RSA RISK FRAMEWORK
FOR CYBER INCIDENT RISK:
UNIFYING IT SECURITY
AND BUSINESS RISK
MANAGEMENT
EXECUTIVE SUMMARY
The worlds of business risk and IT security are rapidly converging. In a recent RSA-commissioned survey, 80% of risk and security professionals report that their organizations consider security breaches as a business risk rather than just an IT risk. Cyber risk has become an Executive and even Board issue that is receiving an unprecedented level of attention and scrutiny in so many of today’s C-Suites. This awareness is helping organizations evolve to optimize across both of these domains, and incorporate IT security activities into integrated risk management programs. However, it is also clear that IT security and risk management teams are often challenged by differences in the use of technology, language, and metrics when it comes to acting in a concerted way.

RSA recently undertook the RSA Cybersecurity and Business Risk Study to document and evaluate the challenges that organizations face in creating a mature, cross-functional strategy that optimizes every phase of the cyber incident risk management lifecycle. The study included a survey, commissioned by RSA and executed by Enterprise Strategy Group (ESG) in June 2018, of 306 IT security and governance, risk, and compliance (GRC) professionals working at large (1,000 or more employees) organizations in North America.

Study findings indicate that most organizations are at the early stages of operationalizing a cross-functional, business-driven security strategy, and they need assistance in coordinating and integrating cybersecurity and risk management.

RSA has created an RSA Risk Framework for Cyber Incident Risk to help organizations assess their maturity level and develop the most effective strategy for reducing risk within their unique environments. The Risk Framework provides a methodology and benchmarks for implementing a cross-functional, business-driven approach to cybersecurity that enhances all phases of the breach management lifecycle. Using the model, organizations can fortify their security posture, reduce business risk exposure, and maximize investment returns that utilize proven mechanisms for success.

This paper examines key findings of the RSA study, demonstrates the utility of the Risk Framework in addressing challenges identified in the findings, and offers a path forward for integrating and advancing business driven-security and risk management. It also shows how RSA offerings tie into the Risk Framework to provide a mature, unified solution that optimizes breach management at every step—from preparedness and prevention to detection, response, and process improvement. Using the RSA Risk Framework for Cyber Incident Risk and RSA solutions, IT and business functions can effectively join forces to sustain strategic control of cyber security and reduce business risk.
THE RSA CYBERSECURITY AND BUSINESS RISK STUDY: KEY CHALLENGES IN UNIFYING IT SECURITY AND BUSINESS RISK EFFORTS

Driven by a combination of Modernization (Digital Transformation), Malice (growing attack risk), and Mandates (intensifying regulatory requirements), organizations are seeking help in addressing requirements that are both large and difficult. It’s no longer realistic to protect all assets equally; effective strategies focus on determining the business value of assets, understanding the potential business impact of security threats, and then prioritizing asset protection based on what matters most to the business. This business-driven, risk-based approach leads to a more optimized distribution of resources across protection, monitoring, detection, and incident response. In its most mature form, it allows organizations to coordinate and integrate the breach management lifecycle across IT and business risk functions so that organizations can respond agilely, proactively, and optimally to any incident. In doing so, they are better positioned to minimize risk related to revenue/mission, reputation, and regulatory compliance.

RSA conducted the RSA Cybersecurity and Business Risk Study to investigate the challenges that organizations face in creating a mature, cross-functional strategy and to learn more about where organizations stand on the continuum of maturity. As part of the study, RSA commissioned Enterprise Strategy Group to identify the challenges that IT, IT security, and business risk leaders encounter and the best practices they recommend as they strive to manage cybersecurity and business risk more effectively.

For the purposes of this study, RSA groups respondents into two categories: 1) IT security, which includes IT and IT security respondents, and 2) business risk, which includes respondents working in governance, risk, compliance, auditing, and legal. Appendix A includes more information about the survey.

KEY FINDINGS
Following are key findings of the study and their implications for organizations working to advance a business-driven security strategy.

Most organizations consider security breaches to be a business risk, not just a security risk.
Eighty percent (80%) of respondents agreed or strongly agreed that their organization considers security breaches to be a business risk, not just a security risk.
IT security and business risk teams struggle to bridge the gap between their separate functions. Sixty-nine percent (69%) of respondents agreed that the relationship between IT security and business risk teams can be difficult to coordinate.

**Perspective on the Relationship between IT Security and Business Risk Teams**

Please indicate whether you agree or disagree with each of the following statements.

