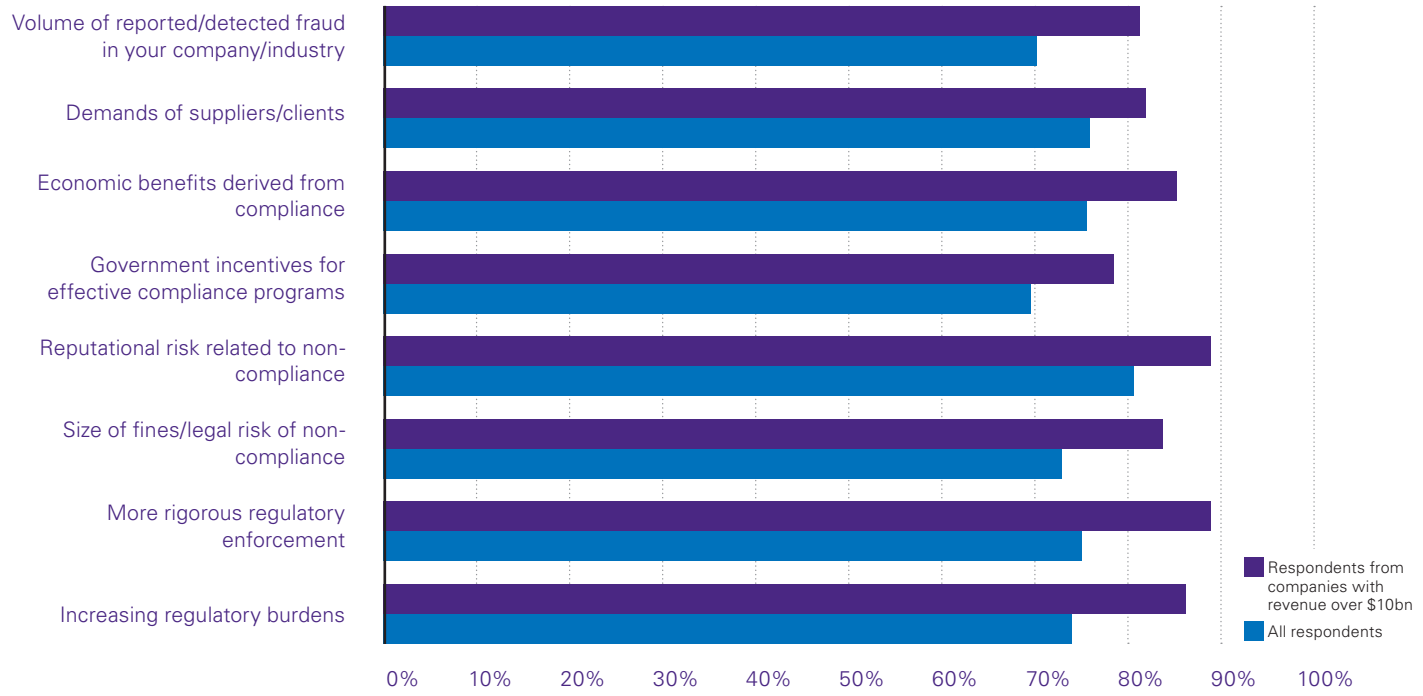
Almost all those surveyed reported that their companies had taken steps to address cyber security risks, including implementing two-factor authentication (55 percent), improvements to network security (54 percent) and better training (47 percent). The resultant investment needed to meet these cyber security challenges could be substantial. Calderón reports that, at Grupo Bimbo, "the board increased the cyber security budget by more than five times. It may well increase more." This increase was necessary even though fewer than one in five of Grupo Bimbo's employees works from home.

69 percent of those surveyed say that remote work has been a major cyber security challenge for their businesses

The COVID-19 outbreak and related shift to remote working have made it harder for companies to address their cyber security; 67 percent of respondents remain concerned about the cyber risks of a hybrid working environment. The end of the pandemic, or at least lockdowns, may be in sight for some, but permanently altered work patterns in the Americas mean that efforts in every aspect of the threat loop require urgent attention.

