RSA

Security & Risk: How to Talk Digital Risk with The Board

Issue 1

Gartner

Answers for the Board: Navigating the Discussion Around Security and Risk

With the rise of the modern, digital enterprise, the discussion at the top of the organization has evolved. Information technology – once the purview of a few – is now the opportunity for many. As digital transformation creates unprecedented avenues for growth, the conversation at the executive level around technology has become more nuanced, more probing, more in depth – and ultimately, more complex. This shift is well known for those individuals tasked with presenting a concise picture of the risks related to business operations.

The conversation around risk though should not be a negative experience. Understanding uncertainty – both possible positive outcomes and potential negative events – provides clarity in decision making. While there may be major trepidation entering a board meeting to discuss risk, the dialogue is fundamental to survival in today's market. Fear of obstacles and challenges cannot stop organizations from growing. As strategies are built from top down, risk information presented to boards and executive teams will have a direct impact on a company's success in seizing opportunities in the market and driving future investment.

Security and risk leaders are handed a considerable challenge, but with that challenge comes the opportunity to profoundly impact your organization's strategy. Preparation is critical in getting the answers to the right people. In the following pages, we explore what it means to be a "risk-ready" enterprise and offer strategies and tactics, including those outlined in Gartner's report "Five Board Questions that Security and Risk Leaders Must Be Prepared to Answer," to ensure your next board meeting is a success. We hope you find these insights helpful as you prepare for the next discussion with your executive team. As always, RSA is focused on providing you with solutions on your journey into the digital future.

Steve Schlarman
Director, Product Marketing, RSA

Research from Gartner

Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer

As board members realize how critical security and risk management is, they are asking leaders more complex and nuanced questions. This research helps security and risk management leaders decipher five categories of questions they must be prepared to answer at any board or executive meeting.

Key Findings

- Interest in security and risk management is increasing at the board level, with 90% of security and risk management leaders having reported to the board at least once in the last year.
- Board confidence in the organization's ability to prevent and respond to incidents is low, with only a minority of boards expressing confidence in such abilities — a key deficiency that results in limited support.
- Security and risk management leaders often struggle to respond to board questions that are shaped by media reports and compliance concerns, leading to a cultural disconnect and breakdown of trust between business leaders and technology leaders.

Recommendations

Security and risk management leaders should:

- Categorize board questions into five types of queries and prepare responses that lead the discussion toward assurance, compliance and support for security practices.
- Develop the story of shareholder value in front of the board and the story of enterprise value in front of executives.
- Use this research to decipher complex questions to arrive at an outcome that balances the need to run the business against the need to manage risk.

Introduction

Interest in security and risk management (SRM) at the board level is at an all-time high. In 2019, Gartner conducted its security and risk survey and found that four out of every five respondents noted that risk influences decisions at the board level.[1]

Similarly, in 2016, Gartner estimated that by 2020, 100% of large enterprises will be asked to report to their board of directors on cybersecurity and technology risk at least annually (see "How to Build an Effective Cybersecurity and Technology Risk Presentation for Your Board of Directors"). In 2018, 91% of organizations having annual revenue of at least $1 billion have briefed the board on their cybersecurity program at least once in the last year.

It is difficult now to imagine that any board involved in the direction of a large company — and even a midsize organization — would not be aware of the public and government scrutiny on the topic of security and risk management. Boards today are more informed and more prepared to challenge the effectiveness of their companies' programs. In 2015, 22% of directors reported that their boards had no or very little knowledge of cyber risk. That figure dropped to 15% this year.[2]

Preparations for such dialogue usually focus on what the message contains. Boards want to know how the organization is performing; in fact, from a security and risk management perspective, they are required to know by many regulations that may hold the board liable if they fail to do so.

