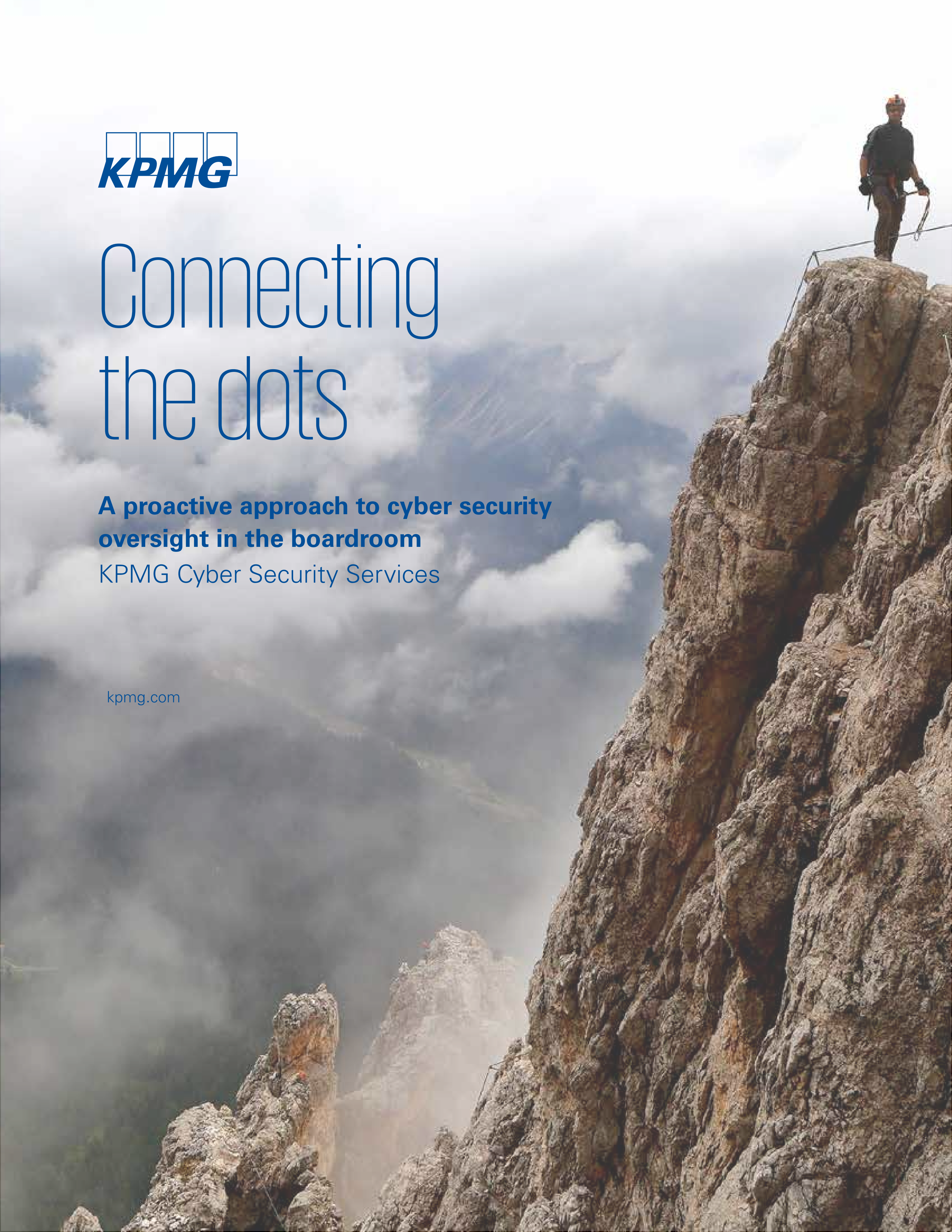


Connecting the dots

A proactive approach to cyber security oversight in the boardroom

KPMG Cyber Security Services

kpmg.com

Connecting the dots

A proactive approach to cyber security oversight in the boardroom

Leading organizations have long been attuned to the need for vigilance against cyber threats—and for many of them, cyber security has become a pillar of their risk management programs. Increasingly, however, leaders across industries are taking important steps to put cyber security at the foundation of their overall business strategies. Having moved the protection of critical assets outside the confines of the IT department, these leaders are making cyber security a valued part of their efforts to innovate and drive revenue growth.