Data Snapshot II: Compliance is an all-of-business concern

To what extent are the following increasing the time and attention that your company's leadership is paying to compliance issues?[3]



Compliance is no longer (if it ever was) simply a matter of staying on the right side of the law. As the chart shows, over 70 percent of all respondents, and more than 80 percent working for large businesses, report that rigorous enforcement, increasing regulatory burdens and potential penalties increase the time and attention that their corporate leaders give to compliance issues.

However, stakeholder demands, economic benefits and reputation are just as likely to focus leadership attention on compliance: 64 percent of those surveyed report that suppliers and customers are increasingly demanding proof of compliance with data-privacy regulations, and 52 percent say the same about corruption and money-laundering legislation.

Beth Rose at Ford is not surprised: "With the evolution of social media and the proliferation of people opining on reputation and brand, you have to be concerned about getting compliance right."

Strict enforcement and the importance of avoiding inadvertent connections with non-compliant behavior through partnerships and mergers with third parties are also imperatives.

This wider set of considerations broadens the role of the compliance function. Garcia Jiménez says that, while compliance is still about mitigating risk, it is now also about "narrative building, internally and externally."

Part of the job is to show regulators and other stakeholders, and society at large, the economic, social and environmental benefits that the business provides to the community.

This wider narrative building has other spin-off benefits for companies. Most notably, good compliance helps to communicate a company's trustworthiness to other stakeholders, whether regulators, investors, partners, or customers.

[3]The chart shows the proportion of respondents that have selected either option 4 or option 5 on a 1-5 scale, where 1 is defined as "Not at all", 3 is defined as "Somewhat" and 5 is defined as "Greatly"

Threat levels are rising

The challenges of working remotely are only part of a wider pattern of increased difficulties related to fraud, compliance, and cyber security: 69 percent of respondents expect an increase in the risk of at least one of either external or internal fraud in the next year, and 29 percent project a rise in the risk of both.

Worries about growing cyber crime are widespread: 77 percent say that cyber-security risk will increase in the next 12 months; only 7 percent foresee a decline. Galimberti agrees, saying, "companies are facing more and more hackers, ransomware, phishing and other attacks."

The increase in instances of fraud and cyber attacks is not always connected. Calderón notes that any pressure on operating models can create an increase in fraud risk. In the food and beverage industry, for example, consumer interest in healthier products at lower prices is reshaping demand. A shift toward using lower-cost suppliers to meet this new demand requires due diligence related to how these partners do business, including such considerations as how they negotiate contracts and ensuring they don't keep prices down by using highly polluting processes.

Nevertheless, fraud and cyber insecurity do overlap to an increasing degree. The types of cyber attacks for which the greatest number of respondents saw increases in the past year include phishing (44 percent), scamming (33 percent), spyware (22 percent) and ransomware (20 percent).

69 percent of respondents expect an increase in the risk of either external or internal fraud in the next year

Current business trends inadvertently increase this convergence of fraud and cyber risk by providing fraudsters with new opportunity. Calderón notes, for example, that "digitization of processes, going to the cloud, [and] using more mobile devices" all carry risks. Rose adds that "with everyone being remote and on computers, bad actors have found more creative ways to operate." She adds that such efforts are not all online. The data supports her: 17 percent of respondents reported a rise in social hacking, whereby cyber criminals use social engineering and manipulation of human behaviors to gain access to systems.

