Welcome

Digital transformation. It’s inescapable, powerful and daunting. While it began slowly decades ago, in the digitization of information, infrastructures and ecosystems, its force is now felt in the digitization of our communities and even our interpersonal relationships. With connection speeds going up, data becoming the modern currency and the cost of storage going down, more has become possible, which has led to even more becoming imaginable. Yet digital transformation doesn’t come without ripple effects that disrupt traditional ways we engage with customers, our networks and each other.

As a leader in security and risk management for 35 years, RSA will continue to deliver game-changing innovations to help our customers address new waves of progress. RSA has contributed in many ways—from driving the early digital transformation of e-commerce through creation of certificate authorities that enabled secure transactions, to exercising leadership today in omnichannel fraud prevention; risk-based identity and access management; security analytics, threat detection and response; and integrated risk management.

Now, our customers look to us to help them achieve more ambitious transformation initiatives, as they adopt cloud computing, machine learning, IoT, autonomous vehicles and robotics. These advancements will enable them to accelerate business opportunities, create engaging customer experiences and modernize connected infrastructures. But digital transformation comes with digital risk, which has impact and consequence at a scale, scope and speed we are only just beginning to understand.

What is digital risk?

The unwanted and often unexpected outcomes that stem from digital transformation, digital business processes and the adoption of related technologies.

As organizations embrace the advantages (positive risk) of technologies, the volatile, hyper-connected nature of digital business amplifies the negative side of risk. Add ever-increasing cyber maleficence, complex digital privacy regulations, and consequential security and data privacy events to everyday business, and decisions once made by practitioners in functional silos are catapulted up to the boardroom. Organizations depend more than ever on digital business operations and digital products and services, all of which offer an infinite number of corners and crevices for risk to hide.

This report shines some light into those shadowy places and offers important perspectives on the state of risk in this digital world. As you take a more unified approach to digital risk, you will be able to anticipate challenges and understand what risks are worth taking. RSA’s mission is to help you evolve how you manage uncertainty in today’s high risk, digital world—so you can enable innovation and progress for your organization.

Holly Rollo
Senior Vice President & Worldwide Chief Marketing Officer
RSA
Table of Contents

RSA Digital Risk Study ................................................................. 4
  Introduction ................................................................. 4
  Transformation is in Progress .............................................. 5
  Top of Mind ................................................................. 7
    Digital Risk Management Priorities .................................... 7
    Risk #1—The Risk of a Cyber Attack .................................. 8
    Risk #2—The Risks Associated with a Dynamic Workforce .......... 9
    Risk #3—It Depends .................................................. 10
  Looking Forward .......................................................... 11
  The Need for Increased Collaboration .................................... 12
  Consequences of Digital Risk ............................................... 13
  Moving Toward Solutions ................................................ 14
  Conclusion ................................................................. 17

A CISO’s Guide to Talking to the Board About Cyber Risk ................. 18

Industry Perspectives .............................................................. 21
  Energy ................................................................. 21
  Financial Services .......................................................... 22
  Manufacturing and Logistics ............................................... 24

Practitioner Spotlight: Managing Third-Party Identity Risk Can Reap Rewards ..................................................... 26

Contributors ................................................................. 30
Introduction

RSA designed a survey to better understand organizations’ perceptions of—and priorities and plans for—managing digital risk. We define digital risk as the unwanted and often unexpected outcomes that stem from digital transformation, digital business processes and the adoption of related technologies. Six hundred qualified respondents, including security, IT, risk, compliance, operations and finance professionals, completed the survey in North America in 2019.

The survey revealed several key findings:

- Digital initiatives are prevalent across organizations of all sizes and industries, and organizations acknowledge their digital efforts present a unique set of risks.
- Digital risk comes in many forms, and risk management priorities are most often driven by an organization’s digital strategies. Cyber attacks, workforce dynamics, data privacy and process automation are top-of-mind issues affecting organizations’ risk management priorities.
- Organizations have digital transformation efforts underway, but in general, their risk management practices aren’t keeping pace with the rate of change and complexity that digital transformation brings.
Transformation is in Progress

Digital initiatives are prevalent across organizations of all sizes and industries. Six in 10 respondents who said they were engaged in digital transformation stated their organization has a high level of engagement, while only 12 percent indicated a low level (beginning and planning stages). These results were relatively consistent across industries (only respondents in the public sector reported significantly less engagement at this time), which show how digital initiatives are rippling across most industries. Due to a variety of pressures, including increasing competition, organizations are utilizing emerging technology to achieve a wide range of benefits—from optimizing existing internal processes to creating entirely new business models.

The digital world has its own unique sets of risks that are simultaneously connected to and distinct from physical world risks (e.g., natural disasters, health and safety issues, etc.). The fact that 94 percent of respondents said they understand the concept of digital risk indicates an awareness that digital transformation initiatives are changing the nature of risk within organizations.

With organizations’ significant focus on digital transformation and its unique impact on risk, broad definitions of digital risk are helpful to communicate the wide-ranging effects of digital operations.

---

**Figure 1. Organizations' Digital Transformation Status**

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

- 2% Planning
- 10% Beginning to Engage
- 25% Somewhat Engaged
- 63% Extensively Engaged

(n=600)

**Figure 2. Understanding of the Phrase 'Digital Risk'**

Are you familiar with the phrase ‘digital risk’?

- 68% Yes, and I have a complete understanding of this term
- 27% Yes, and I have some understanding of this term
- 1% No, and I’m not sure what it means
- 5% No, but I can guess what it means

(n=600)

*Response percentages may not add up to 100% due to rounding*
When prompted to indicate which definition of digital risk best reflects their understanding of the term, the largest proportion of respondents who have some understanding selected the definition that links digital risk to specific technologies such as artificial intelligence (AI), the internet of things (IoT), cloud and others. The second most commonly accepted definitions were split between one that broadly focuses on the risks related to digital transformation and another that narrowly focuses on cybersecurity risks specifically.

Given the prevalence of the emerging technologies in driving digital transformation, the two definitions involving emerging technologies and digital transformation are closely related and provide a wider lens that better reflects the true nature of digital risk.

Technologies such as IoT, social, big data and analytics provide new ways to optimize operations, but they can also change a company’s risk profile. Our survey results signal this: Nine out of 10 respondents reported their risk profile has expanded over the past two years due to digital transformation. In addition, 88 percent of respondents indicated they expect this expansion to continue over the next two years.
Key Finding

Digital transformation efforts are underway at many organizations and are changing those organizations’ risk profiles. Not only has change occurred over the last two years, but respondents also expect it to continue.

