CONTENTS

Executive Summary .......................................................... 3
The Cybersecurity and Business Risk Survey .......................... 4
Introduction ............................................................................. 5
The Shared Pain in Security and Risk ...................................... 7
A Convergence of Security and Risk ...................................... 10
Conclusion ............................................................................... 12
EXECUTIVE SUMMARY

Despite their best efforts and investments, some organizations still experience difficulty as a result of organizational, operational and even cultural differences between their IT security and business risk functions. These gaps can be seen in the ways security and risk teams describe their environments, their challenges and even their relationships with one another.

In early 2018, RSA commissioned the Cybersecurity and Business Risk Survey, executed by Enterprise Strategy Group (ESG), to learn more about the challenges and priorities of IT security and business risk professionals.

This report, which reflects select findings from the survey, is intended as a glimpse into the minds of security and risk leaders. It describes the pain these teams feel in pursuit of protecting their organizations’ digital assets and data, in the face of challenges from the forces of modernization, malice and mandates. Encouragingly, at the same time, it reveals another trend, suggesting that these teams are breaking out of their silos and starting to work more closely together toward their common goal of helping their organizations manage digital risk.

The survey responses indicate that these teams are embracing the convergence of IT security and business risk by prioritizing the interconnectivity of security and business functions, and by seeking to overcome the limitations of siloed strategies with a more inclusive approach. This kind of approach, driven by business priorities and context, is best positioned to protect what the organization values most. If one thing is clear in the survey’s responses, it is that working to establish common metrics, integrated tools and agreed-upon priorities can help these teams more effectively and efficiently manage the organization’s digital risk.
THE CYBERSECURITY AND BUSINESS RISK SURVEY

In early 2018, RSA commissioned an online survey, executed by Enterprise Strategy Group (ESG), to learn more about the challenges and priorities of IT security and business risk professionals.

The 175 respondents include a mix of IT/IT security professionals and business risk/governance, risk and compliance (GRC) professionals (see FIGURE 1) employed at organizations in North America, with at least 1,000 employees (see FIGURE 2), and in industries including, but not limited to, financial services, public sector, professional services, healthcare and manufacturing (see FIGURE 3).
INTRODUCTION

Defending the network isn't getting any easier, according to our respondents. The Cybersecurity and Business Risk Survey asked respondents to start by answering some big-picture questions to help set the stage. Of the results, a select few stood out as indicative of the current threat environment and the surveyed organizations' daily challenges.

When asked if their organization had experienced a security breach in the past two years, 70 percent of respondents confirmed they had (see FIGURE 4). What's more, 85 percent of those who had experienced a breach in the past two years actually experienced two or more in that timeframe (see FIGURE 5).

This grim trend isn't surprising, though. Today's attackers are able to employ the tools, techniques and procedures at their disposal to orchestrate sophisticated campaigns, target a specific organization or employee, persist until successful, and dig in for the long haul. This particular threat multiplier—dwell time—is a salient one for respondents: more than 60 percent overall said, in some cases, attackers had been on their network for several months prior to being detected (see FIGURE 6).

![FIGURE 4: EXPERIENCED A SECURITY BREACH IN LAST 2 YEARS?](Source: ESG Research, Cybersecurity and Business Risk Survey, March 2018; n=175)

![FIGURE 5: NUMBER OF SECURITY BREACHES IN LAST 2 YEARS?](Source: ESG Research, Cybersecurity and Business Risk Survey, March 2018; n=122)

![FIGURE 6: RESPONDENTS' BREACH INCLUDED DWELL TIME](Source: ESG Research, Cybersecurity and Business Risk Survey, March 2018; n=175)
Knowing more about the frequency and success of attacks, among these other insights, is critical to better understanding the overall threat environment. This is largely because such information is often closely guarded, because it could impact the revenue and brand reputation of the victim, even if reasonable precautions were taken. As such, most of the world tends to only see the big breaches that make the news, and that affects our understanding of the current state. From the perspective of the respondents, who live each day with the realities of security and risk management, the view is much different.

Despite the multitude of outside challenges highlighted in the responses, there is some agreement that change needs to come from within, focusing on bridging cultural and operational differences and creating a common language, expectation and measurement for security and risk management. Leadership can help; in fact, the convergence can only happen with real sponsorship and support all the way up to the board.