62%
Expect new data privacy regulations in next five years

47%
Expect new environmental regulations in next five years

46%
Expect new labor regulations in next five years

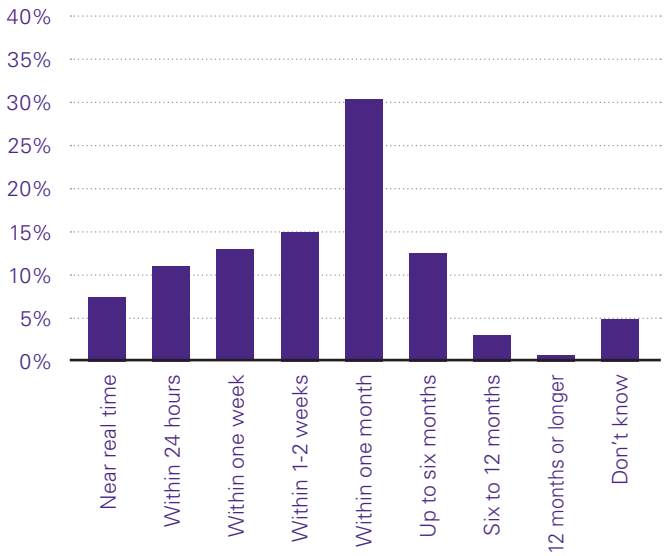
41%
Expect tougher enforcement of existing rules in next five years

General compliance risk is also likely to grow in the next year, according to 60 percent of those surveyed; only 17 percent of respondents expect a decrease in compliance risk. This challenge, as Ford's Rose explains, is a multi-faceted one, including more compliance requirements in fields with substantial existing regulations; the likely introduction of rules in new areas; and more active enforcement by compliance officials. As the results above show, a substantial number of respondents expect new regulations related to data privacy, environmental regulation and labor relations over the next five years. Overall, 89 percent of respondents say that there will be new compliance requirements in at least one of these areas in the next year. Rose confirms that "the current US administration has made no secret that it is ramping up enforcement and that it is regulating more in all areas. These include environmental, social and governance [ESG] regulations. Cyber will continue to grow. They all bleed together."

Latin America is seeing similar regulatory increases. Galimberti reports that Brazil's General Data Protection Law, which entered into force in September 2020, has driven compliance activity by companies large and small. The law accords substantial rights to data subjects – including that of data access – as well as requiring all companies that process data to appoint a data protection officer. Calderón adds that environmental requirements in areas such as water consumption and waste management are growing. These are "a challenge, but at the same time an opportunity to respond to consumer needs," he says.

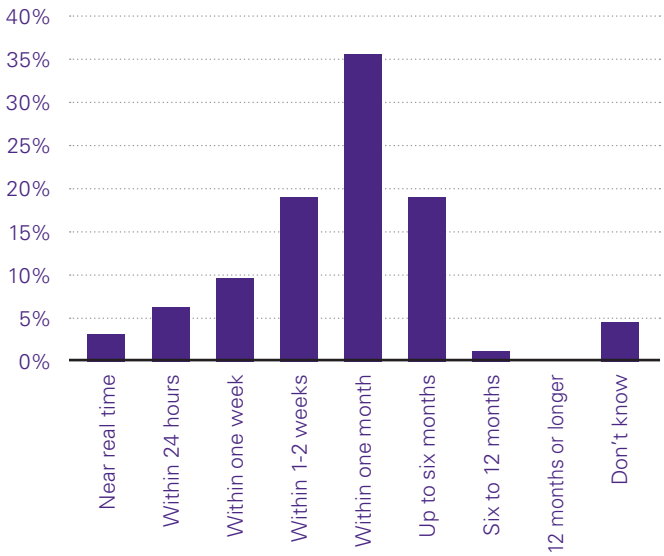
Data Snapshot III: Slow responses, insufficient concern

How long does it typically take to identify a cyber attack or breach at your company?



Median: Approximately 2 weeks

How long does it typically take to contain a cyber attack or breach at your company once identified?