How should the board respond in this rapidly evolving environment? With cyberattacks and data leakage posing daily threats to organizations globally, investors and regulators are increasingly challenging board members to step up their oversight of cyber security, calling for greater transparency around major breaches and the impact they have on the business.

Participants in KPMG's *2017 Global Audit Committee Pulse Survey* indicated that the effectiveness of risk management programs generally—along with legal/regulatory compliance, cyber security risks, and the company's risk controls—topped the list of issues these board members view as posing the greatest challenges to their companies. Indeed, more than 40 percent of survey respondents said their organizations' risk management program and process "require substantial work," and a similar percentage said that overseeing those major risks is increasingly difficult.

For their part, however, many business leaders already understand the need to address cyber security as part of their overall business strategies and not solely as an IT risk. According to KPMG's *2017 U.S. CEO Outlook Survey*, CEOs expect to make significant cyber investments over the next three years. In fact, 76 percent of CEOs see an investment in cyber security as an opportunity to find new revenue streams and innovate, rather than an overhead cost. These leaders increasingly understand that by adopting a more agile security strategy, they can expand the value of their cyber security efforts—from protecting critical assets to embracing new business opportunities and improving competitive advantage.

Board members need to consider what information they require to be able to assess their organizations' cyber security programs. Beyond focusing on whether management is appropriately addressing cyber risk, boards should begin to ask to what extent management is driving business value through cyber security. Certainly, directors need to hear from a chief information security officer (CISO) or CIO with subject matter expertise who can help them make informed decisions. But what should be their key areas of focus?

In our experience, board members are wondering: Am I asking the right questions? How do I get comfortable? Are we doing enough? How do I know we are doing the right things and making the right decisions? Assuming our assets are safe, is cyber security supporting business growth and innovation?

Cyber Security: a business and boardroom priority

By now, corporate boards understand that cyber security must be at the top of their agendas. Far from solely an information technology (IT) issue, cyber risks are an enterprise-wide risk management issue, and severe repercussions are resulting from the growing number and complexity of cyber events.

In just one recent example, following the revelations of the attack on the SEC Edgar database in September 2017, SEC chairman Jay Clayton warned: "Market participants also face regulatory, reputational and litigation risks resulting from cyber incidents, as well as the potential of incurring significant remediation costs." He noted, "Cyber security efforts must include, in addition to assessment, prevention and mitigation, resilience and recovery." And because cyber events "pose a systematic risk to our markets or U.S. financial stability," Clayton emphasized, "Issuers and other market participants must take their periodic and current disclosure obligations regarding cyber security risks seriously, and failure to do so may result in an enforcement action."[1]

Our research and experience reinforce the need for urgent action. Taking a proactive approach to improving cyber security governance—connecting the dots between IT and the business, and providing the board with the information it needs—can help position the company and the board to more selectively address the evolving threat and implications of a major cyber security breach. From there, they can consider their cyber security efforts through the lens of revenue growth and sustainability.

What is at stake?

Since many global organizations have been victims of cybercrime over recent years, board oversight of cyber security is no longer just a leading practice—it is a necessity. Investors, governments, and global regulators are increasingly challenging board members to actively demonstrate diligence in this area. Regulators expect personal information to be protected and systems to be resilient to both accidental data leakage and deliberate attacks.

While much of the conversation focuses on protecting privacy and personal data, boards need to take a larger view of the sensitivity—and value—of what the organization is seeking to protect. Cyberattacks damage the organization's reputation for trustworthiness, impacting its market value as well as the confidence and goodwill of its customers and suppliers. Such attacks threaten intellectual and physical property, resulting in delays or failures to deliver goods or information. Employees lose time in crisis management, and they are inevitably distracted from their day-to-day responsibilities. Just the effort to make the business whole, with all its stakeholders, can lead to considerable administrative cost and legal expense. Considering how much is at stake, ensuring cyber security must become a critical aspect of the board's oversight responsibility.