However, the numbers that illustrate board attitudes toward security issues are not reassuring. Although interest in risk management has grown, only 37% of board respondents feel confident or very confident that their company is properly secured against a cyberattack, compared to 42% last year. A slightly higher percentage (49%) is confident or very confident

in the ability of management to address cyber risk. But more than one-fifth of directors (22%) expressed dissatisfaction with the quality of cyber-risk information provided to the board by management.2

SRM leaders need to be able to give the board something that they care about and that is meaningful to them. But the confusion that results from the wider discourse around technology — including exaggerated, incomplete or contradictory public information — leads to asking the wrong questions, which the board nevertheless asks, over and over. These include: *How secure are we? Why do we need more money for security, when we just approved X last year? What do you mean we got hacked a hundred times?*

These questions distract from the most relevant aspects of the risk management discussion. Security and risk management leaders should orient their interactions with the board to ensure that the organization's leadership has the right understanding to support the overall security practice.

Once these conditions are identified, most board questions can be contextualized into one of five categories: the trade-off, the risk, the performance, the threat landscape and the incident.

Analysis

Communicating to the board should begin with an awareness of the audience: Who are the individuals on the board? What is their background? What role do they serve on the board — including any responsibility or background in cybersecurity?

Beyond individual passions and concerns, boards collectively usually care about three things:

- **Revenue/mission:** Operating or nonoperating income and enhancing nonrevenue mission objectives
- **Cost:** Future cost avoidance and immediate decrease in operating expenses
- **Risk:** Financial, market, regulatory compliance and security, innovation, brand, and reputation

Board members expect their leaders to interpret topic-specific information into its broader business impact. Security and risk management is one of these topics. Here, the board and the SRM leader will usually undergo a journey that revolves around maturity. This will often begin with simple questions that have no proper answers. For example, "Why is security so expensive?" Throughout this journey, perspectives may be shared and regulations may be enforced that impact this relationship. Eventually, the discussion will evolve into the ability of the security and risk management function to facilitate the digital ambitions of the organization, including achieving and maintaining competitive advantage (see Figure 1).

Regardless of where you think you might be on this journey, most board questions can be categorized into the following five buckets:

- The trade-off question
- The landscape question
- The risk question
- The performance question
- The incident question

The Trade-Off Question

> ***Example board questions: "Are we 100% secure? Are you sure?"***

The trade-off question is one that security and risk management leaders struggle with the most. These are questions that require improvising and are usually asked by board members who are unaware or uneducated around the impact of security and risk on the business. In this context, it's impossible to prevent 100% of incidents; the CISO's role is to help identify and assess the greatest risks for the organization and allocate finite resources toward managing them. In response to the question about complete security, a security and risk management leader might respond as follows:

"Considering the ever-evolving nature of the threat landscape, it's impossible to eliminate all sources of information risk. My role is to work with other facets of the business to implement controls to manage the risks that may prevent us from improving our brand image and operational efficiency this year. In security, there is no such thing as 'perfect protection.' As our business grows, we have to continually reassess how much risk is appropriate. Our goal is to build a sustainable program that balances the need to protect against the needs to run our business."

FIGURE 1 Board Questions About Security and Risk Management

"Here are some projects we will implement in the next 24 months that helps us achieve just that..."

Figure 2 illustrates a spectrum of risk management that leaders and teams can use to orient board conversations around appropriate risk.

The Landscape Question

> ***Example board questions: "How bad is it out there? What about what company X went through? How are we compared to others?"***