Figure 4. Expected Change to Risk Profile*

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

Top of Mind

Digital Risk Management Priorities

The primary objectives of an organization’s risk management program typically depend on its digital strategy. But the industry in which an organization competes also influences its risk management objectives, and our survey results bear this out.

Respondents whose organizations are currently engaged in digital transformation were asked to think about their organization’s strategy for managing the risks related to digital transformation over the past two years and the next two years, and we presented them with a variety of possible risk management objectives. Notably, each objective is ranked #1 by at least some respondents, meaning every risk management objective is someone’s top priority. Fewer than 1 percent of respondents stated their organizations do not have a strategy to manage digital risks, which further indicates that all these objectives matter to companies undergoing digital transformation.
## Risk #1—The Risk of a Cyber Attack

The top risk management objective for the past two years, as indicated by survey respondents, was not surprising: More than half (53 percent) of respondents whose organizations are currently engaged in digital transformation cited managing cyber attack risks among their top three digital risk management priorities. Cyber attack risk came out on top in an aggregate (i.e., across all respondents) view of the survey results.

### Managing Cyber Attack Risk is a Top Priority, by Size of Organization

(last two years—percentage of respondents who selected this objective as one of their top three, n=600)

<table>
<thead>
<tr>
<th>Employees</th>
<th>1,000-2,499 Employees</th>
<th>2,500-4,999 Employees</th>
<th>5,000-9,999 Employees</th>
<th>10,000 or More Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50.2% (1)</td>
<td>56% (1)</td>
<td>51.3% (1)</td>
<td>55.3% (1)</td>
</tr>
</tbody>
</table>

*Overall rank in parenthesis*

### Managing Cyber Attack Risk is a Top Priority, by Industry

(last two years—percentage of respondents who selected this objective as one of their top three, n=600)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Finance &amp; Insurance</th>
<th>Wholesale &amp; Retail</th>
<th>IT, Tech &amp; Telecom</th>
<th>Healthcare &amp; Pharma</th>
<th>Public Sector</th>
<th>All Other Sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>41.4% (2)</td>
<td>63% (1)</td>
<td>54.9% (1)</td>
<td>52.9% (1)</td>
<td>53.1% (1)</td>
<td>53.1% (1 – tie)</td>
</tr>
</tbody>
</table>

*Overall rank in parenthesis*

### Managing Cyber Attack Risk is a Top Priority, by Respondent’s Department

(last two years—percentage of respondents who selected this objective as one of their top three, n=600)

<table>
<thead>
<tr>
<th>Department</th>
<th>IT</th>
<th>Finance</th>
<th>Operations</th>
<th>Security</th>
<th>Compliance</th>
<th>Risk</th>
<th>Other LOB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>52.5% (1)</td>
<td>51.4% (1)</td>
<td>48.5% (2)</td>
<td>61% (1)</td>
<td>55.6% (1)</td>
<td>51.9% (1)</td>
<td>51.2% (1)</td>
</tr>
</tbody>
</table>

*Overall rank in parenthesis*

Cyber attack risk was clearly top of mind for respondents regardless of organization size or department. The fact that this risk ranked consistently for nearly all respondents suggests that managing cyber attack risk may very well be the most critical challenge facing organizations’ digital transformation today. Many respondents, when asked to consider these risks in the future, still identified managing cyber attack risk as the leading risk management objective.
Risk #2—The Risks Associated with a Dynamic Workforce

Coming in second place on the aggregated view of risk management objectives over the past two years were the risks that may arise from enabling a dynamic workforce. A dynamic workforce may work securely from anywhere using any device, which can provide many benefits but may also introduce or expand risks. Forty-four percent of respondents whose organizations are currently engaged in digital transformation placed this risk among their top three risk management objectives.

Managing Dynamic Workforce-related Risks is a Top Priority, by Size of Organization
(last two years—percentage of respondents who selected this objective as one of their top three, n=600)

<table>
<thead>
<tr>
<th>Size of Organization</th>
<th>1,000-2,499 Employees</th>
<th>2,500-4,999 Employees</th>
<th>5,000-9,999 Employees</th>
<th>10,000 or More Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>43.2% (2)</td>
<td>48.8% (2)</td>
<td>46.2% (2)</td>
<td>33% (5)*</td>
</tr>
</tbody>
</table>

Overall rank in parenthesis

*In organizations with 10,000 or more employees, managing workforce-related risks ranked behind cyber attacks, compliance failures, privacy risks, and cloud-related risks.

Managing Dynamic Workforce-related Risks is a Top Priority, by Industry
(last two years—percentage of respondents who selected this objective as one of their top three, n=600)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Finance &amp; Insurance</th>
<th>Wholesale &amp; Retail</th>
<th>IT, Tech &amp; Telecom</th>
<th>Healthcare &amp; Pharma</th>
<th>Public Sector</th>
<th>All Other Sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>43.2% (2 – tie)</td>
<td>37.3% (3)</td>
<td>49.6% (2)</td>
<td>44.2% (2)</td>
<td>37.8% (4)</td>
<td>53.1% (1 – tie)</td>
</tr>
</tbody>
</table>

Overall rank in parenthesis

Managing Dynamic Workforce-related Risks is a Top Priority, by Respondent’s Department
(last two years—percentage of respondents who selected this objective as one of their top three, n=600)

<table>
<thead>
<tr>
<th>Department</th>
<th>IT</th>
<th>Finance</th>
<th>Operations</th>
<th>Security</th>
<th>Compliance</th>
<th>Risk</th>
<th>Other LOB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>51.5% (2)</td>
<td>39.2% (3)</td>
<td>40.8% (3)</td>
<td>49.4% (2)</td>
<td>37.5% (3 – tie)</td>
<td>49.4% (2)</td>
<td>36.6% (4)</td>
</tr>
</tbody>
</table>

Overall rank in parenthesis

Notably, respondents’ views of the importance of managing this risk in the future varied widely. For example, more respondents in the public sector believe this will be a risk in two years than think so currently, while fewer respondents from the financial services industry believe it will be a risk in two years than think so currently. Meanwhile, respondents working in operations roles believe this risk will be their main risk management objective, over both cyber attack and privacy risk, in two years. Clearly, the priority of managing the risks associated with a dynamic workforce is, well, dynamic. It certainly ranks high in priority generally, but various sectors have different perspectives on its relative placement.
Risk #3—It Depends

From an aggregate perspective, there was little consensus around the third most important risk area.

