RSA

2ND EDITION
JANUARY 2020

# Digital Risk Report

# Welcome

We continue to see the evolution of technology every day. Our daily life, our corporate life, our homes, families, relationships... our very future is being transformed by the power of digital inevitability. While the future is constantly in flux, we have learned two very important lessons from the past that apply to the digital transformation that is unfolding before our eyes.

> **One:** Digital transformation is a global opportunity. Technology has torn down borders, opened personal and business opportunities, and made possible relationships and communication that years ago were science fiction dreams. But while technology is central, at the end of the day, digital transformation is about people.
>
> **Two:** This digital future does not come without risk. For those of us on the front lines of digital transformation within our organizations, we must understand the complex and accelerating nature of risk that may be exploited to our benefit – or stand in the way of our success.

This report cracks open the implications of these two lessons. First, we provide a global view into the impact of digital transformation on risk and security management. The RSA Digital Risk Survey provides insight into global perceptions and priorities related to managing digital risk. We also provide an analysis into the Middle East region – a part of the world that is taking digital transformation head on by pursuing a wide-range of ambitious plans. We also wanted to underscore the human element of risk and security. Cyber risk, fraud, and the rise of the dynamic workforce may appear to be technology-driven topics but there is a significant undercurrent of human elements that affect your organization's risk.

These two golden rules of digital transformation are fused into RSA's DNA as we continue to help our customers pursue their digital ambitions. In facing this digital inevitability, organizations must proceed with confident caution – willing to take certain risks while balancing control and security. As we have for the last 35 years, RSA products and services are directly involved with maintaining this stability. From advanced threat detection to identity management to fraud prevention to integrated risk management – RSA is helping organizations manage the unwanted and often unexpected outcomes that stem from digital transformation, digital business processes and the adoption of related technologies.

**Holly Rollo**
Senior Vice President & Worldwide Chief Marketing Officer, RSA

# Table of Contents

# The RSA Digital Risk Survey: Global Results

**Steve Schlarman** and **Jane Wright**

## Introduction

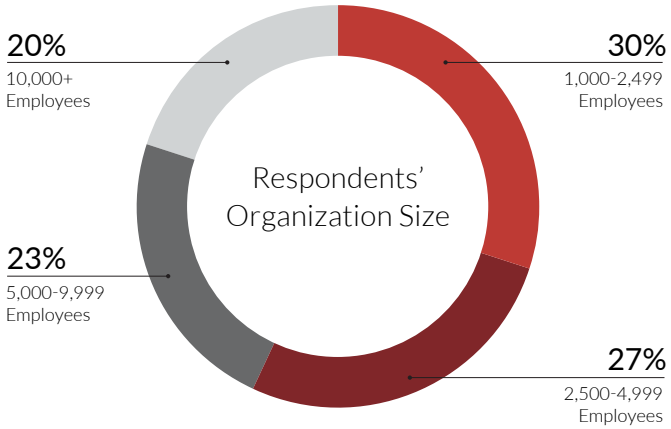
Over the course of 2019, RSA executed a series of research efforts to analyze the shift in risk and security requirements that organizations experience as they pursue digital initiatives. While some organizations have completely transformed their business with digitally driven products and services, many organizations are still working through adoption of innovative technologies to optimize operations and unlock value utilizing existing legacy IT systems. Despite the wide range of digital transformation incarnations in organizations, it is undeniable that emerging technologies such as IoT, mobile, social, big data and advanced analytics have opened many doors for business. In turn, the risk and security industry have a fair share of opportunities—and challenges—in the digital world.

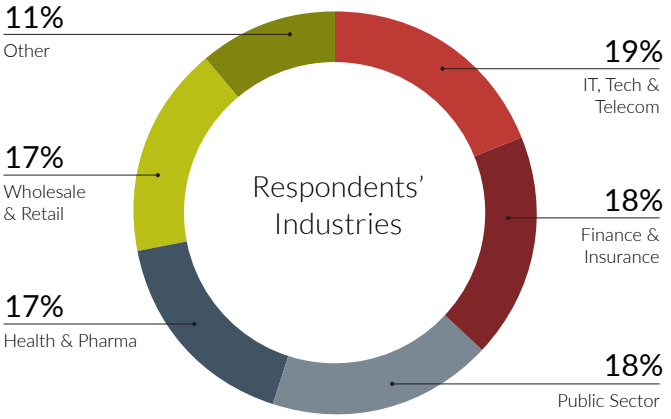
As part of this exploration into the nuances of risk in the digital world, RSA designed a survey to better understand the perceptions and priorities for managing digital risk. RSA commissioned research firm Vanson Bourne to execute the survey to 600 qualified respondents in North America. In the first edition of the RSA Digital Risk Report, published September 2019, RSA published the findings based on the survey conducted in North America. Intrigued by the findings, RSA expanded the scope of the survey to include a broader, global perspective, adding 450 respondents in Western Europe and Asia, Pacific, Japan (APJ), for a total of 1,050 respondents.

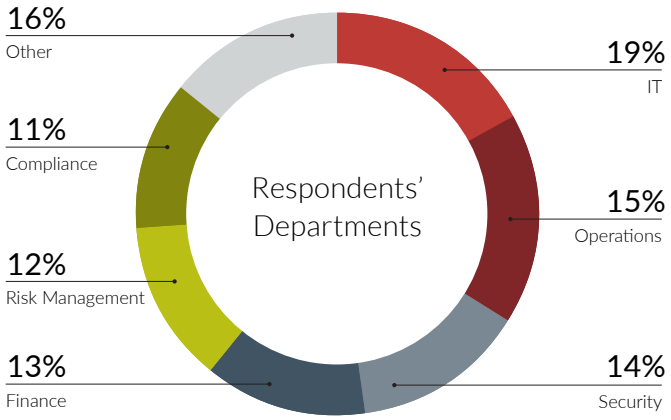
| Timeline | | | |
|---|---|---|---|
| Fielded | May-June 2019 | August 2019 | August 2019 |
| Region | U.S., Canada | U.K., France, Germany | Australia, Japan, Singapore |
| Sample size | n=600 | n=300 | n=150 |

The global survey results confirmed many of the initial key findings:

- Digital initiatives are changing the face of business across the globe, regardless of organizational size and industry.
- Digital transformation (DX) has created both unique risks and evolutionary changes to tradi-tional risks.
- Risk management priorities are affected by an organization's digital strategies. While cyber attacks, workforce dynamics and third-party risk are top-of-mind issues, every organization feels the effect of digital transformation in different ways.
- To meet the demands of the digital transformation efforts underway, security and risk management processes must leverage collaboration across IT, security and risk functions along with an increased involvement of the business.



# Digital Is Driving Change

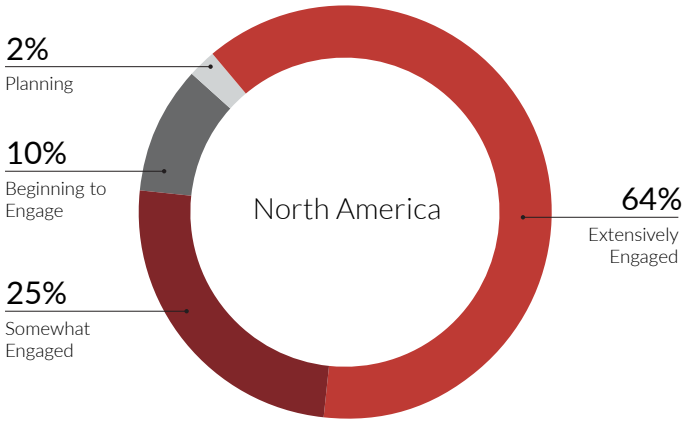
Whether you consider efforts as a revolution of your business model or an evolution of your operations, digital initiatives are prevalent across organizations of all sizes and industries. Within the original survey in North America and the expanded survey in other regions, taken collectively, six in 10 respondents state their organization has a high level of engagement with digital transformation (DX). Regional breakdowns indicate differences in the level of adoption of digital transformation initiatives.

Cloud initiatives, namely moving a significant number of workloads to the cloud, were cited as the most common type of digital transformation efforts. As organizations embrace more cloud architectures, both public, private and hybrid, the ramifications ripple across the risk and security landscape. Visibility into these environments can become problematic as well as the challenge of the shift of operational management and responsibility. But cloud is not the only type of digital initiative that is affecting organizations. Additional types of digital transformation cited in the survey include extending applications and services to customers, extending the digital footprint to a wider environment and enabling a "work anywhere" workforce.