(Percent of respondents, N=306)

The relationship between business risk and IT security can be difficult to coordinate.

Source: ESG Custom Research, Cybersecurity and Business Risk Survey, June 2018

The most common challenge to establishing a strong working relationship between IT security and business risk groups is the use of different tools and technologies. When asked about their challenges, both IT security and business risk respondents pointed to “different tools and technology” more frequently than any other challenge. IT security respondents also cited different language and different metrics as top challenges, while business risk respondents said different reporting structures and different language were especially challenging.

**Challenges to a Strong Working Relationship**

What challenges are there to establishing a strong working relationship between IT security and business risk management?

(Percent of respondents, N=175 IT/IT security and 131 Business Risk respondents, multiple responses accepted)
IT security and business risk respondents agree on three actions that their organizations could take to improve the coordination between IT security and business risk managers.

When asked what actions their organizations could take to improve the relationship between IT security and business risk managers, both groups focused on improving the understanding and quantification of the impact of security breaches, getting executive management involved in the oversight of the two groups. Other helpful actions cited by IT security and business risk respondents included standardizing on common language and terminology and moving to more formal processes and communications between the two groups.

These responses serve as a guide for organizations that aim to integrate and advance cybersecurity and risk management. For example, organizations can apply a formal, overarching framework or methodology that provides specific guidance and sets a direction for improving communication between the IT security team and business risk managers so they can better understand the impact of security breaches.
IT security and business risk respondents both report that their organizations have some weaknesses with regards to breach detection and breach response. This finding indicates that effective threat defense continues to be a core concern across the organization.

Perspectives on Breach Detection and Response

Please indicate whether you agree or disagree with each of the following statements.

<table>
<thead>
<tr>
<th>Statement</th>
<th>IT Security Respondents (%)</th>
<th>Business Risk Respondents (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>My organization has some weaknesses with regards to IT and business role assignment.</td>
<td>64%</td>
<td>62%</td>
</tr>
<tr>
<td>It can be difficult to detect security breaches in a timely manner.</td>
<td>67%</td>
<td>56%</td>
</tr>
</tbody>
</table>

A cross-team incident response plan and breach detection training are important actions for preventing a security breach. When asked about the most important actions their organization could take to prevent a security breach, IT security and business risk respondents cited investing in breach detection technologies and developing an incident response plan—especially an incident response plan that extends to other parts of the organization. The top response for IT respondents was “Invest in security breach detection technologies” (44%), followed by “develop an
incident response plan within the security department,” and “develop an incident response plan that extends to other organizations” (both 42%).

**Actions to Prevent a Security Breach**

What are the most important actions an organization can take to help prevent a security breach?

(Percent of respondents, N=175 IT/IT Security and 131 Business Risk respondents, multiple responses accepted)

![Graph showing responses to actions to prevent a security breach.](chart)

Source: ESG Custom Research, Cybersecurity and Business Risk Survey, June 2018

There’s a lack of alignment with metrics and priorities between IT security and business risk professionals when responding to security incidents. The survey asked about the metrics that are most important to track in an incident response plan. IT security and business risk professionals’ answers were different, indicating a lack of understanding and cooperation that could make incident response less efficient and less effective. For example, 47% of IT security respondents said that dwell time (the length of time before an attacker or infection is detected) is an important metric for their organization’s incident response plan, whereas only 43% of business risk respondents selected dwell time. In addition, many business risk respondents pointed to detection success rate (41%), while only 38% of IT respondents selected this metric.

In a separate survey question, 60% of IT security respondents, compared to 57% of business risk respondents indicated that in some cases, attackers were on their network for several months before detection. Keeping in mind that business risk respondents were also less likely to consider dwell time as an important metric in an incident response plan, these findings highlight a lack of alignment and differences in perception—around metrics, terminology, breach impacts, and other elements—that can hinder organizations’
understanding or prioritization of risk. They also raise larger questions about what organizations would do differently and how they would invest if IT security and business risk activities (as influenced by tools, language, metrics, and perceptions) were more tightly coordinated.