Almost four in ten respondents whose organizations are currently engaged in digital transformation cited managing data privacy as a main risk objective over the last two years. This tracks to the rise of different data privacy regulations and the headlines high-profile data breaches have made over the same time period. It also speaks to the priority of privacy driven by organizations delivering more digital products and services to their customers.

When respondents were asked to consider their objectives for the next two years, risks related to process automation and the use of AI, connected devices and other OT/IoT technologies rose to third priority, across all respondents. It’s no wonder: AI creates tremendous opportunity for organizations to learn more about their operations and streamline processes, but it also raises questions about the transparency, accuracy and fairness of AI models. IoT, too, remains an uncertain horizon for many organizations given the scale and scope of potential risks it creates.

### Third Most Common Risk Management Objective, by Size of Organization
(last two years, n=600)

<table>
<thead>
<tr>
<th>Size of Organization</th>
<th>1,000-2,499 Employees</th>
<th>2,500-4,999 Employees</th>
<th>5,000-9,999 Employees</th>
<th>10,000 or More Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Privacy</td>
<td>Process Automation</td>
<td>Data Privacy</td>
<td>Data Privacy</td>
<td></td>
</tr>
</tbody>
</table>

### Third Most Common Risk Management Objective, by Industry
(last two years, n=600)

<table>
<thead>
<tr>
<th>Industry</th>
<th>Finance &amp; Insurance</th>
<th>Wholesale &amp; Retail</th>
<th>IT, Tech &amp; Telecom</th>
<th>Healthcare &amp; Pharma</th>
<th>Public Sector</th>
<th>All Other Sectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Privacy</td>
<td>Dynamic Workforce</td>
<td>Process Automation</td>
<td>Data Privacy</td>
<td>Cloud</td>
<td></td>
<td>Cloud</td>
</tr>
</tbody>
</table>

### Third Most Common Risk Management Objective, by Respondent’s Department
(last two years, n=600)

<table>
<thead>
<tr>
<th>Department</th>
<th>IT</th>
<th>Finance</th>
<th>Operations</th>
<th>Security</th>
<th>Compliance</th>
<th>Risk</th>
<th>Other LOB</th>
</tr>
</thead>
</table>
Different Priorities for Different People

One thing the survey highlighted was that nearly everyone has a number one priority; it just isn’t the same priority. While managing cyber attack, dynamic workforce, data privacy and process automation risks rose to the top among all respondents, each risk management objective we presented is a top priority for the future by at least 7 percent of survey respondents.

For example, almost 10 percent of respondents in the technology and telecom sector ranked managing business resiliency risk as their top priority over the last two years, even though business resiliency ranked lower in the aggregate of all respondents. When looking at priorities for the next two years, almost 12 percent of respondents from large enterprises (10,000+ employees) ranked managing business resiliency risk as their top priority.

In simple terms, if this was an MVP or Academy Award voting process, every objective would have received at least 6 percent of the votes for winner.

Looking Forward

Looking at future risk management objectives, respondents’ viewpoints diverged by industry. 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.
The Need for Increased Collaboration

One topic that respondents overwhelmingly agreed upon—regardless of the size of their company, the department in which they work or their industry—is the need to build a strong coalition to manage digital risk. Ninety-three percent of respondents agreed that security and risk teams need to work together in a coordinated way to address risks associated with digital transformation.

Figure 6. Collaboration Between Security and Risk

<table>
<thead>
<tr>
<th>To what extent do you agree with this statement?</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 transformation.</td>
<td>Strongly agree: 56.2%</td>
</tr>
<tr>
<td></td>
<td>Somewhat agree: 36.5%</td>
</tr>
<tr>
<td></td>
<td>Neither agree nor disagree: 6.5%</td>
</tr>
<tr>
<td></td>
<td>Somewhat disagree: 0.5%</td>
</tr>
<tr>
<td></td>
<td>Strongly disagree: 0.2%</td>
</tr>
<tr>
<td></td>
<td>Don’t know: 0.2%</td>
</tr>
</tbody>
</table>

Respondents’ agreement on the need for security and risk teams to work together seems to validate the idea that traditional, siloed approaches to risk management create blind spots in organizations, since a lack of coordination between these two (and other) functions often impedes risk visibility and obscures the critical insights organizations must discover to make risk-intelligent business decisions. These blind spots highlight the challenges companies face operationalizing coordination among IT, security and risk management functions. The good news, according to our survey findings, is that respondents recognize the importance of driving this change.
Consequences of Digital Risk

Our survey results highlight the shifting responsibilities of today’s security and risk management teams. While protecting the business from harm remains a fundamental expectation for both functions, security and risk are now also expected to simultaneously create safe conditions for business relationships and build trust in the market.

Survey respondents were asked to indicate the two biggest consequences that could occur if their organizations were unable to manage their digital risks. Impact on financial performance, customer relationships and the organization’s reputation were most frequently cited, underscoring the concern among respondents that digital risk can have a direct impact on a company’s top and bottom line.

Figure 7. 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.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>our financial performance</td>
<td>28%</td>
</tr>
<tr>
<td>our customer relationships</td>
<td>27%</td>
</tr>
<tr>
<td>our reputation</td>
<td>26%</td>
</tr>
<tr>
<td>our customers’ businesses</td>
<td>23%</td>
</tr>
<tr>
<td>our market share</td>
<td>19%</td>
</tr>
<tr>
<td>our partners’ businesses</td>
<td>14%</td>
</tr>
<tr>
<td>our partner relationships</td>
<td>11%</td>
</tr>
<tr>
<td>our competitive position</td>
<td>10%</td>
</tr>
<tr>
<td>our overall viability</td>
<td>10%</td>
</tr>
</tbody>
</table>

$n=600$

Key Finding

Digital transformation efforts have a direct impact on organizations’ risk profiles. Organizations that are highly engaged in digital initiatives reported their risk profiles have expanded significantly due to their digital transformations. While managing cyber attack risk remains the main priority for many organizations, other risks are considered important, and managing those risks requires a coordinated and concerted effort from security and risk functions.
Moving Toward Solutions

Businesses must be comfortable embracing risk and leveraging new technologies to aggressively pursue market opportunities. In addition, business today demands an open, yet controlled, blend of traditional and emerging tactics. Consequently, organizations must manage the residual risks that emerge as they combine digital and traditional business operations, all while maintaining a highly secure and resilient business infrastructure.