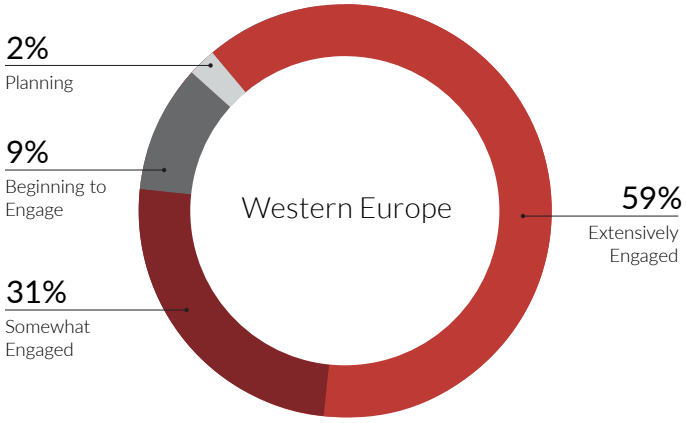
This variety of digital transformation is driving considerable change in the risk profiles of organizations. One of the key findings in the original study in North America was the acknowledgement of change in risk profiles over the last two years and the expectation of change in the next two years. This finding remained similar globally. Digital initiatives are forcing both evolutionary and revolutionary changes in managing risk and security. For some organizations, risk and security processes must address incremental changes in risk identification and control treatments. For example, expanding existing authentication services to address new SaaS business applications is an extension (evolution) of existing controls. Other initiatives represent more drastic (revolution) changes such as the major shift in controls when transitioning major data center operations to a cloud provider.

Figure 1. Organizations' Digital Transformation Status

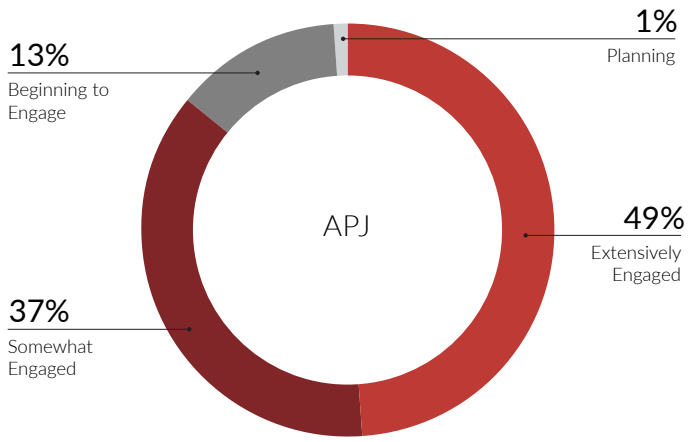
*To what extent has your organization engaged in digital transformation initiatives over the past two years?*




*(n=600)*




*(n=300)*



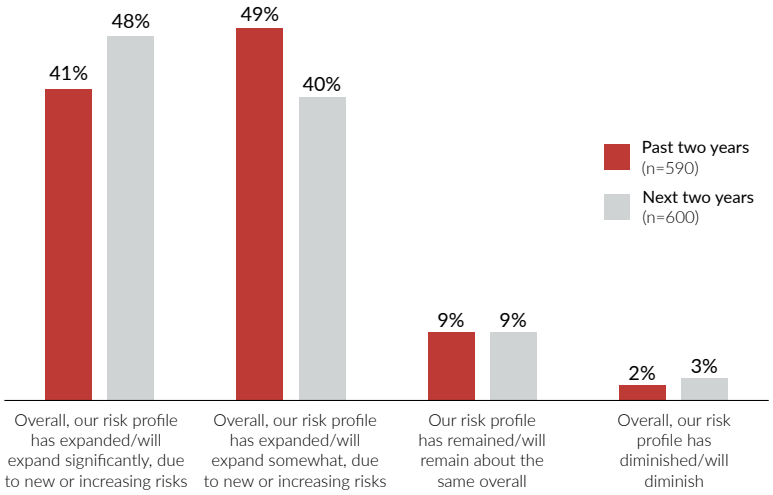

*(n=150)*

**Response percentages may not add up to 100% due to rounding.*

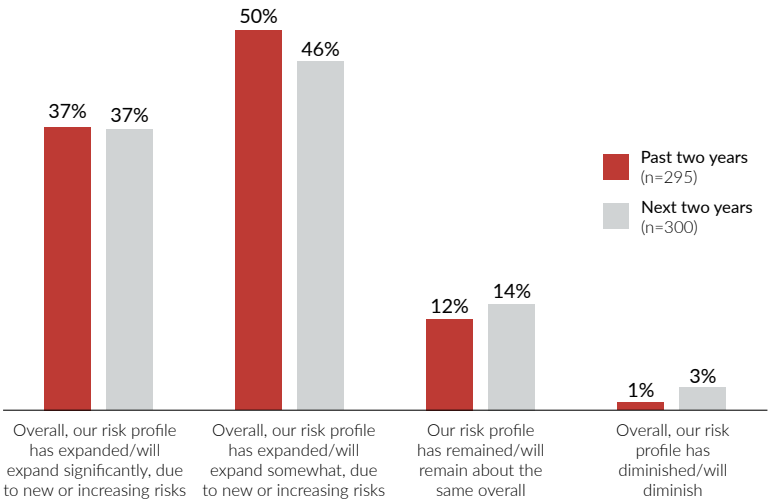
## Figure 4. Expected Change to Risk Profile*

*How has your organization's risk profile changed over the past two years, due to its digital transformation? How do you believe your organization's risk profile will change over the next two years, as you embark on or continue your digital transformation?*

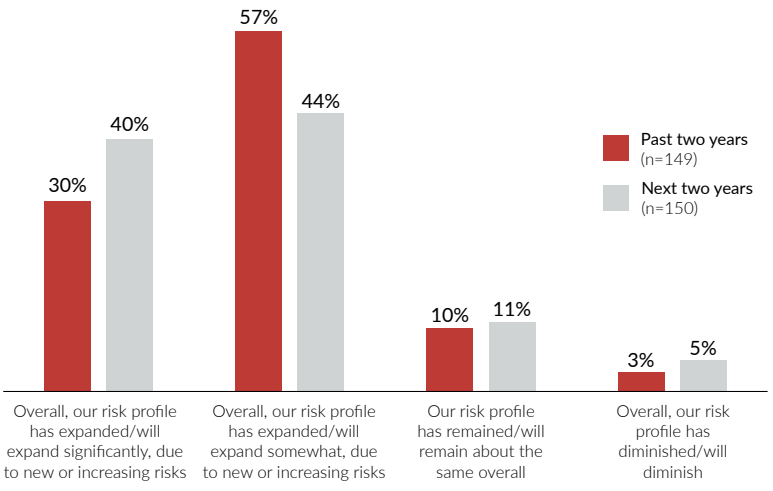
North America




Western Europe




APJ




**Response percentages may not add up to 100% due to rounding.*

| What are the most important reasons your organization will invest in new or extended solutions or services to manage its digital risks? Select one. | Percentage of Respondents |
|---|---|
| Strategy to invest a much as needed (within reason) to ensure digital transformation success | 36% |
| Top executives increasingly focused on managing digital risk | 23% |
| Risk team will lobby for risk management in our digital transformation | 14% |
| Security team will lobby for risk management in our digital transformation | 12% |
| External stakeholders expect us to manage digital risks | 7% |
| Must invest to meet new or more stringent compliance regulations related to the digital transformation | 7% |

*n=1, 045*

In response to this continued change, organizations are looking to expand their capabilities in risk and security management. The respondents indicated desire to invest in risk management solutions proportional to the digital transformation. Maintaining pace with the change is one area of concern. One way to think of this investment is effective digital risk management can keep digital initiatives on schedule. Retrofitting controls after implementation is generally much more costly and less effective.



## Keeping the DX Moving Forward

"I'm trying to find the right balance of moving fast but at the same time building [the DX application] securely. We're building security standards as part of it, but we're looking at slowing down. It's necessary to do that because we had seen scenarios before where things were employed too fast and we were exposing a risk. We caught up with it and we had to back pedal and that's not ideal." **VP of IT, Communications, U.S.**

The challenge of keeping pace with digital transformation is real for security and risk teams. Identifying, assessing and treating risks—whether it is an incremental change or during a major upheaval—is inherently necessary for successful projects. However, when existing processes are reliant on mainly manual methods and are designed for point-in-time assessments, the agility of the business can be hampered.