[1] *September 20, 2017 Jay Clayton speech (https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20).*

Action steps for implementing a cyber security governance plan

Just as no two organizations are alike, no "one-size-fits-all" cyber security action plan will work for all. Some companies have yet to take basic steps. Others have launched cursory efforts, and a few have undertaken robust plans. But virtually none still believe that an IT tool, or collection of tools, is sufficient. Fighting cybercrime requires an organization-wide effort, with plans and processes that are agreed upon and actionable.

Evolving board roles and responsibilities

In our experience, few IT security leaders have provided regular briefings on cyber security strategy to their organization's board members until comparatively recently, but such briefings are happening with greater frequency. Similarly, in an environment where cyber security must be part of business strategy, organizations increasingly understand the importance of a direct reporting relationship between their IT security leaders and the CEO.

Some main considerations for the roles of board members are:

- What roles do senior leaders and the board play in managing and overseeing cyber security and cyber incident response, and who has primary responsibility?
- Do we have a CISO, and who does the CISO report to? Is there a direct line to the CEO?
- Do we need a separate, enterprise-wide cyber risk committee for more regular communication?

Communication effectiveness

A recent survey of 87 directors and general counsels/corporate secretaries conducted by the National Association of Corporate Directors (NACD) noted that 22 percent were not satisfied with the quality of information on cyber security they receive from management. This number indicates that some progress is being made in this area, as it is a significant decrease over the 35.5 percent who stated in the 2017–2018 NACD survey that they were dissatisfied with the quality of the information management provides. The main drivers of respondents' dissatisfaction with cyber security information quality were insufficient transparency about performance issues (44 percent), does not allow for effective benchmarking (41 percent).

For boards, questions to consider on the effectiveness of communication include:

- Do we have a holistic, board-specific framework that "closes the loop" on effective communication throughout the organization?
- Are we asking the "right" questions and sharing the "right" information for a reliable information flow?
- What is the quality of our meetings, our direction, and communication from management?
- What kind of reports are we receiving? Are we transparent and informing our stakeholders?

Communication frequency

Our experience shows that many directors are not satisfied with the quantity of the information provided by management on cyber security and IT risk. Some main considerations for the frequency of communication are:

- Is the frequency of our meetings adequate, and on a recurring basis?
- Is the frequency of our direction adequate, and on a recurring basis?
- Is the frequency of communication from management adequate, and on a recurring basis? How frequently do we receive reports?
- What is our incident response plan, and how are we learning from incidents that are happening?

Closing the loop with these three key questions

From a governance standpoint, how can the board be more effective and close the loop in its information flow? The board must always be proactive, informed, and involved without getting overwhelmed or paralyzed. Based on our board outreach and education programs, we have found these are the three most common, high-level board oversight questions asked by the executive management and the board today:

1

What are the new cyber security threats and risks, and how do they affect our organization?

The first question addresses *strategic* issues from the business process and corporate objectives standpoint. It is about getting an up-to-date, detailed snapshot of the current cyber threat landscape that is understood by all. It looks at getting comfortable with cyber security aspects of core business decisions, cutting through the technical jargon.

2

Is our organization's cyber security program ready to meet the challenges of today's and tomorrow's cyber threat landscape?

The second question addresses *tactical* issues, from a program, (technical) capability, and process perspective, and how they are cascaded throughout the organization. It looks at whether the organization is doing enough due diligence to mitigate risks, depending on its risk profile.

3

What key risk indicators should I be reviewing at the executive management and board levels to perform effective risk management in this area?

The third question addresses the many *operational* issues, clarifying, prioritizing, and ultimately translating them to what it really means from a risk posture point of view and ultimately, closing the loop. This is "where the rubber meets the road, and indicates how you will know whether you are doing the right thing—so you can sleep at night more easily.

These three questions are interrelated and allow for continuous synchronization and integration as the board wants to remain agile and responsive to the evolving and changing cyber threat landscape.