Fortunately, a resounding 82 percent of respondents believe their organizations’ executive leadership is on board with efforts to secure their network and data (see FIGURE 7), and 91 percent say their organization’s cybersecurity budget will increase in 2018 (see FIGURE 8).

The combination should be seen as good news; if organizations want to enact real change and start defending what they hold most valuable, this additional resourcing and support is critical to embracing and accelerating the convergence of security and business risk.

With this set of indicators, we can start to understand the general mindset of the respondents. This is an important context to keep in mind when considering the difficulties they experience from a lack of coordination between IT security and business risk.
THE SHARED PAIN IN SECURITY AND RISK

Security and risk teams not only experience challenges from external threats and actors; some of their pain comes from their internal relationship with one another. More than 70 percent of respondents agreed the relationship between the two teams can be difficult to coordinate (see FIGURE 9).

Respondents cited a number of relationship challenges, some of which spring from the cultural differences between security and risk functions, including differences in terminology, tools, and priorities. Business risk and IT security personnel tend to use different tools and language, exacerbating communication gaps between these groups, according to 69 percent of those surveyed (see FIGURE 10).

Overall, respondents went on to report how the differences in technology, language, metrics, structure, and goals created challenges that made improving the security-risk relationship more difficult (see FIGURE 11 on the next page).
Different tools and technologies (46 percent) stood out as the most cited reasons respondents felt they weren’t growing closer to their peers on the security or risk side of the business. Security systems tend to be very technical and focused on the infrastructure, identifying and addressing the perceived threat and stopping it first and foremost. Risk leaders tend to use different techniques, and thus different tools, focused more on the business to anticipate and assess risk based on their knowledge of the organization and the strategy. When security systems are not able to incorporate risk data, and vice-versa, then neither of these systems will be in concert when the data is used to make important decisions about what protections to invest in, where to apply them, and in what priority.

But the technologies they use are just a part of the web of cultural and operational factors standing between security and risk teams.

- **Terms and Language (41 percent):** Poor communication can be as problematic to the relationship as any technology challenge, if not more. Security performance is often described in pragmatic terms: hits, blocks, alerts, breaches. Risk management tends to use more speculative terms: likelihood, potential, impact. This demonstrates how some security and risk teams, not to mention their tools, may be talking right past one another.

- **Goals and Metrics (34 percent and 40 percent, respectively):** Understanding what success looks like (i.e., goals and objectives), and measuring against commonly understood indicators (i.e., metrics) are requirements in any business undertaking. Technology is where these understandings take shape, and can only provide what it has been asked to provide, based on the human understanding of direction and status.
• **Reporting Structures (39 percent):** With differing goals, it is not surprising security and risk teams have differing organizational structures and reporting hierarchies. This can confound cooperation, given that peer levels are not always clearly identifiable, and communication may move differently throughout each team structure.

These cultural divides are important hurdles organizations must clear to embrace the convergence of security and risk. Breaking out of strategic and operational silos is only useful in the pursuit of something larger, something that can truly work in the favor of both teams, and ultimately the entire organization. Fortunately, as divided as they may seem, there is additional data from the survey to suggest that many more security and risk teams are reaching across the gap that divides them, and combining forces to achieve a common goal.
A CONVERGENCE OF SECURITY AND RISK

Despite lingering challenges and uncharted territory for some, there are indications in the survey responses suggesting that a change is underway drawing security and risk teams together. To start, an overwhelming 93 percent of respondents to the Cybersecurity and Business Risk Survey characterized the relationship between their IT security and business risk teams as good or very good (see FIGURE 12).

This satisfaction with one another is crucial to encouraging these teams to develop security and risk management strategies in concert, fueled by context and enabled by visibility across the spectrum. The continued satisfaction with this relationship will be absolutely instrumental in enabling the convergence of security and risk.

The same pain points that separate these teams are noted as the areas where these teams are prioritizing their efforts. In another good sign, most respondents (82 percent) said their organizations consider security breaches as a business risk, not just a security risk (see FIGURE 13). This is just one simple, but critical, agreement that can help organizations bridge some of the aforementioned organizational and cultural gaps between security and risk teams, from language to goals and metrics.