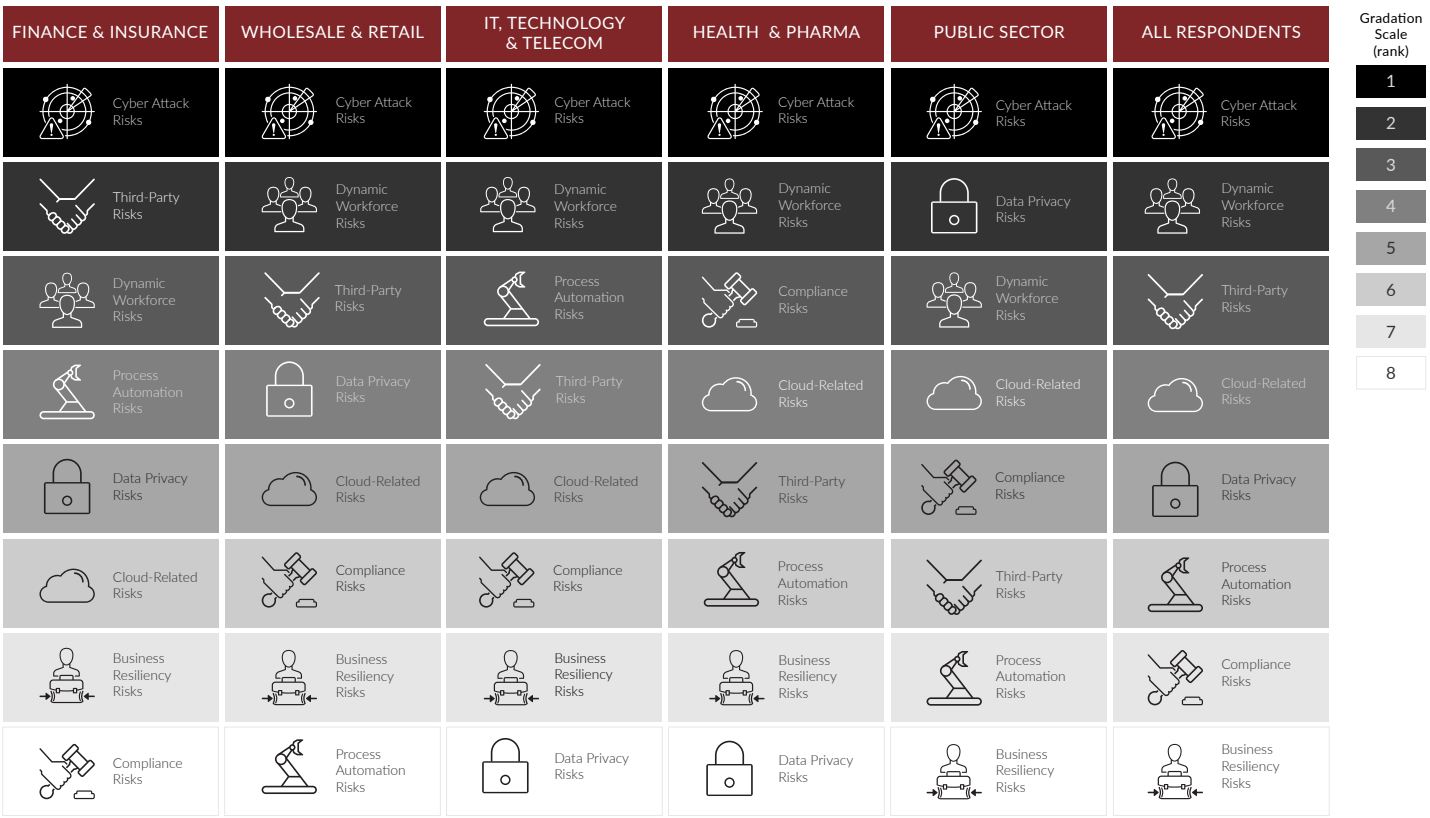
# Prioritization and Collaboration Are Key

In the North American study, the primary objectives of risk management programs were consistent across industry and personas. Cyber-attack risks and dynamic workforce risks were generally the #1 and #2 priorities, respectively. Respondents in North America ranked managing data privacy as their third main risk objective over the last two years; risks related to process automation were ranked #3 for the next two years. Notably, each area of risk was ranked #1 by at least some respondents, meaning every risk management objective is someone's top priority.

These rankings shifted a bit in the global perspective, as revealed by the survey results in Western Europe and APJ. While cyber-attack risks and risks associated with a dynamic workforce held on to the top two priority areas, global respondents ranked managing third-party risks as the third priority. Consistent across the globe though is the identification of each critical risk area as someone's #1 priority. As with the North American results, each area of risk was a main priority for some segment of the respondents in other regions. Looking at future risk management objectives for the next two years, respondents' viewpoints diverged by industry in the global survey. This suggests that the market forces brewing in each sector play the largest role in shaping the risk management priorities associated with an organization's digital transformation.

Figure 5: Top Risk Management Priorities by Industry (next two years)

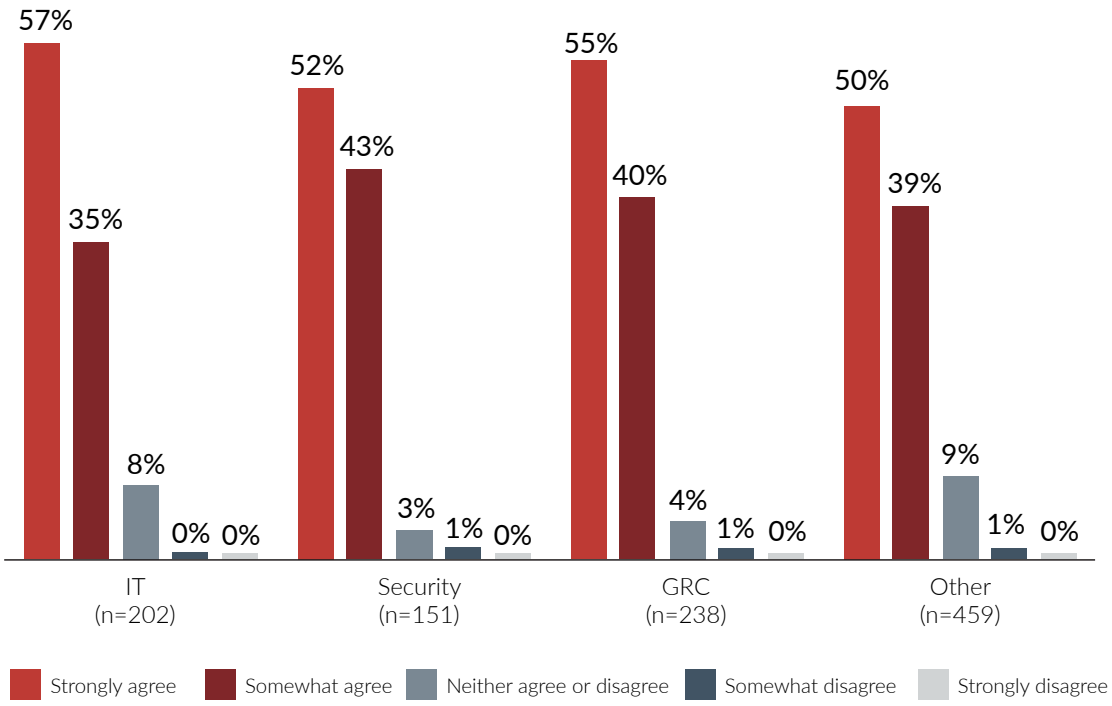
*Please think about your organization's strategy to manage the risks that may emerge or increase due to your digital transformation over the next two years. What do you believe will be your organization's most important objective? Select one.*



One topic that respondents overwhelmingly agreed upon is the need to build a strong coalition to manage digital risk. Respondents in IT were most likely to strongly agree on the need for collaboration, with security and risk teams perhaps looking for a stronger connection to the security and GRC/risk teams. Across the board though, respondents see coordination as an integral part of improving risk and security management effectiveness.