Median: Approximately 2.5 weeks

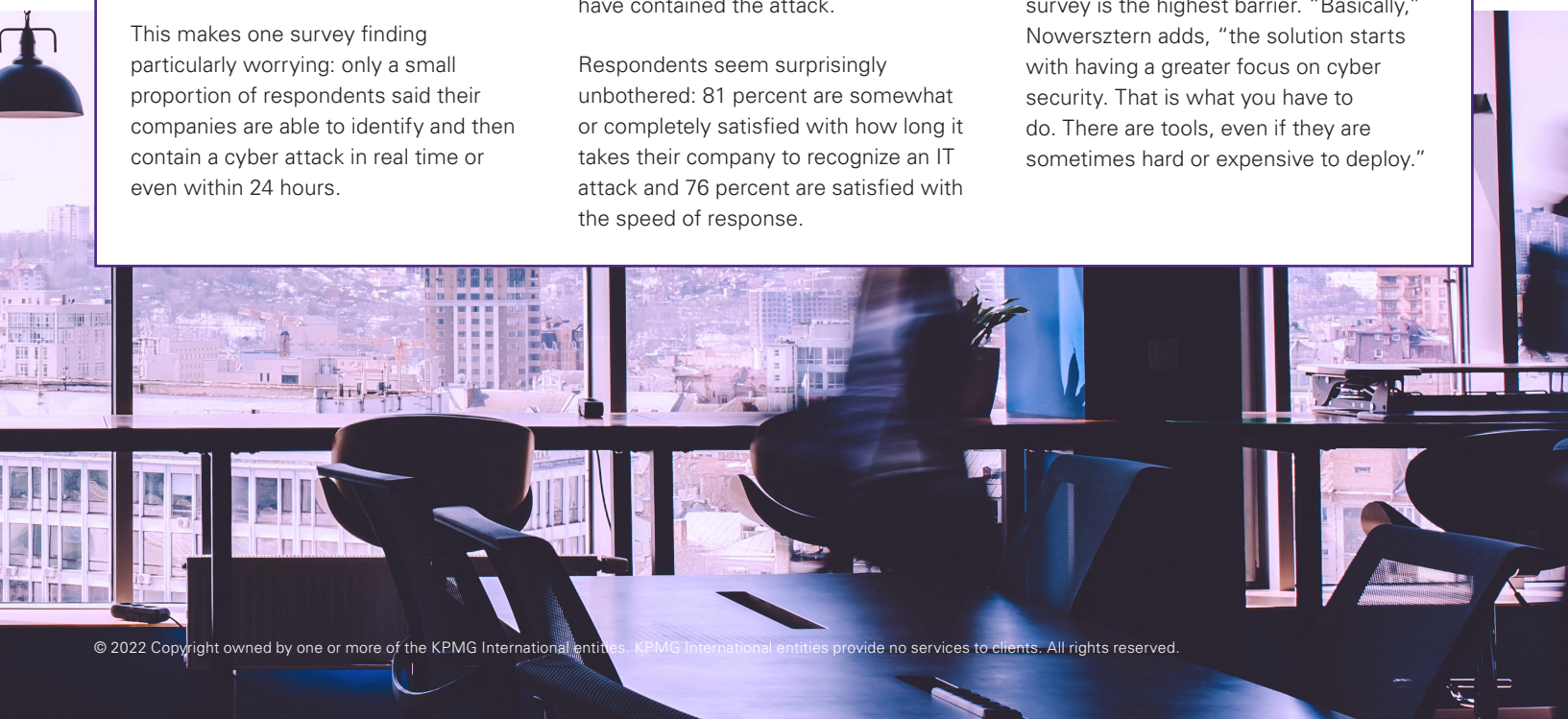
After a cyber incident, "Your data could be gone in minutes or seconds. In that sense, no speed of response is quick enough," observes Ariel Nowersztern of the IDB. Similarly, bad actors are able to damage companies in any number of ways upon gaining access to networks.

This makes one survey finding particularly worrying: only a small proportion of respondents said their companies are able to identify and then contain a cyber attack in real time or even within 24 hours.