Among respondents whose organizations are currently engaged in digital transformation, many have taken the first steps toward managing digital risk. They’re raising awareness inside their companies and beginning to analyze the risks. But much more work lies ahead to prioritize the risks and implement changes designed to reduce and treat digital risk.

Figure 8. 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.

- Raised internal awareness about the possible risks: 60%
- Assessed or analyzed the risks: 57%
- Discovered or identified the risks: 55%
- Implemented process changes to reduce or treat the risks: 54%
- Evaluated or prioritized the risks: 50%
- Implemented technology changes to reduce or treat the risks: 37%
- We haven’t taken any steps: 1%

There are many ways to interpret the results shown in Figure 8, but looking at the converse of the findings may reveal the most meaningful insights. For example, we can conclude that 40 percent of respondents’ organizations have not raised awareness about the possible risks related to digital transformation. Given that 88 percent of respondents said they expect their organizations’ risk profiles to expand in the future, as a result of their digital transformations (see Figure 4), this awareness gap could signal issues ahead. Risk teams that haven’t started an open dialogue with internal business partners about their expanding risk profiles may face an uphill battle as digital business efforts accelerate.
Even more worrisome, the lines of business (LOBs) driving transformation efforts may be underutilized when identifying risk. Over the last two years, IT was the department most likely to be involved in their organizations’ strategy around managing risks, and this trend is expected to continue, according to the survey results. However, fewer than 10 percent of respondents indicated that the LOB leaders driving digital transformation efforts inside their organizations are involved in risk management. This finding indicates that managing digital risk is largely viewed as the purview of technologists. With little involvement from the LOB leaders driving digital transformation, the whole organization could suffer from an inadequate understanding of the impact of these risks and a lack of alignment on the risk management priorities that matter most.

**Figure 9. 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?

Investments in the Future

Nearly all respondents (99 percent) expect their organization will invest in new or extended solutions/services to help manage digital risk. In the survey results, threat detection and response, data security, and IT and security risk management solutions topped the list of future investment priorities.
For organizations seeking solutions and services to help them manage digital risk, the main obstacles to investment include the pace of change and budget allocations relative to the magnitude of investment in digital transformation. Respondents indicated that justification is not necessarily an obstacle. Moreover, availability of sufficient products or services is also not a major obstacle, provided the organization has the time to implement the solutions and can redirect budget as required to effectively manage the digital risks.

Figure 10. Challenges to Digital Risk Management Investments

What challenges do you expect your organization will have as it invests in new or extended solutions or services to manage its digital risks? Select up to two.

- Must implement our digital transformation so quickly that we may not have time to implement risk management solutions (28%)
- Risks are expanding at a faster rate than we can expand our resources (26%)
- Our budget for the digital transformation will be directed to the digital transformation technology itself with little left over for related investments (25%)
- Budget is already allocated to our current infrastructure with little leftover for digital transformation projects (24%)
- Not able to hire or contract enough skilled staff (21%)
- Products and services available today are too difficult (19%)
- Products and services available today are not sufficient (19%)
- Too difficult to justify the investment to the department(s) that drives the digital transformation (12%)
- Too difficult to justify the investment to our executives or stakeholders (11%)

Key Finding

Organizations are laying the groundwork for digital risk management by building awareness and identifying key risks, but much work and investment remains to keep pace with the rapid rate of digital transformation.
Conclusion

While the benefits of the digital world have expanded growth opportunities, the forces of change are affecting organizations’ risk profiles today and the future priorities of their risk and security functions. The major areas of risk remain the usual suspects of security, workforce, operational and privacy risks, but the nature of digital business amplifies the impact of these risks. The most successful businesses will rise to the challenge of pursuing digital initiatives as pressure to innovate increases, while simultaneously navigating the new complexities and risks that stem from their digital transformation. This challenge is not for the faint of heart. Risk management effectiveness and value are hard to prove with a complex patchwork of tools and internal silos, which may put the business at even greater risk. The RSA Digital Risk Study reveals that as organizations plan their digital future, risk and security strategies must keep pace through awareness, collaboration, investment and relentless focus.

Survey Methodology

RSA commissioned independent research firm Vanson Bourne to execute the survey for the RSA Digital Risk Study. Six hundred respondents in North America completed the double-blind, online survey in May and June 2019.

To participate in the survey, respondents were screened for the following qualifications:

- Working full-time in a supervisory or higher role
- Working for an organization that is engaged in digital transformation, or planning to execute a digital transformation initiative in the next two years
- Involved in (such as influencing or approving) their organization’s digital transformation purchasing decisions

Guided by RSA, Vanson Bourne imposed quotas on the respondent pool to help ensure the results reflected a representative sample of organizations in North America that are or may soon be implementing digital transformations. Quotas were based on:

- Respondents’ departments (IT/Security/Finance/Operations/Compliance/Risk)
- Respondents’ organization size (1,000-2,499/2,500–4,999/5,000-9,999/10,000+ employees)
- Respondents’ industry (Finance & Insurance/Wholesale & Retail/IT, Tech & Telecom/Health & Pharma/Public Sector)
A CISO’s Guide to Talking to the Board About Cyber Risk

Steve Bergman
General Manager, Risk & Cybersecurity Advisory Practice, RSA Global Services

When chief information security officers (CISOs) first began appearing at board meetings to brief directors and top executives on cybersecurity, the experience was sobering for everyone. Directors wanted to know, in no uncertain terms, if their companies were at risk of experiencing one of these damaging security breaches they kept hearing about in the news, what the impact of such an event might be, and what the company was doing to prevent that from happening.

Few CISOs at the time had the quantifiable data or broad-based perspective they needed to answer these pointed questions. They did the best they could, citing highly technical details about software vulnerabilities and patching that provided little assurance to directors that the executive standing before them had this looming risk under control.

Today, boardroom discussions about cybersecurity risk have grown more commonplace—and more sophisticated. Results from the RSA Digital Risk Study indicate that managing cyber risk is a major priority for respondents, many of whom consider cyber attacks to be one of the risks most likely to derail a company’s digital (and business) strategy. Whether these risks impact revenue, regulatory compliance or a company’s reputation, most boards recognize that cybersecurity poses a new and unparalleled challenge to their company’s success. As a result, they’re dedicating key expertise and resources to oversee this challenge.