## Figure 6. Security and Risk Teams Need to Work Together

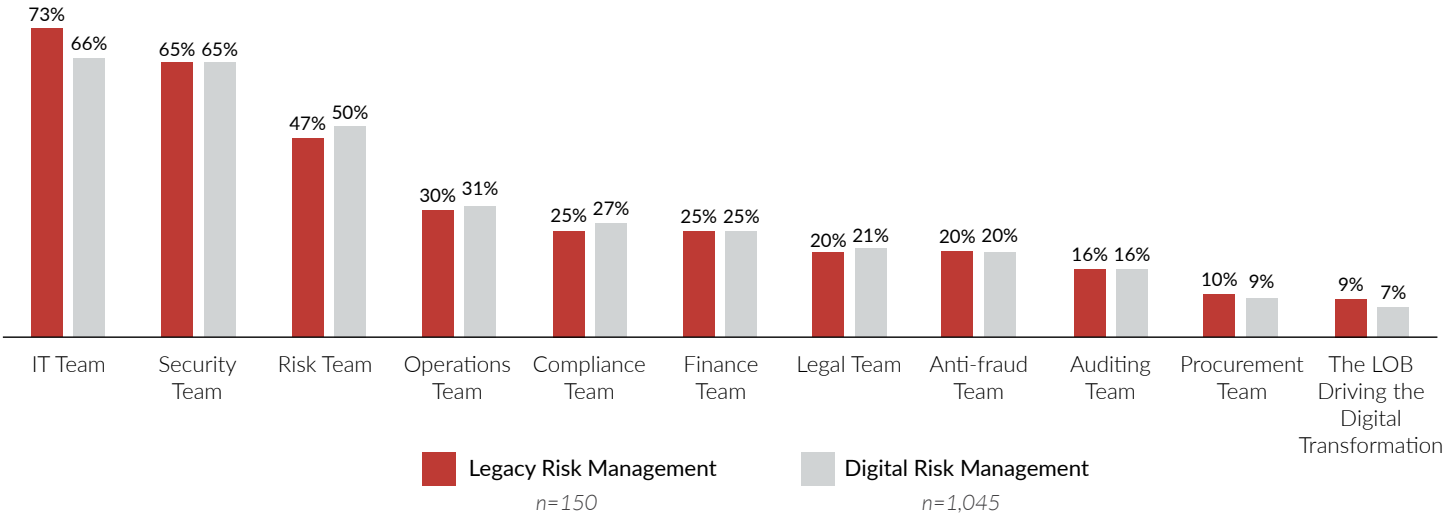
*To what exent do you agree with the following statement? The security and risk teams in an organization need to work together in a coordinated way (such as sharing data or planning processes together) to effectively manage the risks that may emerge or increase due to their organization's Digital Transformations.*




The pressure to integrate forces may be due to the fact IT, security and risk teams are carrying a tremendous load when it comes to managing digital risk and therefore must work together to break down traditional, siloed approaches to risk management. A key observation of the survey, is the small (<10%) role, the line of business that is driving the digital transformation plays in managing digital risk. Engagement with the business is critical in understanding the strategic business objectives – the very need for managing risk. This deficiency was noted in the North American survey and it continued in the global perspective.

## Figure 7. Departments Involved in Risk Management

*Over the past two years, which departments in your organization were most involved in your organization's strategy to manage the risks that arose from its legacy (non-digitized) operations? Over the next two years, which departments in your organization will be most involved in your organization's strategy to manage the risks that may arise from its digital transformations? Check all that apply.*




The response in this area denotes an ongoing challenge to enlist the business in addressing digital risk. Without this engagement, the strategy can become slanted towards a technologist view. From the IT and security teams' perspective, they must shoulder the burden as the business may feel "this is just a technology issue and can be solved with technology." However, many digital initiatives require risk management adjustments not just in the technology arena but in the business process layer. Risk and security issues must be addressed in the first line of defense – the business itself. Without a collaborative approach across all teams, risk can hide in the 'cracks in between the lines of defense'.

## Building Collaboration

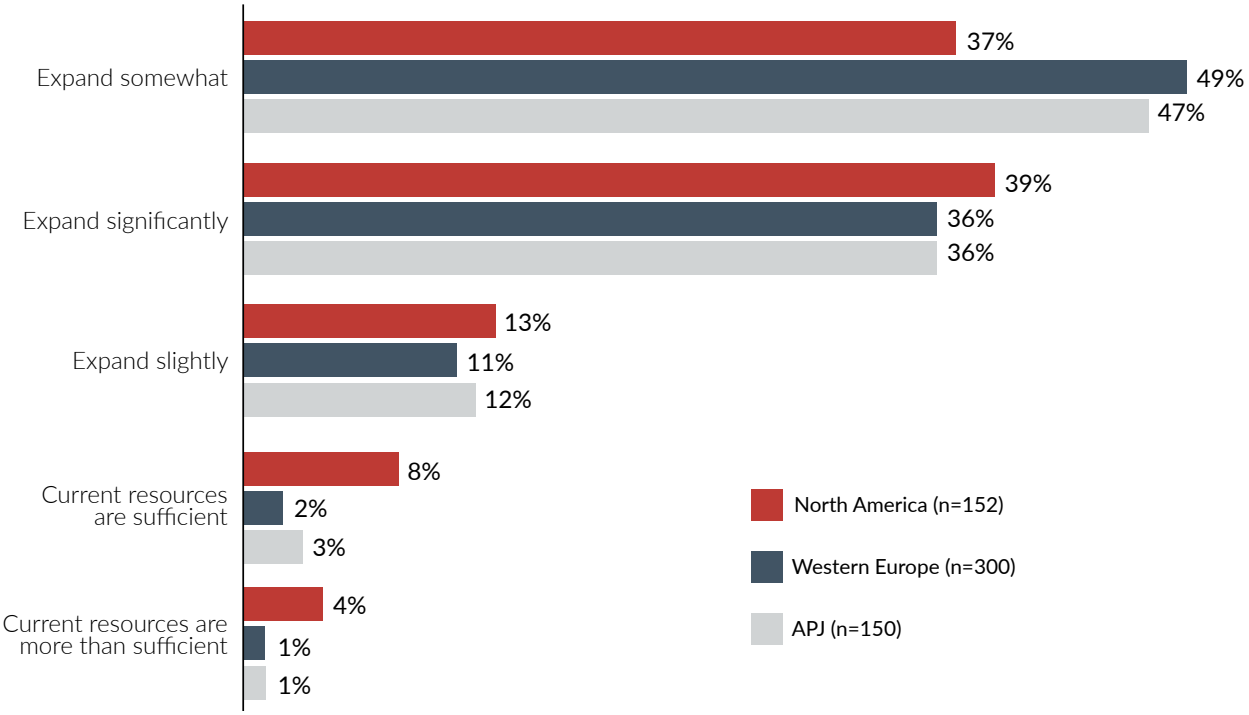
**"When we do transformation projects, we don't do it like the old times when the IT team would just go and do a project, we actually get stakeholders from all areas of the business involved. They have to be aware of what we're doing and where it impacts them in terms of system change and processes." VP of IT, Finance, U.K.**

Digital initiatives are an excellent opportunity to build collaboration between key operational groups. With groups sharing information and working together, it is a win/win situation. The IT and security teams learn more about the business; the business stakeholders better understand the technology driving their operations.

Another element of managing digital risk highlighted by the respondents is the expansion of resources. Very few respondents felt their current resources are sufficient to meet the changing risk landscape. While Finance and Insurance respondents indicated intent for the greatest expansion of resources, the need to expand resources for digital risk management were generally consistent regardless of industry. In addition to talent and skills, respondents indicated a priority on expanding threat detection and response, network security, vulnerability management, and IT risk management solutions.

## Figure 8. Need to expand Resources for DRM, by Region

*To what extent do you believe your organization will need to expand its current capabilities (such as its IT skills, risk management processes, cyber security technologies, etc.) to ensure it can sufficiently manage its risks over the next two years?*




## Coordination Across Your DX

**"We've got Apple Pay, Amazon Pay, Google Pay, all those things that we'd never done before were a whole new area of risk for us. The finance team said they were open to the way things were going to work but they were actually quite old fashioned in their ways of working."**
**Business Transformation and Technology Director, Retail, U.K.**

Digital transformation affects everyone in the business—not just the technologists. Adoption of technical solutions will generally drive changes into core business processes. The old adage "a rising tide lifts all boats" applies here. As technology may raise the operational "boat," alignment of business functions and technology direction is critical in ensuring risks are addressed and business processes are effectively protected and optimized.