The median time for identification is much longer — two weeks — and containment requires an additional two and a half weeks. Overall, according to our survey, it typically takes about a month from the beginning of a cyber attack on a company for the company to have contained the attack.

Respondents seem surprisingly unbothered: 81 percent are somewhat or completely satisfied with how long it takes their company to recognize an IT attack and 76 percent are satisfied with the speed of response.

Nowersztern explains that there are numerous barriers to better cyber security, including a lack of trained professionals and the common perception of cyber security as a cost rather than an investment. Ultimately, though, the muted concern shown in our survey is the highest barrier. "Basically," Nowersztern adds, "the solution starts with having a greater focus on cyber security. That is what you have to do. There are tools, even if they are sometimes hard or expensive to deploy."



Comprehensive mitigating controls remain rare

What kind of protection do companies have in place against the growing complexity of fraud, compliance and cyber threats?

By any number of measures, most have substantial room for improvement, especially in Latin America — although the North American responses give no cause for complacency.

Overall, only a minority of those surveyed say that their companies model international best practice in anti-corruption compliance (18 percent); environmental compliance (21 percent); anti-money laundering compliance (22 percent); anti-fraud controls (23 percent); or data-privacy controls (27 percent).

North American companies benchmark themselves higher. Most respondents from North American companies either think they are meeting international standards or doing well by domestic standards.

By contrast, the most frequent answer from Latin American respondents to these questions is that, while their companies meet their legal obligations, they do not excel by domestic or international standards.

In fact, with respect to corruption and money-laundering regulation, over a quarter of Latin American respondents are unsure if they fully meet even local rules.

To get a more detailed picture, the survey dug into how well respondents ranked their companies on individual aspects of fraud control (11 areas), compliance (seven areas) and cyber security (six areas).[4] A company might not necessarily need to excel in every one of these 26 areas across the threat loop. As Rose says, "Compliance is supposed to be risk-based." Too much effort directed to low-risk areas would be an inappropriate drain on resources. Nevertheless, the matters covered in the survey — such as financial and management controls and prevention of data theft — are sufficiently important for most businesses to strive to improve their management.

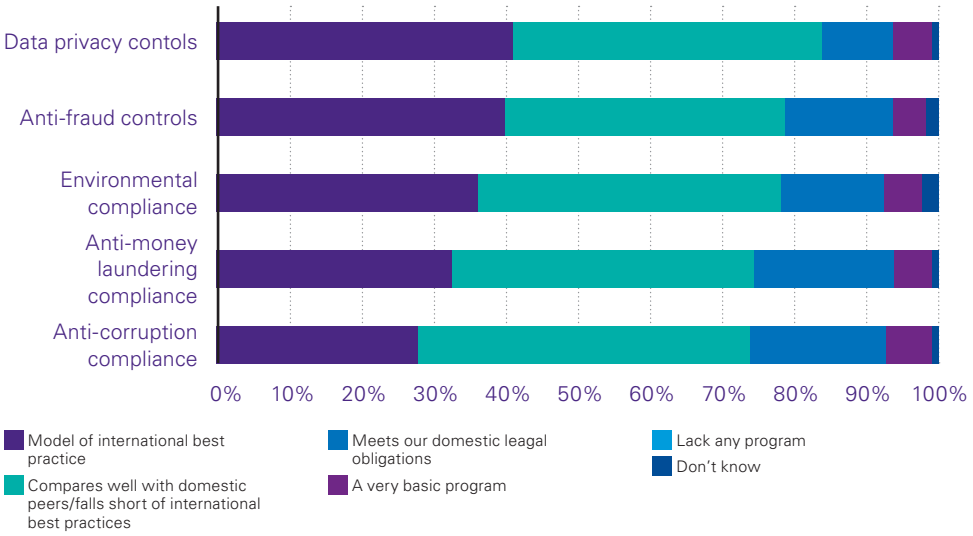
[4]Specific areas covered are:
For fraud control — Financial controls; physical asset security; IT security; management controls and supervision; staff background screenings; whistle-blower or other reporting mechanisms; due diligence processes related to suppliers, partners and/or customers; anti-fraud policies/fraud matrices; risk assessments; staff training; and fraud response plans.
For compliance — Non-compliance prevention; finding and investigating instances of non-compliance; taking action to mitigate instances of non-compliance; reporting irregularities to the authorities in a way that minimizes corporate risk, fines and penalties; adjusting and complying with new regulatory requirements in a timely manner; identifying compliance and fraud risk among potential third parties; and adopting new technologies to improve performance in the above areas.
For cyber security — Prevention of data theft by external hackers; prevention of data theft by employees; prevention of data loss/theft arising from employee mistakes; prevention of data theft by vendors/suppliers/partners; prevention of ransomware attacks; and prevention of other attacks on networks or assets.