Drivers of Board Scrutiny

In 2011, the Securities and Exchange Commission (SEC) first issued guidance on the circumstances requiring public companies to disclose material cybersecurity risks and incidents. The SEC clarified and expanded the guidance in February 2018, citing the “grave threats” that cybersecurity risks pose to investors, the capital markets and the economy. Indeed, a recent study from Cybersecurity Ventures estimates that up to $6 trillion in global assets may be at risk from cybercrime by the year 2021.

Directors’ concerns about cybersecurity are also motivated by personal interest. No director wants his or her reputation tarnished by a dramatic and highly publicized cyber attack on a business that he or she is at least partly responsible for governing. This may explain why some directors are going so far as to form board-level subcommittees on cyber risk that sit alongside established audit, compensation and corporate governance committees. It may also explain why directors are looking to external advisors who can help them understand how best to govern this risk.

Fraud Attack Trends: 1H 2019

As boards and executives discuss their concerns about cybercrime, it’s important to understand the rising frequency of different attacks. The following fraud attack trends and analysis from the RSA® Fraud & Risk Intelligence team represent a snapshot of the global cyber fraud environment and provide actionable intelligence to consumer-facing organizations of all sizes and types to enable more effective digital risk management.

The total number of global fraud attacks detected by RSA increased 63 percent in the first half of the year.

- Phishing—6 percent increase
- Financial malware—80 percent increase
- Social media attacks—37 percent increase
- Rogue mobile apps—191 percent increase

Clearly, the increased activity supports the high level of concern boards feel about potential losses due to cybercrime.
Demands from Corporate Boards

Cybersecurity is clearly the facet of digital risk that’s most pressing to corporate boards today. While many corporate boards are still developing their cyber risk expertise, the most cyber-savvy boards are pressuring their organizations to mature their practices for identifying, assessing, quantifying and mitigating cyber risk. Specifically, directors want to see the following:

- A clear picture of the company’s cyber risk exposure
- Regular reports on:
  - the most significant cyber risks the company faces
  - the business impact of these risks (quantified in financial terms)
  - policies and controls the organization currently has in place to mitigate them
  - any existing gaps
- Assurance that the company’s cybersecurity and cyber risk management practices align with industry standards and frameworks
- Visibility into breach response plans
- Guidelines on the level of cyber risk the business is willing to accept based on the organization’s broader risk tolerance and appetite

Recently, cyber-savvy boards have grown increasingly focused on cyber risk quantification as a means of facilitating informed, data-driven decisions about cybersecurity priorities and investment. This has led executives across functions and business units to populate risk registers and use standard processes and frameworks for quantifying risk. The idea is to drive alignment among business decision-makers, risk owners and board-level committees on the level of risk the business is willing to assume.

Impact on CISOs

The increased demands from corporate boards for greater transparency into cyber risk are redefining the role of the CISO. CEOs and boards of directors expect their CISOs to function as strategic business leaders. They need their CISOs to work collaboratively with leaders across risk, finance, operations and other functions to gain that holistic picture of cyber risk and develop effective cyber strategies, governance models and capabilities that meaningfully address the cyber risks posed across the business. They’re also looking to their CISOs to serve as agents of security transformation capable of making the culture of the cybersecurity function more risk- and business-driven. This is new territory for many CISOs, and it’s forcing them out of their comfort zones of traditional cyber defense.

Some CISOs are meeting these challenges head on, particularly in the financial services industry where risk management and risk quantification are mature disciplines. The CISOs who have gained the confidence of their CEOs and boards by measuring and communicating risk in business terms are regularly “brought to the table” to weigh in on range of topics, from the value of cyber liability insurance to cybersecurity due diligence in M&A transactions.

CEOs and boards of directors expect their CISOs to function as strategic business leaders.
In many ways, CISOs and corporate boards are taking this journey to cybersecurity maturity together. They’re on parallel paths destined to meet—the CISOs honing their leadership skills, business acumen and understanding of risk, while corporate boards learn about the broadening and connected nature of cyber and other digital risks.

As digital transformation grows increasingly critical to organizations’ success and competitiveness, boards are justifiably questioning the associated risks and looking to engage in an open, informed dialogue on how best to mitigate them. The CISOs capable of engaging with the board at this level will be rewarded with the board’s commitment to their agenda.
Industry Perspectives

Industries today are facing a new wave of technology opportunities ranging from IoT and AI to cloud computing and big data. This wave of change is forcing risk management teams to rethink how they are going to address a much larger risk surface with an increased scale and complexity. The RSA Risk Transformation Office is made up of executive-level leaders representing a range of industries who assist by offering insights from their work with previous organizations as well as drawing on experience working with RSA customers. They help executives review and effectively tool risk strategies and roadmaps for success. The following are their front-line perspectives on the impact of digital transformation efforts in three key industries.

Energy

Michael DeLoach
Executive Director, RSA Risk Transformation Office

The energy industry comprises organizations that historically have exhibited varying appetites for cutting-edge technologies. In the oil and gas industry, pursuit of new fuel sources has attracted investments in technologies that have rivaled that of the space industry. At the same time, vertically integrated utilities that are heavily regulated have taken a more conservative approach. In some ways, the way we generate, transmit and distribute electricity has not changed much in 50 years.

But things are beginning to change. The endless pursuit of operational efficiencies, the advent of competition in areas previously considered monopolies, and ever-increasing regulatory oversight have set the stage for widespread digital transformation in the energy industry. For example, the control systems that operate the energy infrastructure have become more and more networked and digitized. Innovations in other industries have prompted energy companies to change the way they interact with customers—for example, by providing them with consumption data to help them make informed decisions about their energy usage. Environmental pressures combined with successes in fuel exploration (e.g., fracking) have changed the economics of energy supply, resulting in a fuel mix that is shifting from coal to natural gas and renewable resources. And in an effort to cut costs, energy companies are implementing cloud technologies to help run their businesses. All of these changes are altering the industry’s risk profile.

Meanwhile, natural and man-made events have disrupted the supply and distribution of energy at a time when society has become extremely dependent on technologies that run on electricity. The cyber attack on the Ukrainian electric grid in 2015 shined a spotlight on this very issue.

Collectively, these factors have grabbed regulators’ attention and pushed the industry to make significant investments in protecting what is widely recognized as a basic human need.