KPMG's Global cyber maturity framework

Recognizing the critical role of boards in addressing cyber security as a holistic business challenge, KPMG designed its global cyber maturity framework to address the need for board engagement in this area and to help boards exercise their oversight responsibilities.

Other global standards focus on efforts on the business side. For example, the National Institute of Standards and Technology (NIST) Cybersecurity Framework helps organizations define and assess the control maturity of a cyber program's operational aspects. It is mutually compatible with KPMG's cyber maturity framework, which is specifically designed to provide strategic alignment for coordinating board and non-IT oversight and governance.

Use of this framework helps organizations and their boards:

- Reduce the risk of cyberattack and mitigate the consequences of a successful attack
- Enable better cyber security decision making with information on measures, patterns of attack, and incidents
- Establish lines of communication and roles and responsibilities for incident response
- Enhance the organization's reputation for cyber security preparedness
- Improve organizational knowledge and competencies regarding cyber security
- Benchmark the organization as a cyber security leader in relation to its peers.

In addition, we offer framework mapping that is compatible with your existing framework.

KPMG's global cyber maturity framework: six domains

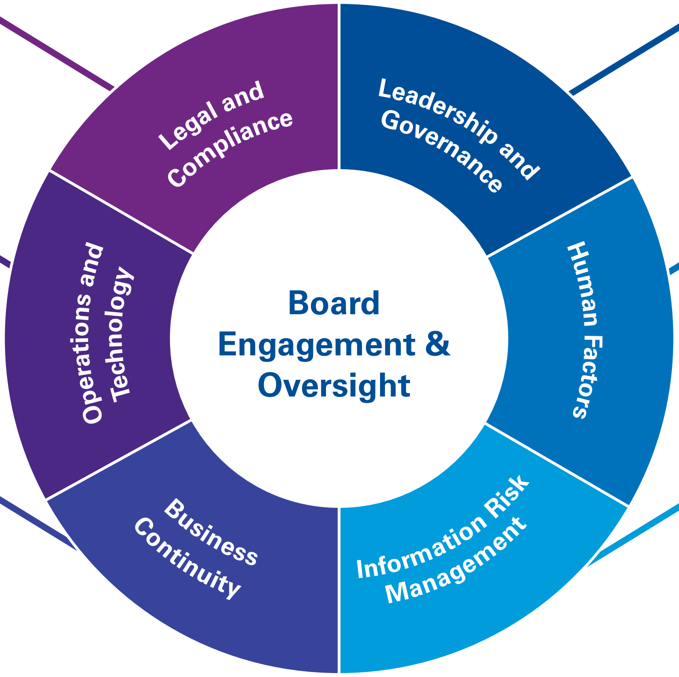
A broad holistic framework for exercising board oversight responsibility

Communication and direction flow through six domains

Within this cyber maturity framework, a strong communications plan is focused on the details and complexity of ongoing *communication and direction* between the board and management. This helps achieve a reliable flow of information among a broad mix of stakeholders. It is not only the frequency of communication that needs to be reassessed, but also, improving the appropriate and efficient quality of communication when addressing risks.

This framework keeps in mind that security is only as strong as your weakest link—and the weakest link most often is people, whether due to someone on the inside, human error, or another human factor.

The objective is to allow for all communication—whether technical, legal, strategic, or operational—to be mutually beneficial for all stakeholders. The right questions need to be asked, and the details matter and need to be meaningful for everyone involved. Our transformative framework, with a proactive approach, helps shape the proper dialogue and overall, improves the information flow to become more transparent and sustainable—thus, closing the loop.


Board Engagement & Oversight
Legal and Compliance
Leadership and Governance
Human Factors
Information Risk Management
Business Continuity
Operations and Technology

Legal and Compliance
Regulatory and international certification standards as relevant

Operations and Technology
The level of control measures implemented to address identified risks and reduce the impact of compromise

Business Continuity and Crisis Management
Preparations for a security event and ability to prevent or reduce the impact through successful crisis and stakeholder management

Leadership and Governance
Management demonstrating due diligence, ownership, and effective management of risk

Human Factors
The level and integration of a security culture that empowers and helps to ensure the right people, skills, culture, and knowledge

Information Risk Management
The approach to achieve thorough and effective risk management of information throughout the organization and its delivery and supply partners

I. Leadership and Governance

Management demonstrating due diligence, ownership, and effective management of risk

How should boards engage?