# Balancing Benefits and Consequences

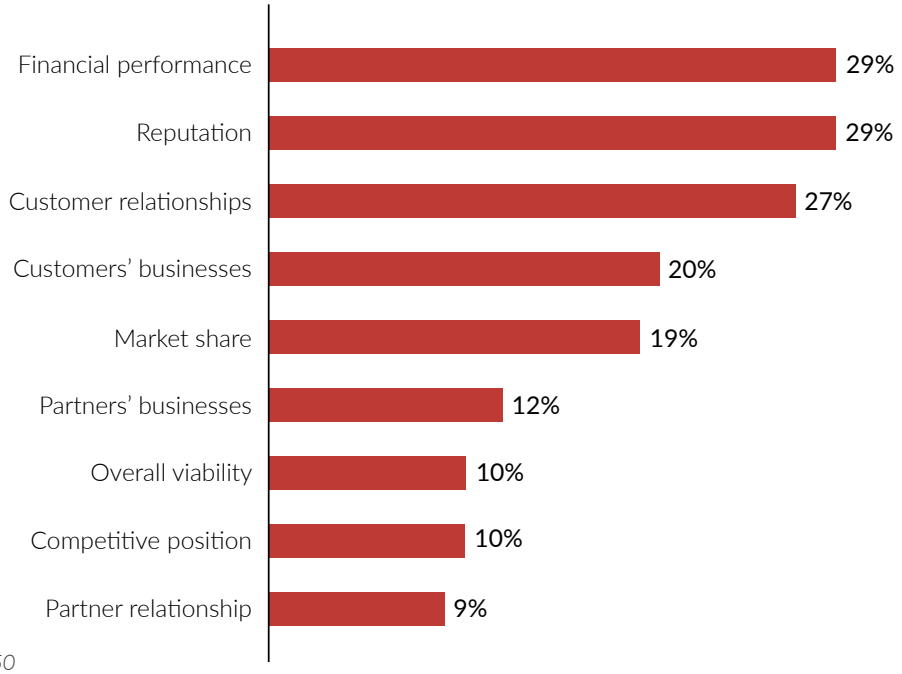
Digital transformation has brought to light many areas where risk and security teams can evolve. One key area noted by our survey respondents is the impact on the customer experience. As digital initiatives frequently involve some connection to end customers, organizations are concerned with financial performance, reputation and customer relationships as the top negative consequences related to digital risks.

Organizations can struggle to understand what their exposure is in meaningful terms—potential losses, customer dissatisfaction, reputational damage and other facets that clearly inform the business leaders what is at stake. While organizations have been utilizing technology for decades, we are at a new juncture when it comes to the digital age.

The speed of change in today's digital world—as highlighted in the changing risk profiles—is a double-edged sword. Change can be positive as companies find new paths to growth through digital initiatives, but the velocity of business can be overwhelming for risk functions to keep up. In addition, the speed of technology may create an opportunity for the next viral marketing campaign but can also be tremendously damaging if that viral event is a negative customer experience. Finally, the complexity of digital business is a major challenge. Business has become a web of connections, data, people, processes, tech, geographies and cultures leading to a complicated, interdependent set of business and technology challenges. The threat landscape, whether you consider a malicious attacker or a rising competitor, has become increasingly complicated and difficult to navigate.

Figure 9. Unmanaged risks could have negative consequences on…

*If your organization was unable to sufficiently manage its digital risks (the risks that may emerge or increase due to your digital transformation), which of the following possible consequences would you be most concerned about? Select up to two.*




*n=1,050*

We see this reflected in our survey as respondents indicated different types of digital transformations covering a wide range of technology shifts. When respondents were asked to identify different categories of digital initiatives, 78 percent selected three or more categories, indicating several types of transformations were ongoing within their company. The fact that multiple technology initiatives were simultaneously affecting the organization is a strong indicator for the increased complexity of digital business operations. For example, 61 percent cited cloud initiatives as a major part of their digital initiatives shaping not only the technology landscape but adding layers of complexity to third-party risk with the relationships with SaaS, IaaS and PaaS providers. Another example was the emphasis on customer and partner applications and expansion of the digital footprint of the organization. This expansion not only increases the attack surface for cyber threats but agile development lifecycles and DevOps are straining risk and security teams' ability to keep up.

| Which of the following types of Digital Transformation initiatives has your organization implemented in the past two years? Select all that apply. | Percentage of Respondents |
|---|---|
| **Cloud** (Moving a significant number of workloads to the cloud or optimizing across multiple clouds) | 61% |
| **Customer apps** (Extending applications or services to customers) | 49% |
| **Digital footprint** (Extending our digital footprint to a wider environment e.g. sensors, mobile devices etc.) | 47% |
| **Dynamic workforce** (Enabling a "work anywhere" workforce) | 46% |
| **Advanced analytics** (Applying advanced analytics techniques e.g. artificial intelligence) | 44% |
| **Process automation** (Replacing legacy/analogue operational processes with digital processes or technologies) | 43% |
| **Partner apps** (Extending applications or services to partners) | 42% |
| **IoT** (Linking our legacy and IoT systems together) | 36% |
| **Agile dev** (Using agile software development) | 36% |
| **Robotics** (Implementing robotics/automation systems) | 33% |
| **Sensors** (Setting up always-connected, sensor-enabled or location-aware technologies) | 29% |

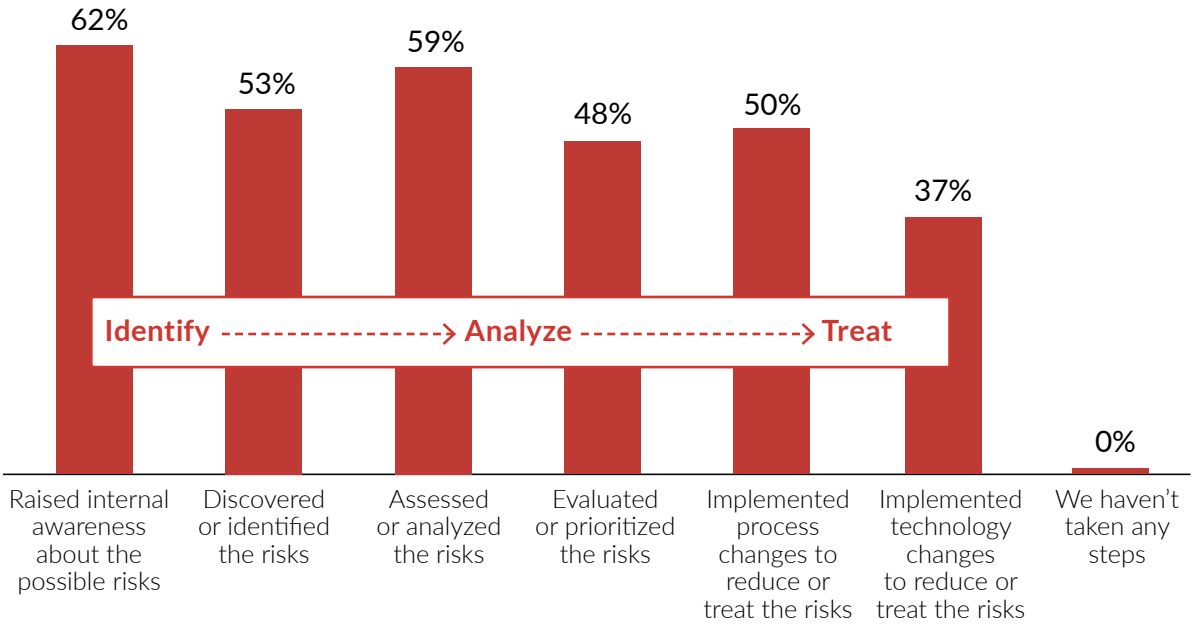
*n=1, 034*

Finally, while the major areas of risk remain the "usual suspects," such as security, compliance, resiliency and third-party risk, digital business is bringing nuances to technology risk that are unique. Traditional risks have evolutionary elements of change; for example, monitoring security in the cloud is different than monitoring security within on-premises environments. In addition, architectures related to digital initiatives create emerging areas of risk, such as risks related to API environments, consumer IoT, and unprecedented data creation and aggregation. Many leaders are grappling with where to start, where to go next, and how to keep a sustainable and evolving strategy aligned with the business.

In the RSA Digital Risk Report First Edition, based on the North American results, we noted that organizations may be behind in educating and initiating risk management efforts related to digital transformation. The global findings were not much different. Ultimately, organizations must implement the basic risk management lifecycle (identify, analyze and treat risk). While many organizations have taken steps (0 percent of the respondents said they have not taken any steps), there is still a majority of organizations that have not gotten past the initial parts of the process. Both process and technology changes are generally necessary to address risk, but only half of the respondents' organizations have implemented process changes; 37 percent of the respondents indicated their organizations had implemented technology changes to reduce or treat risks.