On the positive side, for each of fraud control, compliance consideration and cyber security control, 85 to 95 percent of respondents rated their businesses as excellent in at least one of the areas covered in the survey. However, very few rated their companies as having high-quality performance across the board. We calculated how many of those surveyed rated their companies as excellent for at least half of the areas covered in each category (we call this the 'half-or-more' standard).

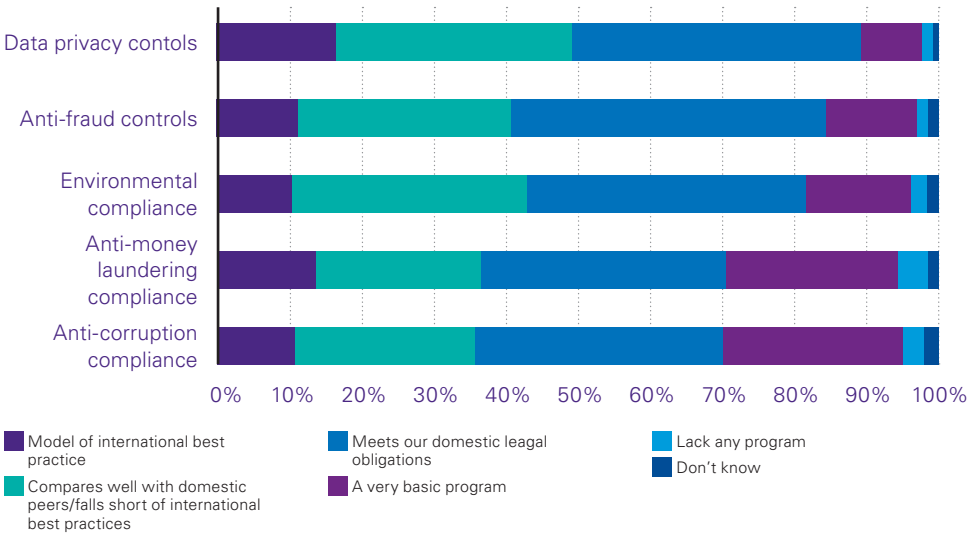
Overall, only 24 percent of respondents said their companies achieved the half-or-more standard as it relates to cyber security, 17 percent as it relates to fraud controls, and just 13 percent as it relates to compliance.

Moreover, only 4 percent of respondents said their companies achieved the half-or-more standard in all three areas. In short, most companies need to enhance the quality of their efforts against fraud, compliance, and cyber risks.

How mature are your company's programs in the following areas?
North American responses



How mature are your company's programs in the following areas?
Latin American responses



The issue is more widespread in Latin America, where just 20 percent of respondents said their companies met the half-or-more standard for cyber security, 11 percent as it relates to fraud controls, and 9 percent as it relates to compliance. The impact of this weakness is clear in other survey results; for example, respondents noted that internal audits were responsible for revealing instances of fraud or breaches of compliance or cyber security at 43 percent of North American companies but only at 27 percent of Latin American companies.

Similarly, other internal controls brought such problems to light at 41 percent of businesses in North America but at just 31 percent of businesses in Latin America.