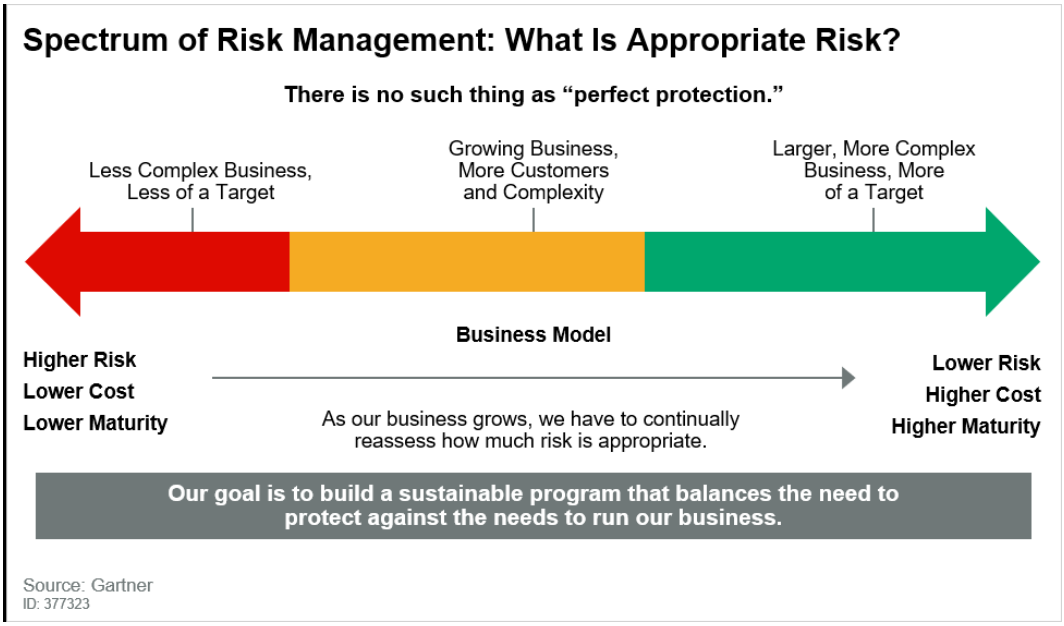
Most board members will want to know what the "weather" looks like. They will read threat reports, listen to broadcasts, read blogs and even be forced by regulation to understand many of these things. They will always ask for benchmarks and look to compare themselves against others, especially peer organizations. Gartner recognizes the need to discuss the landscape, but we also recommend that leaders try to move beyond concepts they do not have control over. Leaders should also avoid trying to quantify risks to the extent possible and attaching specific budget figures to the cost of mitigation based on something that is external. More importantly, while benchmarks provide some material for conversation, they should always be a negligible factor in the decision-making process.

In the threat context, leaders should avoid speculating on the root causes of events affecting other organizations unless they know for sure. The best response is:

"I don't want to speculate on the incident at Company XYZ until more information is available, but I'll be happy to follow up with you when I know more."

Note the relevant external developments, which may be recent, current or emerging events. Obvious examples involve notable incidents,

FIGURE 2 Spectrum of Risk Management: What Is Appropriate Risk?



but could also include such issues as regulatory change, changes to the global financial climate or political developments. Explain briefly what the development is, why it's relevant and what response, if any, your organization is making or will need to make.

If there is an external development that is not relevant, but which you know or reasonably suspect will be on the minds of the board members, then explicitly note it and explain why it's not relevant.

Figure 3 offers a series of responses that security and risk management leaders can use when discussing the broader security landscape.

The Risk Question

> ***Example board questions: "Do we know what our risks are? What keeps you up at night?"***

The board knows that accepting risk is a choice — a decision in response to the enterprise's known risk tolerance. Don't be afraid to remind them of this reality.

Any risks outside tolerance require a remedy to bring them within tolerance. This doesn't necessarily require dramatic changes in short periods of time; beware of overreacting. The board will be seeking assurances that material risks are being adequately managed, and subtle, long-term approaches may be appropriate in some instances.

Figure 4 presents a way to defend risk management decisions. The risk tolerance is illustrated in the diagram. You can change this line to suit your organization's own risk tolerance — make it fatter or thinner — and change the angle to reflect what you can live with. Note also that this chart shows that too little risk is just as undesirable as too much risk. Too much risk is obvious — we are an accident waiting to happen. However, too little risk means that we are probably strangling our organization's ability to be effective.