Figure 10. Steps Taken to Manage Risks

*What steps has your organization already taken to manage the risks that have emerged or increased as a result of your digital transformation? Select all that apply.*




*n=1,029*

## It Is Not Just About the Technology

**"One of our big risks is not aligning the digital experience with our customer base. We may put something in place that we think is what our customers are looking for, but our data intelligence [may not be] accurate and ends up not really providing the services that we were planning to provide." VP Risk Officer, Finance, U.S.**

Customer expectations today have transformed drastically. Customers expect on-time, always-on, up-to-date, immediate access to resources—whether it is their financial account or ordering something online. The stack of technology necessary to deliver digital products and services is a complex ecosystem with risks at every layer.

# Conclusion

Technology has certainly made the world a smaller place. Our ability to disseminate and access information has had radical impacts on the social and business worlds. As organizations fuel their operational evolutions and business model revolutions with technology, digital initiatives are changing the face of business across the globe. Based on the RSA Digital Risk Study, digital transformation is affecting all types of organizations, regardless of geographic region, organizational size and industry. The result is a combination of unique emerging risks and evolutionary changes to traditional risks. These changes are shifting risk management priorities as a function of an organization's digital strategies.

While cyber attacks, workforce dynamics and third-party risk are top-of-mind issues, every organization feels the effect of digital transformation in different ways. Multiple areas of risk must be addressed in a comprehensive, cohesive strategy. The Global RSA Digital Risk Study illustrates that, to meet the demands of the digital transformation efforts underway, security and risk management processes must leverage collaboration across IT, security and risk functions along with an increased involvement of the business.

# The State of Digital Risk in the Middle East

**Alaa Abdulnabi** and **Martin Sutherland**

The Middle East is in the middle of a massive digital transformation and poised to emerge as a leading digital economic powerhouse. If governments and businesses can withstand or work around existing tensions—and if public and private stakeholders can work together to align goals, funding and talent—the region could realize significant economic benefits.

The stakes are high. A McKinsey analysis found that a high level of digitization contributes to a country's economic growth, leading to higher GDP, and a unified digital market across the Middle East (160 million potential digital users by 2025) could increase GDP by up to 3.9 percent—or approximately $95 billion a year.[1] For the region's population, digital advancements can also increase access to, and improve the quality of, healthcare and education, not to mention reducing everything from poverty to CO2 emissions.

A McKinsey analysis found that a high level of digitization contributes to a country's economic growth, leading to higher GDP.

## Strong Governmental Support for Digital Initiatives

Middle Eastern governments are paving the way for digital transformation across the region, championing initiatives supporting the adoption of blockchain, AI, cloud and other digital strategies. Meanwhile, companies are working to define clear digital risk management strategies for new ventures—whether that's moving to the cloud, managing third-party relationships or expanding into new markets within the Gulf Cooperation Council (GCC).

Leading the charge is the United Arab Emirates (UAE), which published its first digital strategy nearly a decade ago, and has since launched strategies for AI, blockchain and more. Dubai was one of the first cities in the region to become a "smart city," with a goal of advancing citizens' happiness through technology and services.

Saudi Arabia is also well on the way to supporting digital transformation. The government and the Crown Prince are taking a leading role with **Vision 2030**, a plan that aims to reduce the country's dependence on oil, diversify its economy, and build digital skills and infrastructure. The Saudi government is developing policy and investing heavily in technology and digital transformation in both its public and private sectors.

Oman has launched a similar initiative, the Digital Oman Strategy, that lays a foundation for Omani digital society and e-government, with the goal of developing a sustainable knowledge-based economy based on digital service delivery.

## Advancing Blockchain

In Gartner's **2019 CIO agenda survey**, 60 percent of CIOs said they expected to adopt some blockchain technologies in the next three years. Tech companies and even governments in the Middle East are no exception, and many are leading the charge. The UAE government, for example, recently launched its **Emirates Blockchain Strategy 2021**, aimed at making 50 percent of government transactions with blockchain technology by 2021.

In Dubai, Sheikh Mohammed bin Rashid Al Maktoum's **Smart Dubai** initiative has launched its **Dubai Blockchain Strategy**, the UAE's first government-endorsed , enterprise-ready blockchain platform-as-a-service, designed to allow organizations in the UAE and elsewhere to move from blockchain testing and development to full production, while digitizing many government processes and citizen services.

And the Saudi Arabian Monetary Agency (SAMA) is looking to sign an agreement with a third-party blockchain cryptocurrency platform for a pilot serving Saudi banks. The goal: faster, more transparent cross-border transactions at a lower overall cost.

In Gartner's 2019 CIO agenda survey, 60 percent of CIOs said they expected to adopt some blockchain technologies in the next three years.

## Securing and Connecting Physical and Digital Worlds

In a region that prides itself on innovation and growth, boosters hope to use large global events, such as **Dubai Expo 2020** and the 2022 Football World Cup in Qatar, as showcases for rising digital and physical interconnectedness. This spotlight on the world stage adds pressure to deliver on the promise of digital transformation—while avoiding physical or digital threats to visitors and participants.

Dubai's expo will open in October 2020; over its 173 days, the event is expected to attract 25 million visitors from 180 nations, who will "connect, innovate and drive creativity" through an interconnected digital platform. Success will mean integrating cybersecurity and human safety features across all facets of the event.

## The Promise of AI

AI technology is another driver of potential growth across the Middle East. **PwC analysis** estimates the impact of AI on the region as high as $320 billion by 2030, roughly 2 percent of the global total. In the UAE, for example, the **Strategy for Artificial Intelligence** 2031 is aimed at deploying AI across the Emirates; the country's Minister of State for Artificial Intelligence predicts that integrated AI will **save the country's government billions** in the near future, radically reducing spending inefficiency.

## Moving to the Cloud

Cloud deployment in the Middle East is not as common as it is in other parts of the world, though infrastructure development is picking up speed. Governments are funding public initiatives, service providers are rushing to a lucrative market, and fast-growing small and medium-sized businesses are quickly adopting emerging technology. The cloud's data processing and storage possibilities make it essential to unlock the potential of new technologies such as blockchain and AI. For now, reports Gartner, despite an expected 1.8 percent year-over-year increase in IT spending—to an estimated US$160 billion total in 2019—the Middle East and North Africa (MENA) region is still lagging far behind its global peers when it comes to cloud spending. And Gartner doesn't expect the region to reach the level of cloud usage that the United States had in 2017 until the end of 2022.[2]

## With Digital Transformation Comes New Risk

The ongoing, ambitious and widespread investments in digital transformation across the Middle East demand an equally expanded view of risk. Just as important as sourcing the right infrastructure and technology is ensuring that it, and its users, are safe and secure. The region's dynamic political situation, as well as the high profile of several critical infrastructure companies, make the Middle East attractive to hackers—and second only to the United States when it comes to both cyberactivity and cyber attacks. To survive and thrive during the region's current wave of digital transformation, businesses must invest in solid, up-to-date risk management frameworks and cyber defense strategy, with a focus on effective management of IT, cybersecurity and digital risk.

Training employees to be good security citizens, to know what is suspicious and how to respond, remains a critical part of any company's security plan.

# The Human Side of Cyber Risk

**Tim Norris**

Decades of digital transformation have had an enormous impact on how individuals, companies, governments, NGOs and even criminals operate. One driving force in the digital revolution is expanding internet use. Today, more than half (53.6 percent) of the global population—nearly 4.1 billion humans[3]—is online. This interconnectedness is driving progress and empowering people on every continent with access to ideas, goods and services, and economic opportunity. Yet the internet—gateway to empowerment and backbone of the digital revolution—is not without its challenges. And that includes new and increasing cybersecurity risks.

## Bad Actors

Of those 4.1 billion internet users, not all have good intentions. In fact, the number of bad actors is on the rise, keeping pace with the ease of financial gain from cybercrime, and bolstered by a burgeoning black market for tools and forums that simplify and automate it. Just as digital technologies transform how organizations operate, the threat landscape, sophistication and volume of attacks dictates how hackers ply their "craft." And the cost to the global economy is huge—Accenture estimates the total global economic value at risk from cybercrime through 2023 at $5.2 trillion.4 It's no surprise that, in the Global RSA Digital Risk Survey, cyber-attack risk was ranked the number-one digital risk across all geographies and industries. Respondents, it seems, are keenly aware of the link between digital technology adoption and increasing risk profiles.

Today, more than half (53.6 percent) of the global population—nearly 4.1 billion humans[3]—is online.

## Addressing the Human Element in Cyber Risk

As the survey data shows, *everyone* is in some way at risk of cybercrime—which is becoming more and more prolific and difficult to manage. And while plenty of cybersecurity vendors will happily pitch you silver-bullet solutions, cybersecurity and risk management have many facets. So which should you address first?