Going forward, energy companies will need to manage these risks with greater focus, discipline and diligence. While reactionary, ad hoc approaches to risk may have been acceptable in the past, these companies now need to take a structured and proactive approach. They may not be
able to predict the next cyber attack, but they can assess their cyber attack risk based on the criticality of their business processes and other factors, and invest in controls accordingly.

As a result of operating in an age of heightened risk and limited resources, energy companies are likely to take a risk-based approach to prioritizing investments. Projects intended to reduce risk will need to be justified based on the degree to which they move the needle. Risks that are more frequently encountered will need to be weighed against those that are less frequent, but that may have a bigger impact. This kind of analysis will require organizations to adopt risk frameworks to help them standardize their risk assessment methodologies and make them more repeatable.

Additionally, energy companies will need to rely more heavily on front-line employees who are seeing these risks firsthand and who possess “class A information” about them. For example, these employees may be network technicians whose burdensome workloads prevent them from doing all the necessary checks to ensure firewalls are configured properly. Energy companies need to give these employees a voice, perhaps by enabling them to contribute to risk registers and assessments. Energy companies will also need to couple top-down and bottom-up risk assessments to develop a holistic understanding of the risks they face across their enterprises.

Finally, these organizations will need to mature their risk management programs to the point where they can respond to current and evolving threats while also addressing future challenges in a sustainable manner. To that end, investment in integrated risk management systems will no longer be optional. Implementation of these systems will be a necessity for organizations seeking to manage digital risk and ensure that everyone has continuous access to safe, clean, affordable energy.

Financial Services

Mark Hofberg
Executive Director and Lead, RSA Risk Transformation Office, CISA, CRISC

Uber. Amazon. Zillow. GoBank. In today’s digital world, technology has opened up a multitude of new choices, channels and conveniences for consumers. And behind every digital consumer action, there’s a digital financial transaction: paying for a rideshare, buying a television on Amazon, borrowing money for a home—even saving for retirement. Banking and financial institutions are embedded in every part of people’s lives and the actions they take every day. There is nothing new about “digital” in the banking sector; there has been no sudden technology-based change. Banks have been digitizing processes since the use of magnetic ink character recognition (MICR) to automate physical check processing, the advent of automated teller machines (ATMs), the introduction of online automated bill pay and electronic payroll distribution, and, most recently, the rise of mobile banking. Banking was one of the first industries to embrace and benefit from digital transformation—and to recognize the risks it brings.

You don’t have to go back very far in time to find an example of the monumental role risk can play in the financial industry. Let’s take a quick walk down memory lane to 2008, when the banking system began to melt down in the wake of several major bank failures, including the...
fire sale of Bear Stearns to JPMorgan Chase in March and the collapse of Lehman Brothers in September of that year. These events and subsequent bank failures led to government bailouts and public outrage over irresponsible banking practices.

Financial experts continue to debate the causes of the banking crisis, but one potential contributing factor that bears mentioning is the lack of a standard risk framework for the industry. Following the crisis, we saw an enormous overhaul of the regulatory environment, coupled with a significant focus on risk and regulation, both internally within banks as well as externally via a myriad of regulatory organizations such as the OCC, FFIEC, Federal Reserve, FDIC, CFPB, SEC and so on.

After the financial crisis, we saw banks operating under new rules intended to prevent failures and protect the banking system. Integrated risk management technology, which evolved from governance, risk and compliance (GRC) technology, has played an enormous role in helping banks and financial institutions tackle risk management and compliance obligations. These risk management systems join people, processes and technology in a collaborative environment to ensure sound risk management decisions can be made with speed and agility, based on data.

Looking ahead, we can see the continued value of risk management as the banking space opens to new players. Recently, as part of an effort to drive modernization of the banking system, the U.S. Treasury Department’s Office of the Comptroller of the Currency (OCC)—in a move hotly contested by state regulators and industry associations—formally invited fintech companies to apply to become special-purpose national banks. As Comptroller of the Currency Joseph M. Otting said in a July 31, 2018 news release, "Over the past 150 years banks and the federal banking system have been the source of tremendous innovation that has improved banking services and made them more accessible to millions. The federal banking system must continue to evolve and embrace innovation to meet the changing customer needs and serve as a source of strength for the nation’s economy." This new opportunity for fintech companies to operate as nationally chartered banks will provide tremendous options for consumers, but these new “challenger banks” will face the same regulatory scrutiny and risks existing financial institutions face.

“Providing a path for fintech companies to become national banks can make the federal banking system stronger by promoting economic growth and opportunity, modernization and innovation, and competition,” Comptroller Otting stated. Since the OCC announcement, more than 50 challenger banks have emerged across the U.S. including Varo Money, Chime, Grasshopper Bank, Joust and others. Through the OCC charter process, a regulatory framework is established to ensure these companies operate in a safe and sound manner while serving customer, business and community needs.

As digital transformation continues, the speed and impact of risks in a hyper-connected world will become more difficult to manage and will require rapid decision and response. Many challenger banks will face risks stemming from heavy reliance on third parties, and from the enormous effort required to institute anti-money laundering and anti-fraud capabilities, fair lending practices, payment processing and other digitally enabled processes. Integrated risk management will be critical to their success.
Effective risk management requires collaboration, integration, transparency and measurements that cross organizational boundaries. Digital banking will enable consumers to execute transactions with speed and agility and, assuming challenger banks adopt technology for integrated risk management, they should be a valuable addition to the U.S. banking system.

Manufacturing and Logistics

Chris Patteson
Executive Director, RSA Risk Transformation Office

The manufacturing and logistics sectors are on the front end of massive disruption. From AI, 3D printing and robotics to drones, self-driving trucks and IoT, technology is upending these industries.

Today, sophisticated manufacturing companies use so much technology on the production floor that the lines between manufacturers and technology companies have arguably begun to blur. Consider that Ford now files more technology patents than Google and Amazon⁶, and that today there are more than a million lines of code in the average high-end car⁷, compared with the roughly 1.7 million lines of code in the Windows kernel.⁸

It’s no wonder leading manufacturing and logistics companies are upping their digital technology game. As if competition within those sectors wasn’t stiff enough, today’s manufacturers and logistics providers face disruption from new, digitally enabled entrants pushing into adjacent markets. Think of the impact ride-sharing companies are having on car sales. Innovative startups are forcing entrenched companies to rethink their business models and how they operate.