- Understand governance structure and have ongoing dialogue with executive leadership team
- Review output of capability assessment
- Review and approve strategy and funding requests
- Participate in general board education
- Request periodic updates of program

Communication
Direction

- Define program ownership and governance structure
- Identify sensitive data assets and critical infrastructure
- Inventory third-party supplier relationships
- Perform assessment of current capabilities
- Define a strategy and approach
- Educate the board and executive management

What should management do?

II. Human Factors

The level and integration of a security culture that empowers and helps to ensure the right people, skills, culture, and knowledge

How should boards engage?

- Set the tone for the culture
- Review patterns/trends of personnel issues
- Understand training and awareness protocols

Communication
Direction

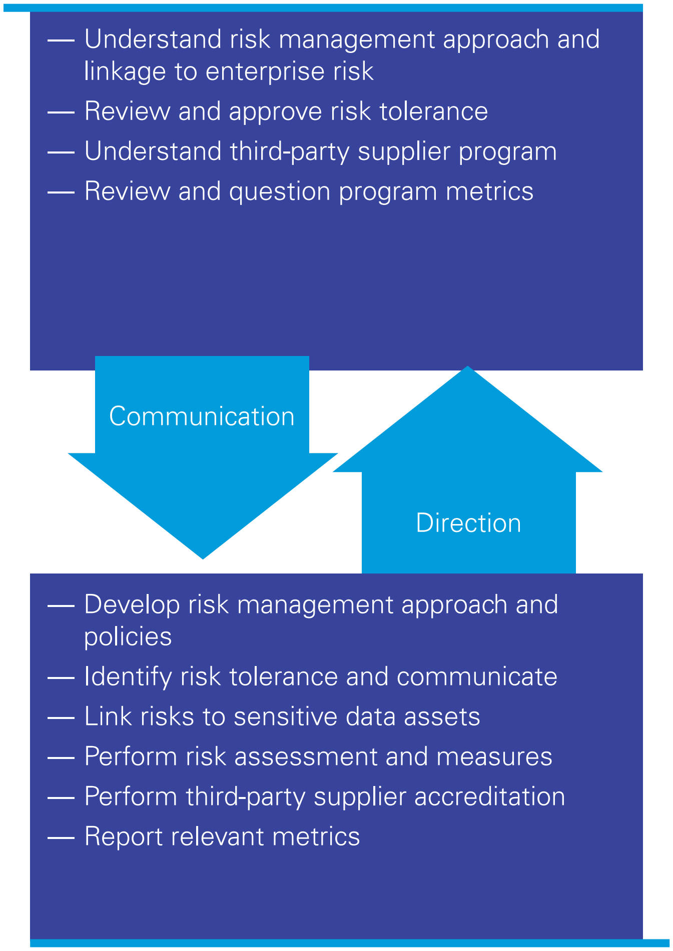
- Define culture and expectations
- Implement general training and awareness programs
- Implement personnel security measures
- Define talent management and career architecture
- Develop specific learning paths for key personnel

What should management do?

III. Information Risk Management

The approach to achieve thorough and effective risk management of information throughout the organization and its delivery and supply partners

How should boards engage?



- Understand risk management approach and linkage to enterprise risk
- Review and approve risk tolerance
- Understand third-party supplier program
- Review and question program metrics