**The importance of good digital citizenship:** Regardless of geographic location, business size or industry, one of the biggest cyber risks for organizations has a human face. When asked about digital risk, nearly all respondents in Ovum's 2019 Managing Digital Risk research report cited "human factors" as their biggest digital risk.[5] Identity remains the number-one attack vector, and stolen credentials are easy to get. Verizon's 2019 Data Breach Report attributes 21 percent of security breaches to human error, nearly a third of them involving phishing and 29 percent stolen credentials.[6] It's clear that even seemingly innocent mistakes—a click on a bad link or poor password practices—can still wreak havoc. On the organizational level, training employees to be good security citizens, to know what is suspicious and how to respond, remains a critical part of any company's security plan.

**A passwordless world:** Equally important is using technology to minimize such human factors. Multi-factor authentication (MFA), for example, moves security away from password-dominated access—promoting productivity while minimizing the impact of any stolen or compromised credentials. In a passwordless world, unauthorized access is no longer a vector for theft.

**Learn more about how RSA is managing consumer risks and promoting more strategic and effective identity and access management (IAM) programs.**

**Strengthening the human firewall:** Organizations are also taking proactive steps to identify risky or careless behavior—think of it as a shift in focus aimed at strengthening the "human firewall." For example, a large university in Saudi Arabia is working to score its staff's security practices, determining each employee's vulnerability to phishing attempts. The program uses technology and ongoing assessments to identify high-risk users, then responds with awareness education and training. Further steps could include overlaying dark-web intelligence on compromised credentials, or offering employees who pass phishing tests a financial bonus.

**Learn more about how cybercrime intelligence services can help shed insight into attacks targeting your organization.**

**Tech defense plus human expertise:** Advanced analytics, artificial intelligence and machine learning can also augment security skills gaps and automate security management by supporting better defense and detection. But adopting the latest and best tool doesn't eliminating cyber threat—you still need human experts to connect the dots and make decisions. And to help human experts recognize and prioritize threats, any tool you choose should offer a consolidated, singular view of the security landscape.

**Learn more about RSA solutions for threat detection and response.**

Adopting the latest and best tool doesn't eliminating cyber threat—you still need human experts to connect the dots and make decisions.

## Managing the Human Side of the Digital Revolution

The digital revolution is capable of creating opportunities anywhere on the planet—along with a new set of digital risks. As we work to protect privacy, data, business operations and human rights, we must rely on both digital and human capabilities. And because human mistakes are as inevitable as human brilliance, when it comes to ensuring security, we must use a combination of technology, awareness and training to help employees become more cognizant of their actions and improve behaviors. Next, we must use technology to simplify processes and strengthen intelligent responses to cyber threats. Only when organizations, governments and individuals work together to manage risk will we see a safer, more secure digital world.

# The Evolution of Fraud in Social Media

**Heidi Bleau**

Modern social media and networking platforms keep communities of like-minded people connected. But their advantages are often exploited by cybercriminals looking to profit from the anonymity, usefulness and global reach they offer.

In an initial RSA study of this phenomenon in 2016, social media-based cybercrime was occurring regularly, mainly on Facebook, QQ and Baidu. As newer platforms gained popularity, so did related criminal activity—extending to WhatsApp, Telegram, Instagram and Snapchat to name a few. Social media continues to be a hotbed of fraud activity with attacks increasing 75 percent in 2019 as online fraudsters look for new ways to steal personal information or peddle stolen goods while remaining largely anonymous.

Social media continues to be a hotbed of fraud activity with attacks increasing 75 percent in 2019 as online fraudsters look for new ways to steal personal information or peddle stolen goods while remaining largely anonymous.

## A Survey of Social Media Criminal Marketplaces

Fraudsters, like legitimate users, are attracted to social media platforms for several reasons. Three big reasons social media provides fertile soil for cybercriminals:

- **Built-in anonymity.** Screen names and customizable user profiles offer an initial layer of anonymity. Free webmail with no identity verification needed makes it even easier for cybercriminals to create anonymous accounts, each ready to be activated as soon as another is compromised.
- **Exclusive, invite-only structures.** Platforms' invite-only and group-management functions help fraudsters choose who they want to communicate and do business with. This enables fraudsters, whose primary concern even above making money is to remain anonymous.
- **Mobile integration.** Today's social media apps are optimized for mobile use, making it easy for fraudsters to monitor scams, make deals and dodge authorities, all in real time.

Across platforms, several interesting trends are shaping the social media fraud marketplaces:

- **Extended feature sets.** Peer-to-peer messaging platforms have evolved, blurring the distinction between instant messaging and social media, so fraudsters can communicate 1:1 or in groups without ever leaving their platform of choice.
- **Multiplatform models.** Fraudsters tend to frequent a wide range of social media-based fraud groups, often advertising scams from one platform to another, and jumping between platforms even mid-conversation. Content is also quite similar across fraud groups, with activity in multiple groups mainly serving to increase the fraudster's reputation and customer base.
- **Criminals thinking like users.** While there are differences between platforms, and reasons to choose one over another, when it comes to social media, fraudsters generally behave like typical business users—most try to be represented on as many platforms as possible, and to reach as wide an audience as possible, in order to maximize the profitability of their products or services.

# Social Media: A Global Bazaar for Payment Card Fraud

Whether they're trying to sell stolen payment cards or set up online credit card stores, fraudsters are using social media platforms as an international marketplace for criminal business. More than 50 percent of fraudulent social media activity observed by RSA is attributed directly to the sale of compromised cards and associated services. In 2019, RSA uncovered more than 26 million unique compromised payment cards, a 23 percent increase over 2018 totals.

An analysis of compromised payment cards recovered by RSA in the first half of 2019 shows that 92 percent of compromised payment cards for sale were attributed to just 15 countries.

Figure 1: Percentage of compromised payment cards by country

| Country | Percentage of payment cards for sale |
|---|---|
| United States | 41% |
| India | 17% |
| Spain | 11% |
| Brazil | 9% |
| United Kingdom | 5% |
| Italy | 5% |
| Australia | 3% |
| Turkey | 2% |
| Mexico | 2% |
| Malaysia | 1% |
| France | 1% |
| Germany | 1% |
| China | 1% |
| Ireland | 1% |
| Canada | 1% |

Credit card fraud stems from several factors. The more people in a region who fall for phishing or malware attacks, the more compromised cards those attacks generate. Another driver is how easy it is for cybercriminals to cash out stolen cards, such as by linking it to online payment services or committing e-commerce fraud. The increasing global reach of social media only multiplies these opportunities.

# Conclusion

Until new regulations or corporate actions limit malicious activity, cybercrime on social media will proliferate—and most likely, fraudsters will adapt to whatever is thrown at them, continually seeking new ways to profit from stolen financial and identity data. In the meantime, understanding the draw of social media can help us understand its attractiveness to the criminal element, and inform how we fight misuse. Social media offers consumer-facing businesses many opportunities—and almost as many risks. The more we know, and the better we track and report social media-based fraud, the more successfully we can target and thwart cybercrime.

The more we know, and the better we track and report social media-based fraud, the more successfully we can target and thwart cybercrime.

# The Unintended Risks of Workforce Transformation:

## The Careless Coworker and More Outrageous Stories

**Tony Karam**

Today, nearly one in three US workers—about 57 million people—earn at least part of their living through the gig economy.[7] Analyst predict 500 million new digital apps and services will be created in the next three years, doubling the number now available.[8] Throw in changing demographics and globalization, and you have a perfect storm of digital and workforce transformation. And as the ways we connect to each other and to information evolve, the pace of change will only accelerate.

On the organizational level, growing workforce transformation can increase communication, collaboration, agility and engagement. But when it comes to security, it can also introduce new access and control risks. An increasingly transient workforce creates a revolving door of joiners, movers and leavers—and generates new challenges in the areas of access management, regulatory compliance and insider threats. Meanwhile, the rapid adoption of cloud-based applications and technologies, the internet of things (IoT) and artificial intelligence (AI), give bad actors exponentially larger attack surfaces to exploit.

A larger, more diverse and more transient workforce means a wider range of personalities, work styles and motivations. To identify and mitigate, the attack vectors likely to do the most damage to a business, security and risk management teams must understand the different types of workers and the potential risks each represents.

An increasingly transient workforce creates a revolving door of joiners, movers and leavers—and generates new challenges in the areas of access management, regulatory compliance and insider threats.