Latin American companies' lower levels of excellence on internal controls may also help to explain the higher levels of internal fraud which respondents from those companies told us they face.

Leaders at many respondents' companies appear to understand that defenses need bolstering. Around 65 percent of those surveyed expect spending on cyber security to increase in the coming year; 53 percent expect increased spending on fraud prevention; and 44 percent expect increased spending on compliance. Only a handful of respondents — under 7 percent in each case — project that outlays in these fields will decline in the next year.

As companies make these spending decisions, the most important advice that our professionals give is not to forget your people. Calderón believes that "training and retention of good employees is one of most important things to prevent fraud. This spreads the right culture." Rose agrees that "the biggest issue is culture."

She adds that getting this right requires not just training but also taking care of fatigued employees in the aftermath of the pandemic. "People may be reaching their limits on a day, or overall, which can lead to mistakes or misconduct. How do we help make sure people are okay, and supported? That is the big one."

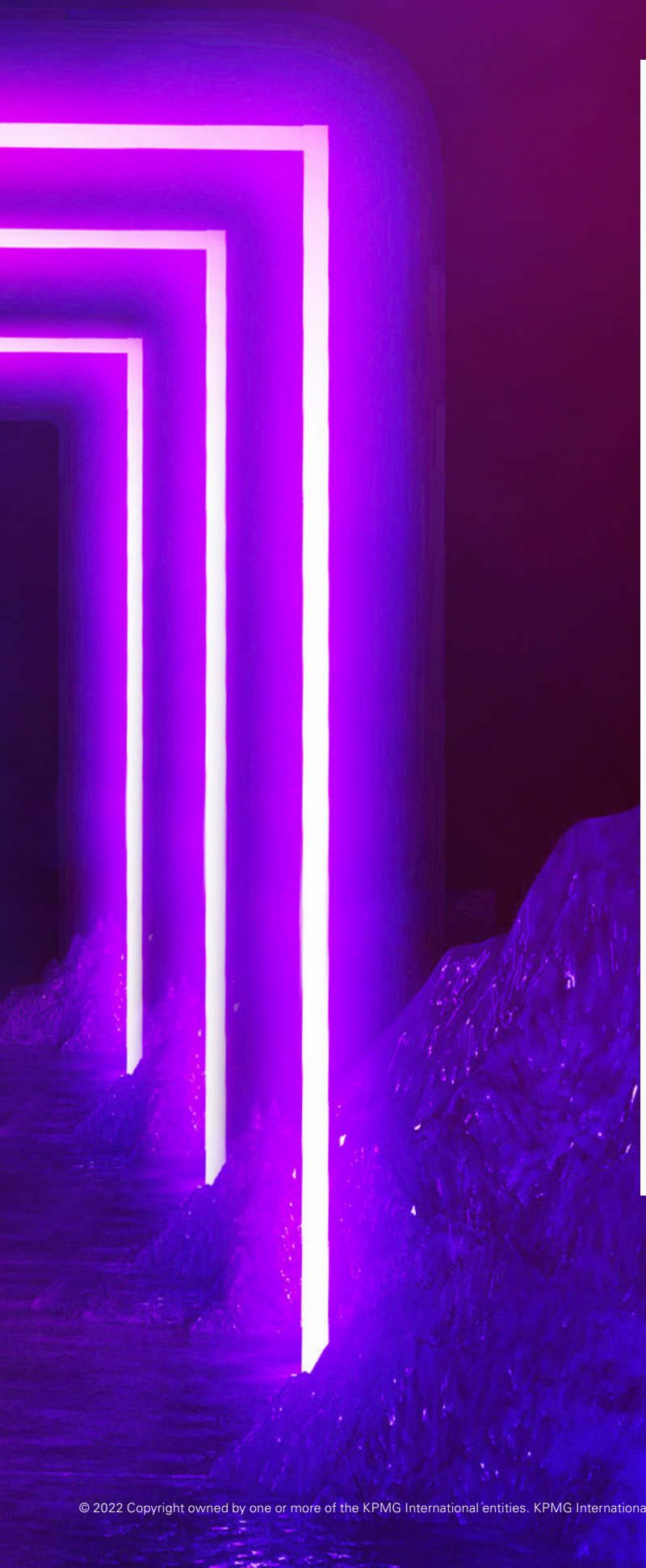
Companies meeting the half-or-more standard