Communication

Direction

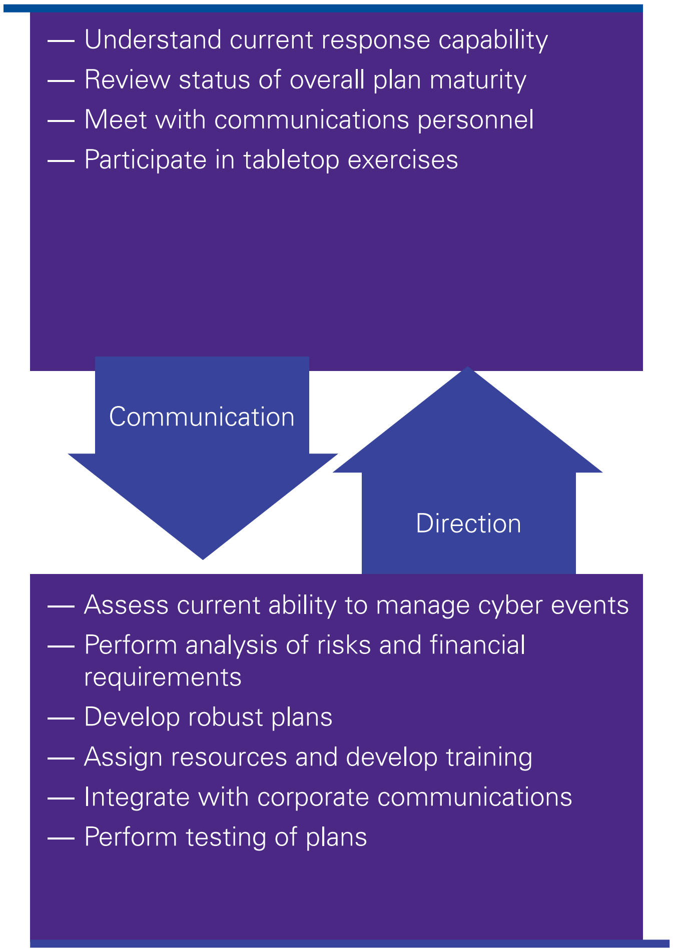
- Develop risk management approach and policies
- Identify risk tolerance and communicate
- Link risks to sensitive data assets
- Perform risk assessment and measures
- Perform third-party supplier accreditation
- Report relevant metrics

What should management do?

IV. Business Continuity and Crisis Management

Preparations for a security event and ability to prevent or reduce the impact through successful crisis and stakeholder management

How should boards engage?



- Understand current response capability
- Review status of overall plan maturity
- Meet with communications personnel
- Participate in tabletop exercises

Communication

Direction

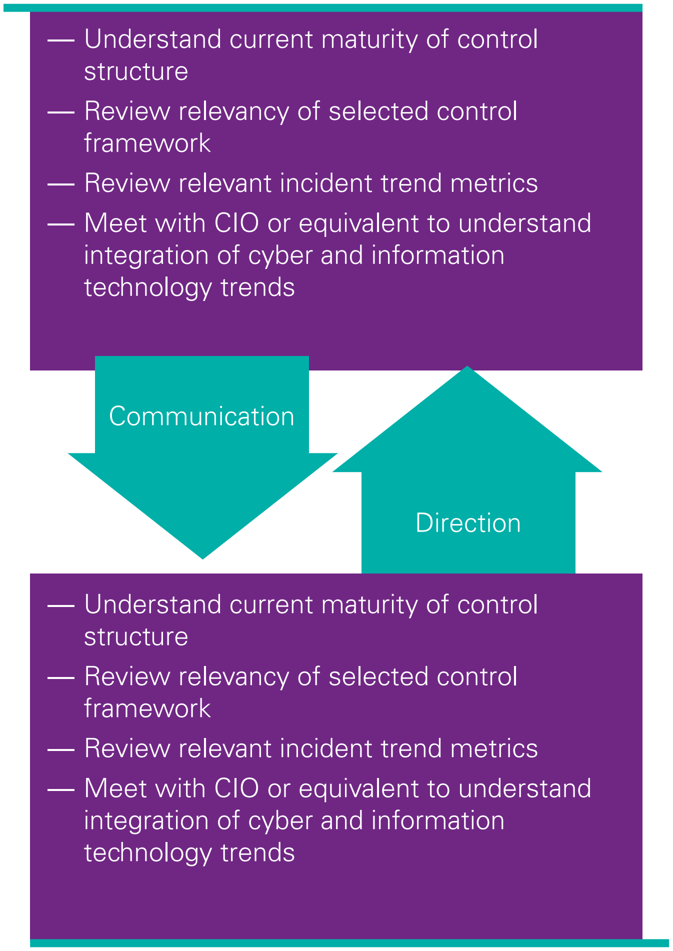
- Assess current ability to manage cyber events
- Perform analysis of risks and financial requirements
- Develop robust plans
- Assign resources and develop training
- Integrate with corporate communications
- Perform testing of plans

What should management do?