### Awareness of Attackers on Network

We’ve determined that attackers were on our network for several months before detection in some cases. (Percent of respondents, N=175 IT/IT Security and 121 Business Risk respondents, multiple responses accepted)

<table>
<thead>
<tr>
<th>IT/IT Security respondents</th>
<th>Agree</th>
<th>Neither agree nor disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>26%</td>
<td>54%</td>
<td>17%</td>
<td>5%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Risk respondents</th>
<th>Agree</th>
<th>Neither agree nor disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>27%</td>
<td>50%</td>
<td>23%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: ESG Custom Research, Cybersecurity and Business Risk Survey, June 2018

### STUDY SUMMARY

To summarize the key findings presented in this paper:

- Most organizations consider security breaches as a business risk, not just a security risk.
- Organizations face challenges related to coordinating the relationship between IT security and business risk functions.
- Their most significant challenges are related to differences in technology, language and reporting.
- When asked about which actions to take to improve the relationship between the IT security team and business risk managers, both groups of respondents focused on improving the understanding and quantification of the impact of security breaches, getting executive management more involved in the oversight of both groups and moving to more formal processes and communications between the two groups. Other helpful actions included standardizing on common language and terminology and standardizing on common tools.
- Many IT and business risk groups recognize that their organization’s IT and business risk management skills are insufficient to effectively manage the cyber incident lifecycle.
- Organizations need more cross-functional collaboration, communication, and coordination in order to help prevent security breaches and improve the risk management lifecycle.

A lack of collaboration and communication between IT security and business risk groups raises questions about how differences in perception may impact decision-making, effectiveness, and overall risk. These findings support RSA’s field observations that organizations need help coordinating IT security and business risk functions in order to better identify, understand, prioritize, and mitigate risk. They also indicate that most organizations are still in the relatively early stages of maturity in terms of operationalizing a business-driven security strategy.
RSA has developed a model that enables organizations to systematically improve integration and coordination across IT security and business risk functions. Using this model, organizations can address security gaps or deficiencies, take steps to optimize the cyber incident risk management lifecycle, and reduce risk. The following section details RSA’s model for accurately assessing the current maturity of an organization’s security strategy and taking steps to methodically mature the strategy across the cyber incident risk management lifecycle.

**THE RSA RISK FRAMEWORK FOR CYBER INCIDENT RISK**

The RSA Risk Framework for Cyber Incident Risk provides a business-driven methodology and benchmarks for achieving a mature breach management strategy that reduces risk, regardless of an organization’s existing technology or use cases. Besides improving the ability to prepare for, detect, and respond to breaches, implementation of the model helps maximize the value of IT security and risk management investments by enabling organizations to extract and optimize the full range of capabilities within point solutions.

**UNDERLYING METHODOLOGY**

The model’s underlying methodology focuses on advancing the organization’s ability to:

- **Prepare**— Establish a well-defined, continuous, and adaptable plan that serves as the foundation of processes to reduce risk. Improve the organization’s capability to align business context, assets, and risk tolerance of the organization. Have an incident/breach response plan and regularly test it via staged exercises.

- **Reduce breach risk**— Respond to changing business requirements, threat intelligence, technology, and regulatory requirements to reduce the risk or impact of a breach.

- **Detect and analyze breaches**— Improve threat visibility and reduce dwell time. When a breach occurs, acknowledge the threat, determine its impact, monitor for continuous threat expansion, and identify the perpetrator.

- **Remediate**— Analyze, contain, and eradicate the breach. Determine steps to recover and/or mitigate its impact.

- **Adapt**— Document, evaluate, and leverage lessons learned to make changes that reduce future risk.
**Figure 1: RSA Risk Framework for Cyber Incident Risk – Maturity Assessment**

Different representations of the RSA Risk Framework for Cyber Incident Risk highlight different aspects of the model. Figure 1 shows the leading indicators of maturity across five main phases of the breach management lifecycle. A detailed scoring system behind these categories and ratings allows organizations to assess maturity for every phase and baseline an initial score based on the company’s risk tolerance. This tally can then be used as a reference point from which to prioritize investments, adjust strategy, and take other actions that advance IT security and risk management.

Organizations at the most mature level of the model optimize security and minimize business risk by coordinating and integrating IT and business risk functions across the entire cyber incident risk reduction lifecycle. Other characteristics of maturity include automation of key processes, advanced analysis capabilities, and continuous improvement of the incident management lifecycle.
Figure 2 identifies the types of capabilities that exist at each level of the model. In many cases, maturity progresses from manual processes to siloed digital processes to highly automated, integrated processes. Organizations at intermediate levels of maturity tend to rely on spreadsheets, online tools, and traditional SIEM tools coupled with non-integrated point solutions, and open source or free tools. The problem with this approach is that it rarely provides a holistic view of the breach environment and typically yields a slow and incomplete response. Lacking the insight, visibility and response forensics capable within today’s modern cyber incident response programs puts organizations at a strategic disadvantage to adversaries that employ the most modern means of furthering their causes.

