KPMG

Connecting the dots

A proactive approach to cybersecurity oversight in the boardroom

KPMG Cyber

kpmg.com

About the authors

Greg Bell

Greg Bell is a principal and serves as the KPMG Cyber US Leader. He is experienced with various areas of information management and information security with particular specialization in the fields of IT risk management and business enablement. In addition, Greg spends much of his time educating and working with directors and executives to better understand the impact of the changing cyber risks to their businesses.

Tony Buffomante

Tony Buffomante is a principal and KPMG Cyber – Strategy & Governance Lead. Over the past 20 years, he has managed and executed information technology security strategies, assessments, and implementations for some of the largest global organizations. Tony is a recognized industry leader in information protection, speaking at industry conferences, and instructing training seminars.

KPMG

Connecting the dots

A proactive approach to cybersecurity oversight in the boardroom

Cyber attacks and data leakage are daily threats to organizations globally, reminding us that we are all potential targets of this type of threat. Attorneys are discussing the potential risk of individual liability for corporate directors who do not take appropriate responsibility for oversight of cybersecurity[1]. Investors and regulators are increasingly challenging boards to step up their oversight of cybersecurity and calling for greater transparency around major breaches and the impact they have on the business.

Given this environment, it is not surprising that cyber risk is now near the top of board and audit committee agendas. According to the KPMG 2014 Global Audit Committee Survey, nearly 45 percent of audit committees in the United States have primary oversight responsibility for cybersecurity risk; yet, only 25 percent say that the quality of the information they receive about cybersecurity is good. So a critical question for every audit committee is: What information do they require—or is most critical—in assessing whether management is appropriately addressing cyber risk? Certainly, directors need to hear from a Chief Information Security Officer (CISO) or CIO who is knowledgeable and can help them see the big picture. But what should be the 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? Are we making the right decisions?

[1] "The Morning Risk Report: Cybersecurity Responsibility Falling to Boards," Risk & Compliance Journal, The Wall Street Journal, March 4, 2015, http://blogs.wsj.com/riskandcompliance/2015/03/04/the-morning-risk-report-cybersecurity-responsibility-falling-to-boards/.

Cybersecurity: a business and boardroom priority

By now, corporate boards have woken up to the call that they must address cybersecurity issues on their front lines, as it is not just an Information Technology (IT) issue. In fact, cyber risks are an enterprise-wide risk management issue.

SEC Commissioner Luis Aguilar's 2014 speech,[2] during which he urged boards to sharpen their focus on cyber risks, rings even more true today and serves as a warning for the future:

> *"…boards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."*

Aguilar addressed what boards can and should be doing to oversee cyber risk, pointing to a potential knowledge gap:

> *"Given the known risks posed by cyber-attacks, one would expect that corporate boards and senior management universally would be proactively taking steps to confront these cyber-risks. Yet, evidence suggests that there may be a gap that exists between the magnitude of the exposure presented by cyber-risks and the steps, or lack thereof, that many corporate boards have taken to address these risks. Some have noted that boards are not spending enough time or devoting sufficient corporate resources to addressing cybersecurity issues."*

We believe the process for closing that gap should not be a mystery. Taking a proactive approach to improving cybersecurity 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 cybersecurity breach.

What is at stake?

Since many global organizations have been victims of cyber crime over recent years, board oversight of cybersecurity 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.

Potential impacts and possible implications for the board include:

- **Intellectual property losses** including patented information and trademarked material, client lists, and commercially sensitive data
- **Legal expenses** including damages for data privacy breaches/compensation for delays, regulatory fines and the cost associated with defense
- **Property losses** of stock or information leading to delays or failure to deliver
- **Reputational loss** which may lead to a decline in market value, and loss of goodwill and confidence by customers and suppliers
- **Time lost** and distraction to the business due to investigating how the breach occurred and what information (if any) was lost, keeping shareholders advised and explaining what occurred to regulatory authorities
- **Administrative cost** to correct the impact such as restoring client confidence, communications to authorities, replacing property, and restoring the organization's business to its previous levels.