V. Operations and Technology

The level of control measures implemented to address identified risks and reduce the impact of compromise

How should boards engage?



- Understand current maturity of control structure
- Review relevancy of selected control framework
- Review relevant incident trend metrics
- Meet with CIO or equivalent to understand integration of cyber and information technology trends

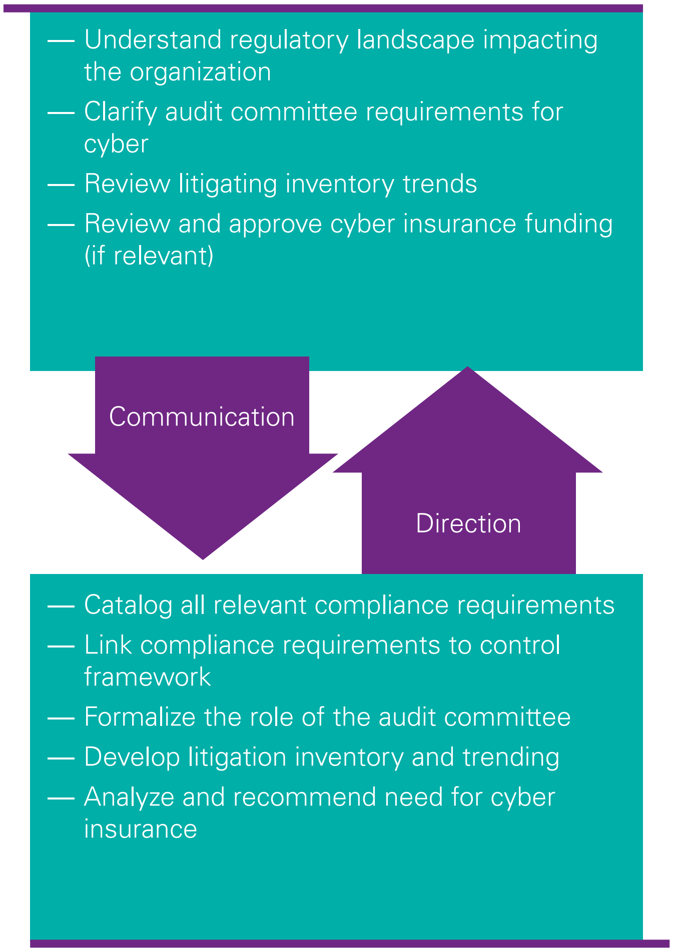
- Understand current maturity of control structure
- Review relevancy of selected control framework
- Review relevant incident trend metrics
- Meet with CIO or equivalent to understand integration of cyber and information technology trends

What should management do?

VI. Legal and Compliance

Regulatory and international certification standards as relevant

How should boards engage?



- Understand regulatory landscape impacting the organization
- Clarify audit committee requirements for cyber
- Review litigating inventory trends
- Review and approve cyber insurance funding (if relevant)

- Catalog all relevant compliance requirements
- Link compliance requirements to control framework
- Formalize the role of the audit committee
- Develop litigation inventory and trending
- Analyze and recommend need for cyber insurance

What should management do?

Continue to connect the dots with metrics

It is important to assess and benchmark the value of the framework by using key performance indicators (KPIs). Which KPIs are on your cyber risk dashboard? Is your organization achieving the cyber risk targets it has formulated? How do the KPIs for cyber risks relate to those of your peers?

Case study

A well-defined process for board oversight of cyber security

A large global manufacturer had a security breach of intellectual property in early 2014, only becoming aware of the issue when alerted by the FBI that it was monitoring transfers of large volumes of data to known hacker systems in a foreign country. After the initial triage activities took place, management had to communicate the issue to the board and explain the exposure, which was changing every day with new information that was uncovered from the investigation.