USE CASES
Organizations of any size or cyber risk maturity can tailor the RSA Risk Framework for Cyber Incident Risk to address their specific use cases. Both RSA and non-RSA products map to the model, allowing organizations to maximize the value of existing investments. Organizations can further optimize operations by using tightly integrated RSA solutions.

HOW RSA SOLUTIONS MAP TO THE RSA RISK FRAMEWORK FOR CYBER INCIDENT RISK
RSA provides a rich portfolio of products and professional services that enable organizations to unify disparate IT security and business risk functions, advance their maturity model, and reduce risk. As shown in Figure 3, RSA Risk and Cybersecurity Practices and RSA product suites address every phase of mature breach management, from pre-breach preparation to post-breach adaptation.
Figure 3: RSA Risk Framework for Cyber Incident Risk (Excerpt)

RSA Advanced Cyber Defense Practice helps organizations advance their capability for continuous process improvement and helps ensure that security and business risk teams are well-coordinated and aligned with identified business tolerance levels when it comes to reducing risk.

RSA Incident Response (IR) Practice helps organizations coordinate security and risk management functions so that IR teams have all the information they need to respond quickly and decisively.

RSA Archer® Suite unifies governance, risk, and compliance management to increase visibility and insight into true business risks and empower organizations to make better decisions throughout the risk management lifecycle.

RSA NetWitness® Platform is an advanced security information and event management (SIEM) and threat defense solution that aligns business risk context to security risks so that security teams can rapidly detect and understand the full scope of a compromise and its associated risks.

RSA SecurID® Suite facilitates business by allowing legitimate users to quickly and easily identify themselves, while mitigating the risk of unauthorized users gaining access to the network and other resources.

CONCLUSION

The RSA Cybersecurity and Business Risk Study indicates that organizations recognize the importance of coordinating IT security and business risk functions, but they struggle to operationalize the concept of business-driven security. The RSA Risk Framework for Cyber Incident Risk provides a maturity model for developing a mature, business-driven strategy that is informed by—and accommodates—both IT and business risk functions across the breach management lifecycle. Organizations can apply products and solutions from the RSA portfolio to fully operationalize the model at the highest levels of maturity. In doing so, they can reduce risks to revenue/mission, reputation, and compliance while safely pursuing opportunities that allow them to thrive.
To find out more about using the Risk Framework to assess and optimize your organization’s security and risk management strategy, please visit rsa.com/risk-frameworks.

APPENDIX A – ABOUT THE SURVEY

RSA commissioned an online survey, conducted by Enterprise Strategy Group (ESG), of IT security, IT, and business risk management (governance, risk, compliance, auditing and legal) professionals in June 2018. The purpose of the survey was to identify the challenges that IT, IT security, and business risk leaders encounter and the best practices they recommend as they strive to manage cybersecurity and business risk more effectively.

Of 306 respondents, 57% worked in IT or IT security roles, and 43% worked in business risk management roles. The respondents were working in enterprises (1,000 to 4,999 employees) and large enterprises (5,000+ employees) in North America (the United States and Canada) with an annual revenue of $100 million or more. Respondents came from multiple industry verticals, including financial, retail, manufacturing, business services, telecommunications, and government.

<table>
<thead>
<tr>
<th>Sample size</th>
<th>n=306</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of IT/IT Security respondents</td>
<td>175 (57% of respondents)</td>
</tr>
<tr>
<td>Number of Business Risk* respondents</td>
<td>131 (43% of respondents)</td>
</tr>
<tr>
<td>Respondents’ company size</td>
<td>Enterprise and Large Enterprise</td>
</tr>
<tr>
<td>1,000-4,999 employees</td>
<td>150 (49% of respondents)</td>
</tr>
<tr>
<td>5,000 or more employees</td>
<td>156 (51% of respondents)</td>
</tr>
<tr>
<td>Respondent region</td>
<td>North America (U.S. and Canada)</td>
</tr>
<tr>
<td>Respondent industries</td>
<td>Primarily: financial, business services, engineering, retail/wholesale, telecommunications, manufacturing</td>
</tr>
<tr>
<td>Survey execution</td>
<td>March through June 2018</td>
</tr>
</tbody>
</table>

* Business risk respondents included professionals with GRC, governance, risk, compliance, legal, auditing and accounting job titles.

©2018 Dell Inc. or its subsidiaries. All rights reserved. RSA and the RSA logo, are registered trademarks or trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 08/18, White Paper, H17336 W 143570.