[2] U.S. Securities and Exchange Commission, speech transcript, "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," by SEC Commissioner Luis A. Aguilar, "Cyber Risks and the Boardroom" Conference, New York Stock Exchange, New York, NY, June 10, 2014, http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

Action steps for implementing a cybersecurity governance plan

No two corporations are the same, therefore there is no "one-size-fits-all" cybersecurity action plan. Some firms still have to take first basic steps. Others have launched cursory efforts to combat cyber crime. And a few firms have implemented robust battle plans, but there is going to always be room for improvement.

No matter where your organization falls in the spectrum, one thing is for certain—it takes much more than just an IT tool to batten down the security hatches. Fighting cyber crime requires a company-wide effort, with plans and processes that need to be implemented. There are some key governance related elements to visit and continuously revisit for consideration as this environment evolves.

Evolving board roles and responsibilities

In a recent cybersecurity survey,[3] just 22 percent of about 1,000 senior-level IT and IT security leaders say their organization's security leader briefs the board of directors on cybersecurity strategy. Sixty-six percent of the panel forecast that three years from now the organization's security leader will regularly brief the board on a recurring basis. Also, only 14 percent of respondents say their organization's security leader has a direct reporting relationship with the CEO. In contrast, 30 percent of the panel predict that the security leader will directly report to the organization's CEO three years from now.[4]

Some main considerations for the roles of board members are:

- What roles do senior leaders and the board play in managing and overseeing cybersecurity 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?

[3] "2015 Global Megatrends in Cybersecurity," p. 3, sponsored by Raytheon, Ponemon institute, February 2015, http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf.

[4] Ibid., p. 4.

KPMG

Communication frequency

A recent survey of more than 1,000 directors at public companies conducted by the National Association of Corporate Directors (NACD)[5] showed more than half (52.1 percent) of directors say they are not satisfied with the quantity of the information provided by management on cybersecurity 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?

Communication effectiveness

The NACD survey also noted that 35.5 percent were not satisfied with the quality of information on cybersecurity and IT risk topics, which was an increase over the previous year.[6]

Some main considerations for the effectiveness of communication are:

- 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?

---

5 "Board members unhappy with information on IT, cyber security," National Association of Corporate Directors (NACD), December 3, 2014, http://www.nacdonline.org/AboutUs/NACDInTheNews.cfm?ItemNumber=12551.

6 Ibid.

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 cybersecurity 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 cybersecurity aspects of core business decisions, cutting through the technical jargon.

2

Is our organization's cybersecurity 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

KPMG's Global Cyber Maturity Framework

Cybersecurity is more than a technology problem—it is a holistic one. In response, KPMG designed a global Cyber Maturity Framework specifically to assist organizations in addressing these critical questions by combining the most relevant aspects of existing international cybersecurity standards and governance frameworks.

While we recognize the "alphabet soup" of existing framework options available (which are primarily IT or controls driven) are valuable, we believe KPMG's Cyber Maturity Framework is a broader, more thorough, and more holistic way to address board engagement and how boards can exercise their oversight responsibilities.

For example, while the National Institute of Standards and Technology (NIST) Cybersecurity Framework is beneficial for defining and assessing the control maturity of the operational aspects of a cyber program within the current environment, KPMG's Cyber Maturity Framework is specifically designed to provide strategic alignment for coordinating board and non-IT oversight and governance. Together, both frameworks provide mutual compatibility.

We regularly provide multidisciplinary assessments for boards that are focused on their business globally against these six domains: 1. Leadership and Governance, 2. Human Factors, 3. Information Risk Management, 4. Business Continuity and Crisis Management, 5. Operations and Technology, and 6. Legal and Compliance.

The application of a holistic model incorporating these six domains can bring the following benefits:[7]

- The reduction of the risk that the organization will be hit by a cyber attack from outside and the reduction of any consequences of a successful attack.
- Better decisions in the field of cybersecurity—the provision of information on measures, patterns of attack, and incidents is thus enhanced.
- Clear lines of communication on the theme of cybersecurity. Everyone knows his or her responsibilities and what must be done if incidents (or suspected incidents) occur.
- A contribution to a better reputation. An organization that is well prepared and has seriously considered the theme of cybersecurity is able to communicate on this theme in a way that inspires confidence.
- The enhancement of knowledge and competences regarding cybersecurity.
- The benchmarking of the organization in the field of cybersecurity in relation to its peers.