In extreme cases, organizations that rest on their laurels and fail to respond quickly to disruption could follow the fate of Kodak. The risk of not innovating needs to be balanced with the risk that new, non-traditional competitors could topple your position in the market. Manufacturing and logistics companies need to evaluate the likelihood and cost of losing market share to an emerging competitor and put plans in place to offset those risks. Yet those plans may necessitate taking on more risks—e.g., investing in a new technology or acquiring a startup.

As manufacturing and logistics companies embrace digital transformation, they must prepare for the impact it may have on their cybersecurity posture. Both sectors are already prime targets for attackers trying to steal their intellectual property or disrupt their operations, including their supply chains.

This kind of cyber attack risk is widely expected to increase as manufacturers and logistics providers weave sensors and other connected devices deeper into their day-to-day operations. IoT expands these organizations’ attack surfaces, giving adversaries more entry points to exploit. Understanding how these technologies connect to your infrastructure and critical processes is the first step to mitigating these risks.

Cyber attacks often lead to a variety of other risks, including business disruption and privacy breaches. Take the case of the NotPetya ransomware, which taught manufacturers, logistics
providers and other companies tough lessons about business resiliency. In the wake of NotPetya, many companies resorted to employing decades-old manual processes in an effort to maintain business operations. But companies affected by the malware whose processes were newer and entirely digital were at a loss. NotPetya underscored the importance of not just having business continuity plans, but making sure those plans are accessible to everyone who needs them in the event of catastrophic disruption. It also highlighted the importance of incident management and response—in this case, how companies managed the ransomware incident once it started and how quickly they recovered made a palpable difference in reducing losses. Bottom line: As organizations become more dependent on digital technology, they need to understand how to operate during—and quickly recover from—a crisis.

With respect to privacy risk, many of today’s digital business strategies seek to engage consumers on a very personal level. This type of personalization requires manufacturers to analyze scores of data points about the end consumers of their products. At the same time, there are more and more local and global privacy regulations dictating what companies can and can’t do with customer data—and big fines for companies that violate them. So manufacturers need to make sure their digital strategies comply with a wide range of privacy regulations that may give consumers “the right to be forgotten” and that may require organizations to obfuscate consumer data, dispose of it after a certain period of time, or otherwise cause them to question whether or not they really need to retain it.

Finally, but no less important, manufacturers and logistics companies must contend with third-party and supply chain risk. Product pedigrees and supply chain trust are now required to mitigate the risk of malicious technology being introduced into products and other forms of tampering. This is leading some manufacturers to use blockchain technology to manage product provenance. At a minimum, combating this threat requires an understanding of the risk posed by third, fourth and Nth parties, combined with new levels of due diligence around upstream providers. Assessing ecosystem risks in this manner may help manufacturers determine if dual sourcing is an appropriate strategy for mitigating third-party and supply chain risks.

Cyber attack risk, resiliency risk, privacy risk and third-party risk serve to illustrate the interconnected nature of digital risk in the manufacturing and logistics sectors. The more interconnected these risks, the greater their impact. Managing these complex digital risks will require manufacturing and logistics companies to coordinate traditionally siloed functions like IT, security and risk management and to use standard processes and frameworks. The organizations that undertake the hard work of bringing these functions together will be in a better position to pursue digital transformation with confidence and reap the benefits of taking calculated risks.
Practitioner Spotlight: Managing Third-Party Identity Risk Can Reap Rewards

Angel Grant
Director, RSA Digital Risk Solutions, CISSP

When was the last time you looked at your third-party identity management strategy? As your organization embraces digital transformation efforts and innovations, it is the perfect time to innovate your third-party identity management strategy to improve convenience, minimize vulnerabilities and optimize identity governance.

During security and risk strategy planning, many organizations focus most of their time on insider and external threat actors; as a result, they often fail to create a digital risk security strategy for managing their third-party identities’ access controls. This results in vulnerabilities caused by lack of visibility and understanding of the true business risks arising from third parties outside their control, including fraud and theft, business interruption, reputational damage and data breaches. This risk escalates as more third, fourth and Nth parties gain access to networks, apps and critical data—including customer records, intellectual property, patient records, strategic plans, financial data and more.

Oftentimes, a negligent Nth party unintentionally compromises security by misusing partner resources, mishandling sensitive data or exposing weak security practices. In fact, according to a Ponemon study of third-party risk in the U.S. and the U.K., 59 percent of data breaches in 2018 were caused by a third party—yet only 16 percent of companies affected said they effectively mitigate third-party risks. Furthermore, in the U.K. alone, cyber attacks reported in the financial services sector have gone up 1,000 percent since 2017, with third-party failures involved in 21 percent of incidents.

Current methods of governing Nth parties and their access to critical online resources are not sustainable with the rapid growth of third-party ecosystems. Several factors increase the likelihood that your business will be impacted by these outside parties at some point in your relationship: the growing number of third parties in your ecosystem, the complexity of the relationships, increased regulatory scrutiny of these relationships and the many ways risk can arise from them. Also, the more critical your organization’s dependence on a third party, the more likely adverse impacts could be catastrophic.

Why Are Third-Party Risks Increasing?

Complex ecosystems
In years past, most third-party relationships typically involved similar organizations. Now third parties can be partners, supply chains, vendors, external technologies (IoT, APIs, AI), joint ventures, “gig economy” players and more. And this ecosystem is expanding exponentially because third parties are using more third parties themselves.

Workforce transformation: globalization and the revolving-door workplace
Organizations operating in multiple regions must address how workers in those regions often
need to comply with data sensitivity and privacy regulations in different ways. Combined with
the surge in contractor and gig employees (who have a "work anywhere, anytime, from any
device" mindset), this complexity makes it harder to manage the risk.

Inadequate third-party governance capabilities
Third-party risk is introduced when people don’t follow basic risk lifecycle management—which
starts with capturing known (new and changing) third-party relationships and verifying that
the third party fits within the organization’s desired risk profile before contractually binding
the relationship and initiating joint activities. If governance is not performed properly, it will
exacerbate 1) the “shadow” third parties that result when vendors are contracted directly by
business teams instead of through approved channels such as the procurement organization,
and 2) the pursuant “islands of identity” issues that result when user identities are stored in
multiple user stores without unified visibility and control.

Organizational silos between third-party risk management, security and business
Silos create even more exposure. These risks can result in direct losses, a loss of stakeholder
confidence and regulatory compliance exposure.

Expanding attack surface
Third-party workers’ mobile devices, cloud apps and IoT technologies have all created more
potential points of vulnerability for cyber attacks. Threats are becoming more sophisticated
and harder to detect—especially if they are managed by the third-party vendor.