Prior to the incident, the board had only been briefed on cyber security on an annual basis, as part of a broader IT update from the CIO. Now the board became understandably very active in trying to understand the current state of cyber security risk at the company and how it could be better managed in the future.

The company hired KPMG Cyber Security Services to perform board education and a cyber maturity assessment of the organization's people, process, and technology controls to mitigate cyber threats and risks. After the initial report was complete, it was presented to the board with a full road map of prioritized remediation activities designed to close short-term gaps in the security program and execute longer-term strategies to navigate the evolving threat landscape.

After allocating funding to the initiatives on the road map, the board requested quarterly updates from management on the progress of the program in addition to an ongoing look at current operations. Management leveraged KPMG's assistance in developing dashboards of KPIs for board reporting; however, given the sensitivity around the breach and the heightened awareness of director responsibility, the board did not stop at reviewing management's materials.

KPMG was hired to perform a quarterly independent "health check" of the company's progress and validate some of the information presented in key metrics. In this role, KPMG continued to be a sounding board for the audit committee, sitting in all meetings, providing additional education on emerging trends, and validating management's assertions. Board oversight ultimately became a less complex and scary topic for directors, and the company now has a well-defined process to facilitate the communication and direction information flow between management and the board.

Conclusions

- Board oversight of cyber security is a required C-level activity.
- A cyber security governance plan needs to consider evolving board roles, as well as communication frequency and effectiveness.
- Close the loop in information flow by leveraging the three most often asked questions to address strategic, technical, and operational issues.
- KPMG's Global Cyber Maturity Framework addresses how to exercise board oversight responsibility in six enterprise-wide domains with a broader holistic approach.
- An organization's framework should efficiently and appropriately address ongoing communication and direction throughout the organization.
- Understand the enhanced value of benchmarking framework metrics and mapping the organization's framework against industry standards to stay proactive and to continue to close the loop.

Why KPMG?

KPMG brings a business context to cyber security for all levels of your organization—from the boardroom to the back office.

We know cyber security is a business issue, not just an IT issue.
Cyber security is a strategic enterprise risk that goes far beyond IT. Uncontrolled, it can impact product integrity, the customer experience, investor confidence, operations, regulatory compliance, brand reputation, and more. That is why cyber security demands attention not only from the CIO, but also from others in the C-suite, the board and, indeed, employees and business partners throughout the organization.

We translate cyber security into a language your business can understand.
Cyber security affects different parts of your business, and we translate cyber risks into an appropriate language for each of those parts. Whether we are working in your boardroom, back office, or data center, we seek to provide a jargon-free explanation of your cyber threats, the potential impact to your critical assets, and the recommended response.

We provide a business-led approach, supported by deep technical skills.
We bring a combination of technical domain experience and extensive cross-functional business skills including people and change, financial management, risk management, global compliance, and organizational design. KPMG professionals understand how cyber security risks affect the various layers of your business not just the technology layer so we can advise you in a context that is relevant to you.

We work collaboratively with you to meet your cyber security needs.
Instead of coming to you with a preconfigured approach, KPMG professionals take the time to understand your business priorities, strategic direction, and operations—so we can bring an appropriate context to your cyber security risks and help protect your critical business processes.

We know your industry.
As you are navigating cyber security, it is important to have an adviser at your side who understand the challenges, threats, and strategies in your industry. At KPMG, we bring both the business context and the industry context to cyber security. Leveraging the industry experience of KPMG professionals around the world, we understand where your industry is coming from in cyber security—and where it is going.

Contact us

Greg Bell
Principal, Global Cyber Security Services Co-Leader
T: 404-222-7197
E: rgregbell@kpmg.com

Tony Buffomante
Principal, Cyber Security Services U.S. Leader
T: 312-665-1748
E: abuffomante@kpmg.com

KPMG Cyber Security Emergency Hotline 855-444-0087

www.kpmg.com/us/cyber

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.