Part of the problem with cultural and operational silos is that they prevent a well-rounded understanding of the strategic or tactical situation. One way to remedy this is to approach security strategy as a collaborative exercise that should include business risk management as much and as early as possible in the process. When asked about this, 41 percent of respondents agreed collaboration was the best action they could take to improve the security-risk relationship (see FIGURE 14 on the next page).
There are indications from the respondents that some teams are doing more than just thinking about the value of security and risk working together, and especially so in response to a previous breach. Following up on the aforementioned breach statistics, 44 percent of respondents said that their organizations increased coordination and communications between risk and IT security personnel as a result of a security breach within their organization or within their industry. Further, 43 percent said their organizations developed or enhanced an enterprise-wide business risk framework as a result of a breach (see FIGURE 15).

What business risk-oriented actions, if any, has your organization taken or expanded as a result of a previous security breach in the past two years at your organization or within your industry?
(Percent of respondents, N=175, multiple responses accepted)

<table>
<thead>
<tr>
<th>Action</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased coordination and communication between business risk and IT security personnel</td>
<td>44%</td>
</tr>
<tr>
<td>Developed or enhanced an enterprise-wide business risk framework</td>
<td>43%</td>
</tr>
<tr>
<td>Developed ways for business risk management and IT security teams to improve collaboration</td>
<td>42%</td>
</tr>
<tr>
<td>Invested in new software solutions to support business risk management process</td>
<td>42%</td>
</tr>
<tr>
<td>Increased executive management’s involvement in business risk management</td>
<td>41%</td>
</tr>
<tr>
<td>Found ways to leverage IT security tool investments to manage business risk</td>
<td>37%</td>
</tr>
<tr>
<td>Hired new or additional risk analysis staff</td>
<td>32%</td>
</tr>
<tr>
<td>Hired a Chief Risk Officer or other executive focused on business risk</td>
<td>29%</td>
</tr>
<tr>
<td>Purchased some type of cyber insurance</td>
<td>26%</td>
</tr>
<tr>
<td>None of the above</td>
<td>2%</td>
</tr>
</tbody>
</table>

FIGURE 15: TOP 2 RISK-ORIENTED ACTIONS RESULTING FROM A BREACH
Source: ESG Research, Cybersecurity and Business Risk Survey, March 2018
CONCLUSION
The Cybersecurity and Business Risk Survey sheds new light on the experiences and hopes of security and risk leaders in pursuit of the ultimate goal: protecting organizations from the increasing challenges of modernization, malice and mandates. RSA’s study contributes to the ongoing discussion about whether and how to rethink and strengthen the relationship between these teams, including how far they have come and how much further they still need to go.

The latter point is clear when looking at another facet of the responses, one that betrays a difference of opinion on the priority and direction of next steps. Some responses to this survey showed that, for all of their general agreement, the teams themselves don’t seem to agree on what steps are most important to pursue first.

For example, there was a notable difference between how IT/IT security and GRC respondents prioritized exposing risk managers to IT security initiatives early as a way to improve the relationship between the two groups. While 47 percent of IT/IT security respondents selected this as an option, the most popular response among the cohort, only 28 percent of GRC respondents felt this was a viable action to take (see FIGURE 16). Another salient example comes when respondents were asked about the importance of improving business risk identification tools and metrics (See FIGURE 16). As with the previous example, it was cited much more by IT/IT security respondents (36 percent) compared to GRC respondents (17 percent).

Which of the following actions could your organization take to improve the relationship between the IT security team and business risk managers?
(Percentage of respondents; IT/IT Security N = 122 and GRC N = 53; multiple responses accepted)

<table>
<thead>
<tr>
<th>Action</th>
<th>IT/Security</th>
<th>GRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expose business risk managers to IT security initiatives early so they can assess risk properly</td>
<td>47%</td>
<td>28%</td>
</tr>
<tr>
<td>Improve business risk identification tools and metrics</td>
<td>36%</td>
<td>17%</td>
</tr>
</tbody>
</table>

FIGURE 16: SECURITY-RISK DISAGREEMENT ON SOME OPTIONS FOR IMPROVEMENT
Source: ESG Research, Cybersecurity and Business Risk Survey, March 2018
In both of these examples, not only are these teams not in concert around key aspects of the security and risk management relationship, but also the IT/IT security respondents were more interested in taking firm steps to improve the gaps and consider business risk than the business risk respondents. Whether a cultural gap or a misunderstanding of where the important work needs to be done, fundamental discrepancies like these will continue to challenge security and risk teams, despite their level of commitment to the security-risk convergence.