One of the most common issues we encounter is that assessments are quite subjective or based on flawed methodology. Leaders must have evidence to support the assessment, even if they are not called upon to present it. Serious decisions can be made on the basis of this type of diagram. If they cannot sustain the position, credibility is lost. Note that the risks in Figure 4 are expressed in business

FIGURE 3 Spectrum of Risk Management: What Is Appropriate Risk?

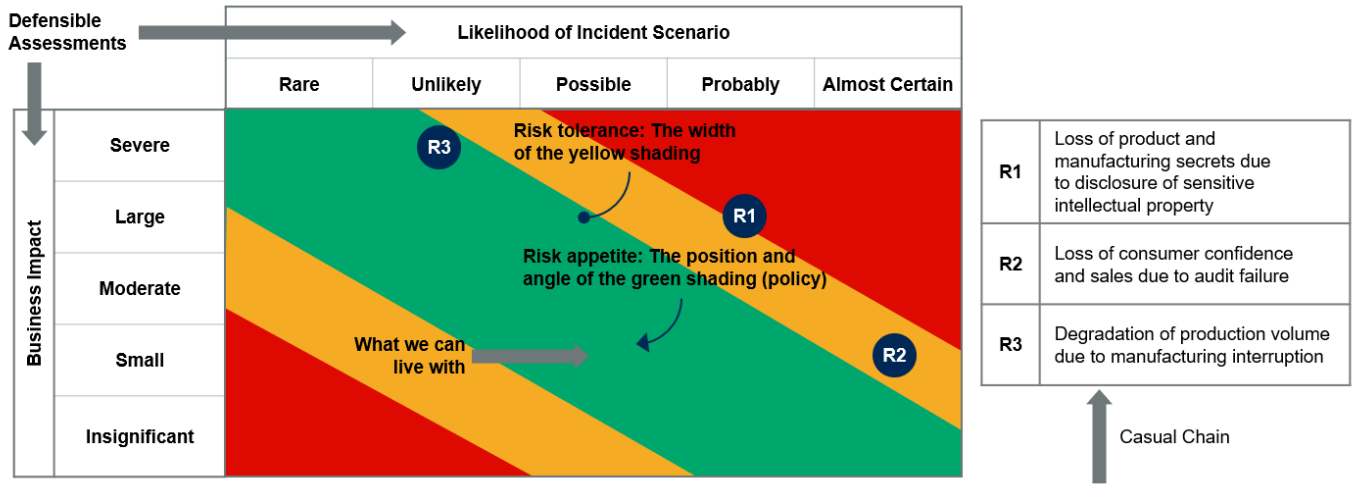
SRM Leader Responses to Broad Security Questions

External Event	Response
Our primary competitor suffered a widely publicized, successful attack.	• We have a similar weakness that could facilitate the same attack. We are addressing that weakness. • Enhanced monitoring capabilities have been implemented.
There has been an increase in attacks against electricity grids in three of our national points of presence.	• We do not anticipate becoming a direct target. • Business continuity plans are being updated and tested to overcome a prolonged outage.
We fall under the ambit of the new EU General Data Protection requirement.	• We have prudent and conservative privacy practices already in place. No changes are necessary.

Source: Gartner
ID: 377323

FIGURE 4 Material Risk Management

Show How Well (or Otherwise) Material Risks Are Being Managed



Source: Gartner
ID: 377323

impact, not in technical language, to ensure the audience will fully comprehend what is at stake.

Another aspect to consider is whether to portray the typical outcome or the worst-case outcome. For example, most security incidents result in mild outcomes that are well within the capacity of most organizations to absorb. However, there is the rare incident that results in a catastrophic outcome. Decisions around the presentation of typical risk scenarios or worst-case risk scenarios should be discussed with relevant executives such as the CEO, the CRO and the CFO.

The Performance Question

> ***Example board questions: "Are we appropriately allocating resources? Are we spending enough/why are we spending so much?"***

The board will want reassurance that security and risk management leaders are not standing still. If they have been effective in making the argument that security is always a moving target, then staff will need to demonstrate how the team is moving to ensure that the organization stays safe. This is particularly important in cases where the work program is based on management of the material risks. This is also useful for showing where the money is being spent and that it is not just a limitless quantity with no return.