Gain the Benefits—Not the Risks
Organizations must undertake a forward-looking third-party risk management strategy to
prepare for modern identity and authentication challenges. To properly prioritize actions, it is
important to understand your organization’s risk tolerance and have visibility into what your
third parties are accessing in the first place. Next, business context, identity insight and threat
intelligence data must be analyzed to create insight. Once data is collected, the next step is to
make sense of it and ensure it aligns with your risk tolerance.

- **Business context.** What is the impact on the business if a third party has rogue access to
  an application or asset? How critical is this asset?

- **Identity insights.** How confident is the organization that the user is who they claim to
  be at the time of access? Does the organization know enough about the user, what they
  should access and how they typically behave to drive access decisions?

- **Threat intelligence.** What does the organization know about potential threats to any
  aspect of how a user accesses resources—from the device they are using, to the network
  they are on, to whether the infrastructure supporting the access can be trusted?

This information must be considered to evaluate the level of risk, as well as the impact on the
business, for each access request. Once you have visibility and insight, you can take the right
action that is aligned to your organization’s risk tolerance.
Manage Third-Party Risk by Controlling Identity and Access Risk

Leverage machine learning and behavioral analytics to gain context and identity insights. Behavioral analytics not only provides stronger identity assurance, it also provides invisible authentication, removing friction from access. At the same time, it helps organizations adapt to the changing threat landscape without sacrificing a strong information security posture or compromising compliance obligations. Design your behavioral analytics risk strategy to identify patterns in three areas: network, user and device.

Adopt continuous authentication to strive for a zero risk and trust approach. Organizations achieve continuous authentication by building identity and device trust, continually assessing that trust based on the organization’s risk tolerance, and requiring additional authentication only when the level of identity assurance is beyond the established risk tolerance.

Govern third-party access with an automated, analytics-driven approach. This simplifies access approvals and certifications, and speeds provisioning and deprovisioning, while managing gaps like overprivileges, segregation-of-duties violations or requests that need extra attention. Many times, external users—like consumers, third parties and open APIs—are granted access to sensitive information or to roles inconsistent with their needs, creating vulnerabilities. Automating the governance process of third-party access helps mitigate risks.

Tear down the silos with a holistic digital risk management strategy. Third-party identity management must become more integrated into security, IT, risk and compliance teams. The need for holistic digital risk management solutions will drive sharing of identity insights with threat management tools, and of threat intelligence with identity and access management systems. Such a strategy helps to ensure the broader visibility and context that organizations need to drive intelligent decisions, reduce false positives and increase security.

Understand the role identity plays in IoT authorization, authentication and governance. As we enter the IoT age, one of the fastest-growing third-party relationships is with devices doing things on behalf of humans. To successfully embrace this innovation, organizations must provide these devices with rules that align with authorized access and activities, and continuously monitor the devices’ entitlements.

Eliminate “shadow” third parties. To prevent unknown third parties from accessing your organizational resources, simplify the procurement process and educate business teams on the business and security risks they introduce when they bypass proper onboarding processes. It is vital to identify the types and amount of risk the third party poses to your organization (such as information security risk, financial risk, resiliency risk, strategic risk, environmental risk, etc.); know what digital channels third parties have access to; have basic treatments in place to keep risk at an acceptable level; monitor third-party online activities in real time; and respond to threats and fraud attempts originating from third parties.
The potential threat of an information security or fraud issue arising from a third party does increase digital risk dramatically. But a forward-looking risk management strategy will help you speed threat detection, investigation and mitigation—even as you embrace innovation.

Understanding what users have access to and knowing what they can do with their access are table stakes for any effective risk management program. Allowing third parties access and connectivity to sensitive systems and data is the new norm as organizations must embrace digital transformation to innovate and remain competitive. Remember, risk is OK—in fact, it is a good thing for your organization if it is managed properly. When you take appropriate steps to create a risk management strategy for third parties’ digital identities, you become able to confidently prioritize what matters most, whether that is performing access certifications, authenticating users to critical business assets or blocking rogue user access.
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.

Steve Bergman
General Manager, Risk & Cybersecurity Advisory Practice, RSA Global Services

As the leader of the RSA Risk & Cybersecurity Advisory Practice, Steve Bergman works with RSA’s largest customers to develop business risk and cybersecurity strategies that align with growth strategies. Measuring and quantifying risk to drive informed business decisions is a core focus of his work with C-suites and corporate boards. Prior to joining RSA, Steve held a variety of leadership positions: He served as CEO of personal data cloud analytics company 360ofme, CIO of Easter Seals and CIO of Goodwill Industries. In addition to his executive roles, he has led consulting and advisory engagements at both KPMG and Fortium Partners.

Chris Patteson
Executive Director, RSA Risk Transformation Office

Chris Patteson advises RSA customers on their integrated risk management programs. He also researches emerging risk modeling methods and techniques for cyber operations and compliance-based risk. Prior to RSA, Chris spent a decade with FedEx where he oversaw the company’s GRC infrastructure and managed a team of data scientists, application developers and forensics specialists to build new methods, models and architectures for managing fraud and cargo security.
Michael DeLoach  
Executive Director, RSA Risk Transformation Office  
At RSA, Michael DeLoach works with energy companies to mature their risk and compliance management programs using the RSA Archer Platform. A 27-year veteran of the energy industry, Michael has held leadership positions at Duke Energy and American Electric Power in engineering, IT, cybersecurity, reliability and regulatory compliance. He is a former member of the NERC Compliance and Certification Committee.

Mark Hofberg  
Executive Director and Lead, RSA Risk Transformation Office, CISA, CRISC  
As the leader of the RSA Risk Transformation Office, Mark Hofberg works with clients in banking and other industries to ensure their risk strategies meet the challenges of digital transformation. He brings deep financial services industry experience to his role at RSA, having previously served as senior vice president of operational risk management at one of the largest banks in the U.S. He holds a patent for a software selection process he developed and has another patent pending in process risk prioritization.

Angel Grant  
Director RSA Digital Risk Solutions, CISSP  
Angel Grant has more than 20 years of experience in the security, e-commerce and financial services industries. Prior to her current role, she led RSA’s Identity and Fraud & Risk Intelligence go-to-market solutions. Angel represents RSA on the FS-ISAC board, PCI Council Board of Advisors, and the Risk, Regulatory and Security Advisory Committee of NACHA’s Payments Innovation Alliance.
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.