North America

31%	27%	18%
Cyber security	Fraud prevention	Compliance controls

Latin America

20%	11%	9%
Cyber security	Fraud prevention	Compliance controls



Conclusion: Is your company prepared for the triple threat?

Before the COVID-19 pandemic, fraud, non-compliance and cyber attacks already presented an expensive threat to companies across the Americas. Now, these have grown more extensive and complex.

Looking ahead, executives expect another widespread increase in risk across the three threats.

Most companies have some defenses in place, but comprehensive excellence is rare. This is especially the case in Latin America, where our survey suggests, for example, that a lack of effective controls is responsible for higher levels of internal fraud. North American companies are doing better, but most still fall short.

The majority of companies are set to spend more money in, and increase leadership focus on, these areas. KPMG recommends that they take these five steps to mitigate the triple threat:

01

Set the right tone from the top

Senior management and the board should ensure that they promote a culture that encourages ethical conduct and a commitment to compliance. As part of this, they should establish standards and procedures to prevent and detect fraud, mitigate compliance and cyber security risks, and monitor compliance with those standards. To support this, companies should put in place protocols that ensure that the board is knowledgeable about and can exercise reasonable oversight over compliance and ethics.

02

Carry out a risk review

Companies should implement a comprehensive enterprise risk assessment process that includes fraud and misconduct, compliance and cyber security risks and focuses on actual — not hypothetical — risks. This means that management, the board, internal audit, compliance, operations and other stakeholders need to work together to identify key risk areas and design controls to mitigate them.

03

Communicate effectively

Companies should evaluate existing protocols for training and communication to detail how messages about risk can flow most effectively across the organization. All relevant people should be receiving clear communications from senior management that control responsibilities must be taken seriously. To back this up, targeted training will help employees to understand their own role in safeguarding company assets and enhancing internal control systems, as well as how their own activities relate to the work of others.

04

Strengthen detection

Employees are critical in uncovering major fraud and misconduct. Organizations where employees believe they have a responsibility to raise their hands and report misconduct are the ones that will likely detect fraud and misconduct early. At these organizations, employees feel comfortable raising the alarm and do not fear retaliation; they expect management to be responsive. Organizations need to develop and publicize ways for employees and relevant third parties to report suspected wrongdoing and seek advice and clarification on laws, regulations and company standards of conduct.

05

Create a culture of enforcement and accountability

Companies should consider enhancing their policies and protocols to include elements of enforcement and accountability that are not punitive. For example, they might make ethical principles, integrity and behavior part of their performance evaluations and provide incentives or rewards for achieving goals related to ethics-related objectives or performance targets. This helps to push the message that disciplinary measures in instances of fraud and non-compliance are enforced consistently, regardless of rank, tenure or job function.

Contact us

Marc Miller
Partner, Global & U.S. Forensic Network Leader
T: 212-872-6916
E: marcmiller@kpmg.com

Emerson Melo
Partner, KPMG Brazil
Forensic South America Leader*
emersonmelo@kpmg.com.br

Ana Lopez Espinar
Partner, KPMG Argentina
Forensic South America Leader*
ablopez@kpmg.com.ar

Enzo Carlucci
Partner, Risk
KPMG Canada
ecarlucci@kpmg.ca

Luis Preciado
Lead Partner, Risk Advisory, KPMG Mexico
Forensic Mexico and Central America Leader*
luispreciado@kpmg.com.mx

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com

MADE. | MDE139234 | January 2022