Reinforce the projects that have been completed, and those that are in progress, but are tracking well. It's important to accentuate the positive.

Be ready to explain why projects are running over budget or will be late. The original strategy proposal should have included margins for error with respect to budget and deadline. As long as any overruns are within these margins, they should be noncontroversial. Even if overruns are outside those margins, there may be valid reasons. The main issue is that the board will be seeking satisfaction that the issue will be managed effectively, either by bringing about completion within reasonable limits, possibly with descoping, or, if necessary, by terminating failing projects.

Many leaders understand that security must contribute to business performance; however, they struggle to demonstrate how to do this. One method is the use of a balanced scorecard approach (see Figure 5) in which the top layer expresses business aspirations and the performance of the organization against those aspirations is illustrated using a simple traffic light mechanism. The performance is underpinned by a series of security measurements that are evaluated using a set of objective criteria.

This isn't the only way, of course. Some organizations may have a different type of dashboard to illustrate business performance, and this could be substituted in. For example, some organizations use a simpler set of between six and 10 metrics (see "Develop Key Risk Indicators and Security Metrics That Influence Business Decision Making"). The metrics and format used should be the same as, or consistent with, the metrics and format used to discuss security outcomes with line-of-business executives. Use whatever works for your audience.

The Incident Question

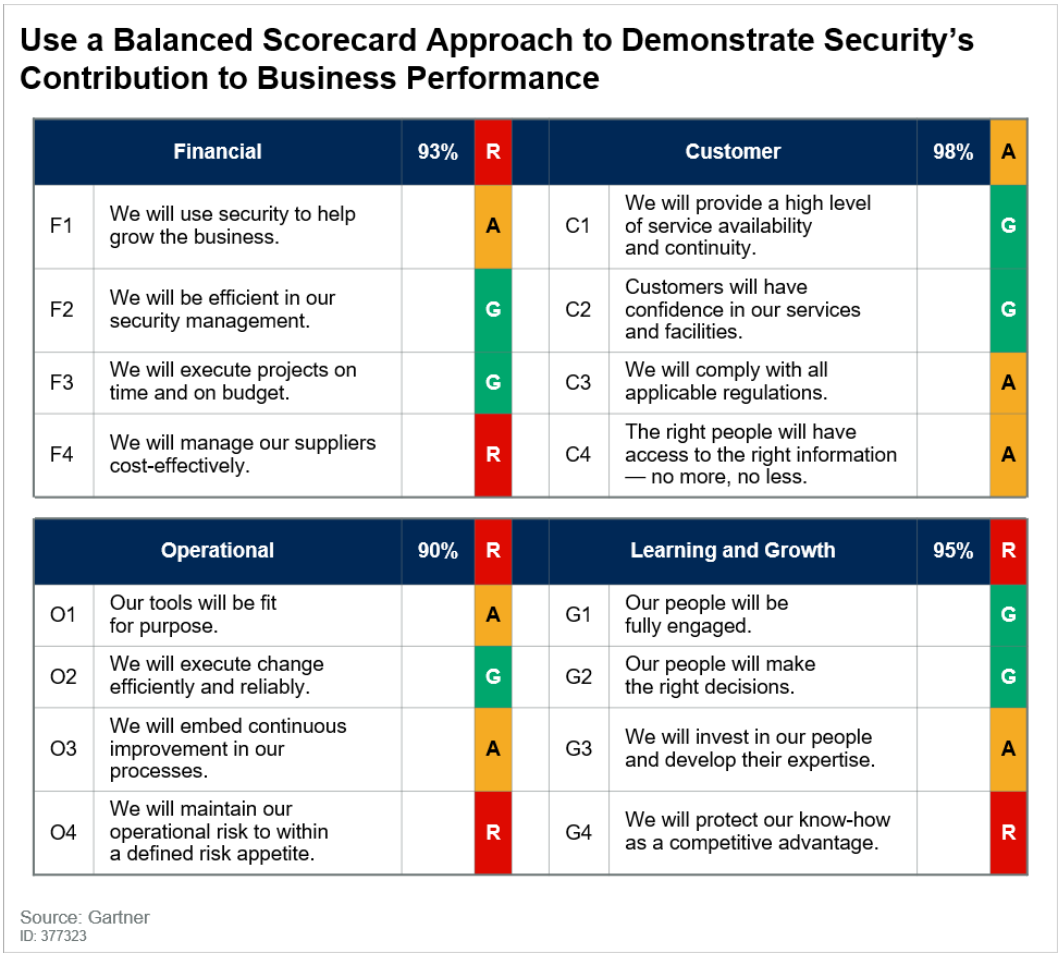
> ***Example board questions: "How did this happen? I thought you had this under control!... What went wrong?"***