## Meet the Careless Co-worker

What's the biggest risk to your business? It's most likely not malicious attackers, but rather the "careless coworker," according to a recent SANS report.[9] The Ponemon Institute found that, of 3,000 insider incidents it analyzed, 64% were directly attributable to employee or contractor negligence.[10]

"Negligence" sounds serious, but it's all too easy for any one of us to cut security corners when we're overwhelmed or on deadline—another recent study found that 45% of employees admit to engaging in unsafe security behaviors at work.[11] Topping that list: actions as seemingly innocent as connecting to public Wi-Fi and using personal email for work—both easy ways to compromise security and accidentally leak confidential information.

Consider the ramifications: a major city in Canada faced a $93M class action lawsuit in which it was accused of "acting with the most obvious neglect." The offense? A staffer accidentally sent an email, containing employee medical records, social insurance numbers, dates of birth and healthcare numbers, to someone outside the region.

**Learn more about the careless co-worker in the infographic The Five Faces of Dynamic Workforce Risk—along with how you can use user behavior analytics to spot insider threats.**

## Look, It's a Phish

When you hear the phrase "digital transformation," you probably think of the Cloud. That's no coincidence; increased reliance on cloud-based applications and data is both a hallmark of workforce transformation and the source of many of its biggest challenges, according to a recent SANS report.[12]

The report also identified email phishing as the top attack vector for digital risk, by far—as did a recent KPMG study of attacks on cloud-based services.[13] Taking advantage of common cloud services workflows, fake emails ask users to review privacy policies or update account information, including usernames and passwords. Any such access or identity compromise is bad. But imagine what hackers could do with stolen admin credentials, including accessing cloud management consoles, provisioning new (shadow) services or changing security or configuration settings.

**Discover more ways to protect against phishing, including how multi-factor authentication can help keep user credentials safe.**

## Can You See Me Now?

For corporate networks and systems, strong authentication and comprehensive access controls serve the same roles as the burly bouncers hired by any popular nightclub. But unlike your favorite club, few corporate networks have anyone watching what's going on inside. When asked which factors they believed most contributed to security incidents and breaches, most organizations listed insufficient monitoring and reporting of user activity.[14] In a 2019 report, for example, 34% of all data breaches investigated by Verizon involved inside actors.[15]

Not having visibility into what users are doing within your networks and applications can have real financial ramifications. For corporations, the cost of malicious insider attacks now averages US$1.6 million per year, a 15% annual increase over last year.[16]

Not having visibility into what users are doing within your networks and applications can have real financial ramifications. For corporations, the cost of malicious insider attacks now averages US$1.6 million per year, a 15% annual increase over last year.

And it's not just those **careless coworkers**. "Workforce risk actors," including **disgruntled employees** and **malicious imposters**, use valid credentials to access a wide range of data. The SANS study found increased monitoring and alerts to be the most effective controls for reducing workforce-related risks.[17] Continuously monitoring user behavior across the entire computing environment makes it possible to spot anomalous activity—and stop both accidental and intentional abuse.

**Learn more about user and entity behavior analytics (UEBA) and how it can help mitigate insider threats from both workers and external bad actors.**

## Looking Ahead

What does the future of workforce transformation risk look like? Will passwords finally become a thing of the past? Will continuous authentication and user monitoring become the norm? And will accelerating change translate to accelerating risk? One thing is certain: As the world becomes more connected, we need more reliable ways to assure that users are who they say they are, their access aligns with their responsibilities, and what they do with that access doesn't put the organization at risk.

Continuously monitoring user behavior across the entire computing environment makes it possible to spot anomalous activity—and stop both accidental and intentional abuse.

# Contributors

**Steve Schlarman**
Director and Portfolio Strategist, RSA, CISSP, CISM

Steve Schlarman leads RSA's research and thought leadership strategy for digital risk management. He has spent the last 10 years at RSA serving as the chief GRC and integrated risk management strategist for the RSA Archer® business. Prior to RSA, Steve was responsible for product development strategy at Brabeion Software, and he was a director at PwC for eight years.

**Jane Wright**
Market Intelligence Manager, RSA

Jane Wright has extensive experience as an industry analyst covering security, risk management and other IT markets. Prior to joining RSA, she worked for IT research firms, including Gartner Inc., where she was a research director, and Technology Business Research, where she launched and ran the firm's enterprise security practice. She also previously served as a senior editor for TechTarget's cybersecurity magazines. Jane began her career in IT at IBM as a systems engineer.

**Alaa Abdulnabi**
EMEA RVP | RSA Identity Business, Channel and Inside Sales Lead

As a leader in RSA EMEA, Alaa Abdulnabi focuses on building world class teams to help partners and customers manage all aspects of digital risk. With more than 16 years of IT and cybersecurity experience, Alaa has led various teams helping organizations develop effective risk management and security strategies, mature their processes and raise their security operations and incident response capabilities.

**Martin Sutherland**
General Manager META, RSA

As the RSA General Manager for the Middle East, Turkey and Africa, Martin brings over 25 years of IT and Security Experience working across a number of vertical markets globally. Prior to RSA, Martin served as CEO of British Telecom's Joint Venture in Saudi Arabia, BT Al Saudia, where he led the management team in defining the company vision and strategy, transforming the organization and its go-to-market portfolio and expanding their digital offering into next generation verticals. Martin has also led teams in Africa, Europe and the CIS region for Bytemobile (and the Citrix Bytemobile Business Unit), Vantrix and IBM.

**Tim Norris**
Product and Solution Strategist

Tim Norris is a Product and Solution Strategist where he is focused on helping organizations address the security and risk management challenges that come from digital transformation. His diverse background has centered around translating technical jargon into tangible real-world solutions that span technology, people, and process. At RSA, Tim is focused on cyber-attack risk through research, customer engagement and analyst relations to validate key learnings and evangelize technology solutions that address both security and business risks associated with our increasingly digital world.

**Heidi Bleau**
Senior Manager, Digital Risk Solutions

Heidi Bleau has nearly 20 years of experience leading marketing strategy and thought leadership programs for high-tech companies. In her current role at RSA, she helps lead the global go-to-market strategy for digital risk management. Prior to her current role, Heidi was the Global Marketing Lead for RSA's Fraud & Risk Intelligence solutions. Heidi is an avid blogger and frequently contributes to the media on topics related to cybercrime and fraud.

**Tony Karam**
Senior Solutions Strategist, RSA

Tony Karam is currently a Senior Solutions Strategist at RSA. A big believer that security "takes a village", Tony brings to his role more than 20 years of B2B cybersecurity experience – including previously leading RSA's global authenticator strategy. Prior to his return to RSA, Tony held various senior-level marketing and product management roles at BeyondTrust, Positive Technologies and Wave Systems.

# About RSA

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.
For more information, go to **rsa.com**.


1 Enrico Benni, Tarek Elmasry, et al, "**Digital Middle East: Transforming the region into a leading digital economy,**" McKinsey & Company, October 2016.

2 Christina Lago, "**Cloud computing in the Middle East: The next big tech market?**," CIO.com, July 2019.

3 ITU Publications, **Measuring digital development: Facts and figures**, 2019.

4 Kelly Bissell and Larry Ponemon, **The Cost of Cybercrime**, Accenture Security, 2019.

5 Maxine Holt, "**Managing Digital Risk: A blueprint for safeguarding digital transformation initiatives,**" Ovum Consulting, 2019.

6 Verizon, **2019 Data Breach Investigations Report**, 2019.

7 Gallup Workplace, **The Gig Economy and Alternative Work Arrangements**, 2018.

8 Frank Gens et al, **FutureScape: Worldwide IT Industry 2020 Predictions**, IDC, Oct. 2019.

9 David Hasar, **Workforce Transformation: Challenges, Risks, and Opportunities**, SANS Institute, December 2019.

10 ObserveIT, **2018 Cost of Insider Threats: Global Organizations**, Ponemon Institute, April 2018.

11 Dimensional Research, **Dell End-User Security Survey 2017**, 2017.

12 David Hasar, **Workforce Transformation: Challenges, Risks, and Opportunities**, SANS Institute, December 2019.

13 Mary Ann Davidson et al, **Oracle and KPMG Cloud Threat Report 2019**, 2019.

14 David Hasar, **Workforce Transformation: Challenges, Risks, and Opportunities**, SANS Institute, December 2019.

15 Verizon, **2019 Data Breach Investigations Report**, 2019.

16 Kelly Bissell et al, **The Cost of Cybercrime**, Accenture/Ponemon Institute, 2019.

17 David Hasar, **Workforce Transformation: Challenges, Risks, and Opportunities**, SANS Institute, December 2019.