An incident is inevitable. Treat it as a blessing in disguise, if possible, and as an opportunity to showcase your leadership skills. The details have to be kept within the context of the business. Leaders must be aware that in some cases the details of the incident may have been tightly controlled (for example, due to particular sensitivities associated with the incident). Therefore, it is possible that some or all board members may not yet be aware of the incident.

Adopting a factual approach, explaining what you know and knowing how you will investigate any remaining unknowns will remove the mystery and provide confidence that you are in control of the incident.

In short, acknowledge the incident, provide details on business impact, outline weaknesses or gaps that need to be worked out, and provide a mitigation plan. Arguably, the "ask" is the most important segment here (see Figure 6). If you are part of a risk-aware organization, then this will be one of many exercises you will undergo on a regular basis. In fact, organizations are now hiring security and risk leaders who have previous breach and incident response experience to supplement their programs.

FIGURE 5 Use a Balanced Scorecard Approach to Demonstrate Security's Contribution to Business Performance



Use a Balanced Scorecard Approach to Demonstrate Security's Contribution to Business Performance

Financial		93%	R
F1	We will use security to help grow the business.		A
F2	We will be efficient in our security management.		G
F3	We will execute projects on time and on budget.		G
F4	We will manage our suppliers cost-effectively.		R

Customer		98%	A
C1	We will provide a high level of service availability and continuity.		G
C2	Customers will have confidence in our services and facilities.		G
C3	We will comply with all applicable regulations.		A
C4	The right people will have access to the right information — no more, no less.		A

Operational		90%	R
O1	Our tools will be fit for purpose.		A
O2	We will execute change efficiently and reliably.		G
O3	We will embed continuous improvement in our processes.		A
O4	We will maintain our operational risk to within a defined risk appetite.		R

Learning and Growth		95%	R
G1	Our people will be fully engaged.		G
G2	Our people will make the right decisions.		G
G3	We will invest in our people and develop their expertise.		A
G4	We will protect our know-how as a competitive advantage.		R

Source: Gartner
ID: 377323

Lastly, leaders must be cautious not to endorse one option as the penultimate choice when in front of the board. The responsibility for oversight of security and risk remains with the SRM leader, but the accountability has to always be defined at the board/executive level.

Decipher Complex Board Questions

There are often no deterministic answers to most board questions. Responses are often more about presenting options for sponsorship rather than a definitive course of action. These options can differ based on maturity of the board, context of the discussion, the frequency of reporting, the communication skills of the SRM leader and so on. However, interpreting and answering board questions is a process that requires each party to understand their role in the process. In this case, the SRM leader must know that the board is ultimately interested in advancing the business goals, and any question that may seem ignorant, immature or perhaps even complicated has a purpose behind it. Gartner recommends that SRM leaders use Table 1 to decipher some common questions that fall into the categories outside of the ones discussed in this research.

FIGURE 6 Response to Board Questions About an Incident

Table 1. Responses to Common Questions Asked by the Board

Questions the Board Asks	What They Mean	What SRM Leaders Should Do
What is X? What should our approach to X be?	We don't know what bad, good or great looks like.	Provide definition and big-picture representation of what the enterprise currently has and specifically how it got that way.
Why do we need X, or why is X that way?	We don't know how to make decisions about this.	Map business capabilities to X and describe limitations of the current state.
What are our options regarding X?	Help us figure out the flexibility and levers we have in order to use this to impact business outcomes.	Co-create and negotiate the strategic story through a persistent focus on cost/value/risk trade-offs of the different options. Do not endorse an option you do not control.
How does X work?	Tell us how it works so we can tell you what to do.	Educate, demonstrate and create a framework story to guide the conversation.
Source: Gartner		

Evidence

This research is based on IT Score data and hundreds of client interactions including the review of over 90 board presentations from January 2018 through March 2019.

[1] 2019 Gartner Security and Risk Survey. This survey was conducted from March through April 2019 to better understand how risk management planning, operations, budgeting and buying are performed, especially in the following areas: risk and security management, business continuity management, security compliance and audit management, and privacy.

The research was conducted online among 698 respondents in the following countries: Brazil (n = 138), Germany (n = 135), India (n = 140), the U.S. (n = 142) and the U.K. (n = 143).

Qualifying organizations have at least 100 employees and $50 million (USD equivalent) in total annual revenue for fiscal year 2018. All industry segments qualified with the exception of agriculture, construction, IT services and software, and IT hardware manufacturing.

Further, each of the four technology-focused sections of the questionnaire required the respondents to have certain job roles/categories and have at least some involvement or

responsibility with at least one of the technology domains we explored.

The findings of this research refer specifically to the risk and security management section.

Interviews were conducted online and in a native language. The sample universe was drawn from external panels of IT and business professionals. The survey was developed collaboratively by a team of Gartner analysts who follow these IT markets, and was reviewed, tested and administered by Gartner's Research Data and Analytics team.

Disclaimer: Results of this study do not represent "global" findings or the market as a whole but are a simple average of results for the targeted countries, industries and company size segments covered in this survey.

[2] "2017-2018 NACD Public Company Governance Survey," National Association of Corporate Directors.

Source: Gartner Research Note G00377323, Sam Olyaei, Jeffrey Wheatman, 19 July 2019

The Habits of a Risk-Ready Digital Enterprise

It's D-day... The meeting starts at 9:00 AM. Carol's timeslot is a tight 20 minutes, squeezed between Human Resources and the afternoon break. As Chief Risk Officer, Carol knew she had to be on point. With an agenda full of critical topics, the board looked to her for guidance in balancing investments and risk. Her mind is swirling with the challenge of summing up the company's risk profile and the myriad of activities across the organization to contain emerging threats – while staying on time, in scope and dodging the potential rat holes of technical discussions. She feels prepared but still has the tinge of nervous energy she relies on to stay sharp. With a last sip, she finishes her morning coffee and takes a deep breath. Gathering her notes and laptop, Carol heads to the conference room. The quarterly board meeting is always a stressful day.

CROs, CISOs and other executives responsible for risk management today are frequently tasked with this seemingly impossible duty. Presenting a clear and coherent depiction of risk across a complex business is already a challenge. However, many times boards are unpredictable in their desire for essential information. Without a clear expectation, the resulting discussion can derail into irrelevant technical discussions or very high-level discussions that leave the board unsatisfied. One way to prepare for the inevitability of the board discussion is to adopt the key habits of a risk-ready digital enterprise.

Think of risk in an integrated manner. In a hyperconnected digital world where systems are strung together over complex infrastructures, risk is no exception. Risks are inherently connected. Risk-ready enterprises view risk in a horizontal and vertical manner – they understand strategic initiatives can be disrupted by tactical events; they know that tactical efforts must be prioritized in the context of the long-term vision. Silos are broken down on a regular basis to ensure collaboration and unified approaches are the foundation of the risk management strategy.

Blend people, process and technology. This phrase "people, process and technology" is used frequently, but putting it into practice can be difficult. There must be a balanced approach utilizing technology where appropriate, optimizing processes and ensuring skills and resources are well matched. Technical purchases and strategies are aligned with skills and process engineering that extend across IT and business.

Engage with the business frequently. Being risk-ready means your strategy evolves as fast as the business. This requires a regular discussion with a shared vision, stated business objectives and a consistent, rolling dialogue between business leadership and risk functions. Business decisions are based on balance of opportunity and risk and the only way to make the informed determination is to have a clear picture of both sides.

Anticipate change and prepare to pivot. Today's market is too competitive to recover from a total restart. Starting over is not an option. Risk-ready enterprises understand the stakes, and agility is expected and built in to the strategy. In the digital world, Agile is not just a development approach adopted by IT operations; it is a business strategy that requires vision, providing guidance without prohibiting flexibility.

ONE OF THE MOST VITAL PARTS OF A DISCUSSION ON RISK IS ESTABLISHING A COMMON VERNACULAR. THIS IS A FREQUENT CHALLENGE WE HEAR FROM CUSTOMERS. DEFINING THE MAJOR TERMS OF RISK PROGRAMS (RISK, CONTROL, ASSET, PROCESS, ETC.) AND THE MEASUREMENT SCALE FOR RISKS CAN BE A DAUNTING TASK FOR SOME ORGANIZATIONS. BUT THE REWARD IS WELL UNDERSTOOD.

AS ONE FINANCIAL SERVICES CUSTOMER RECENTLY STATED IN AN INTERVIEW, "WHEN EVERYONE IS SPEAKING THE SAME LANGUAGE, YOU UNDERSTAND WHAT YOU'RE MANAGING." A COMMON UNDERSTANDING OF RISK IS FUNDAMENTAL TO PROGRESS IN RISK MANAGEMENT MATURITY.

Seek ways to constantly improve. Risk-ready enterprises always have their eyes on the road, not just the rear window. One expectation of risk management is to learn from the past to predict the future, or at least not repeat mistakes. This means tracking meaningful leading indicators, not just lagging metrics. It also allows them to align risk management efforts with business milestones and adjust accordingly.

Understand success depends on others. Expanding business ecosystems are affecting more and more enterprises today. A digital business ecosystem is unavoidable so risk-ready enterprises accept that fact and enable it. External parties offer many benefits ranging from specialty skills to opening new markets, but they also can introduce complex risks. Third-party risk management must be executed inside the organization across functions as well as build the bridges to coordinate efforts outside the organization.

Do more than check the box. Technology can optimize and transform many parts of your business, but it isn't a silver bullet. The constant technology evolution and migration of existing operations utilizing emerging technology opens many doors. Risk-ready enterprises not only kick the tires, but also look under the hood. They search for opportunities to deploy controls that go beyond 'checking the box.' Their risk management strategies optimize the business and put in the right safeguards to move fast, but safely, during their digital journey.

It is 6:30 and Carol leans back in her office chair, proud of her and her team's hard work. The board was satisfied. She stayed on point, deflected distractions and painted a concise picture of the risk landscape. Although there were some rough spots in the past three months, she articulated the events in the context of the business to assuage the board's concerns. Their recent efforts to rebalance their strategy with a solid training program for staff, risk assessment process improvements and security technology deployments had paid off. Her regular meetings with the risk committee had allowed them to understand the strategies of the business unit leaders and anticipate organizational shifts, including the new channel strategy that opened a tremendous new market. The cherry on top was the kudos they received from their regulators recognizing their strategic approach to compliance.

All in all, it was a good day. As Carol powers down her laptop, her mind is already fast forwarding three months ahead, confident in the fact they are charting the right course.

Source: RSA

A CISO's Guide to Talking to the Board About Cyber Risk

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 Report 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 this 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.

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:

- 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.

Taking the Journey Together

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.

Source: RSA Digital Risk Report

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.