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

[7] *Cybersecurity, a theme for the boardroom,* p. 17, KPMG Advisory N.V. (the Netherlands), 2014, authored by KPMG partner John Hermans, http://www.kpmg.com/NL/nl/IssuesAndInsights/ArticlesPublications/Pages/Cybersecurity-a-theme-for-the-boardroom.aspx.

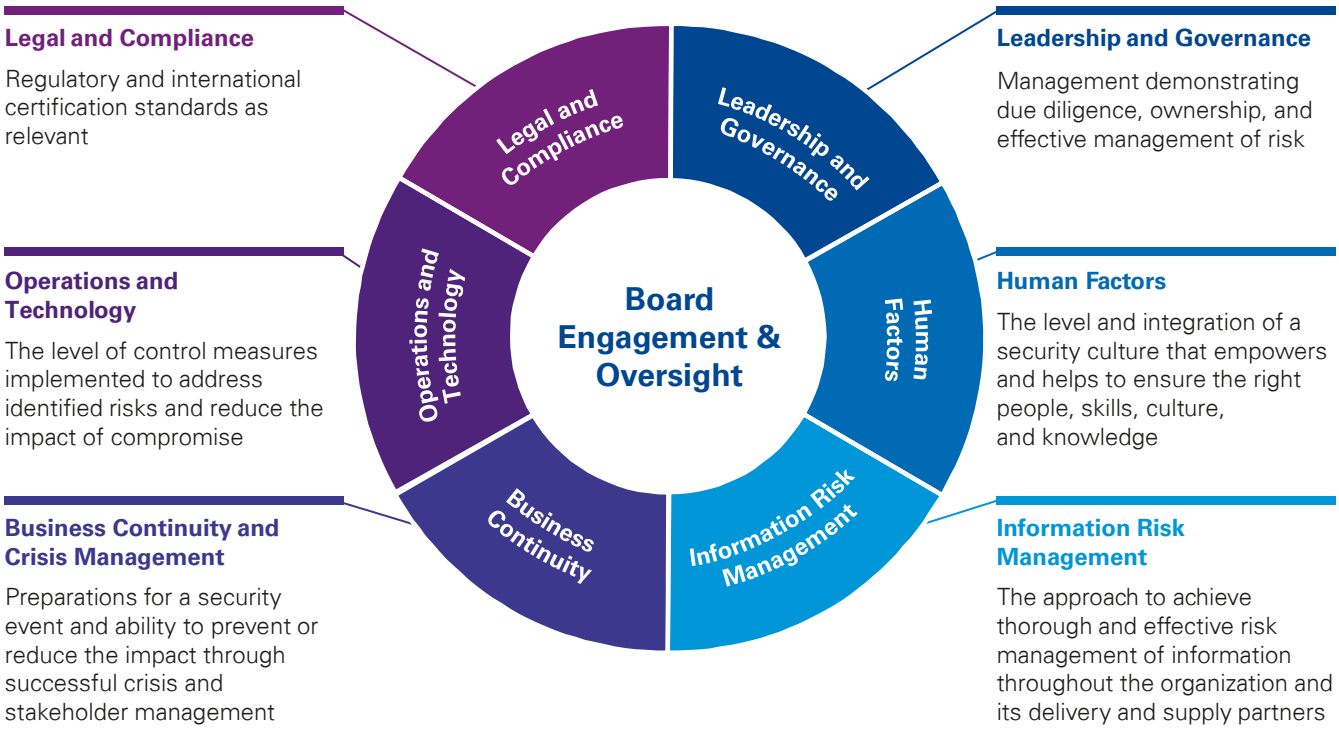
KPMG's Global Cyber Maturity Framework: Six Domains

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.



I. Leadership and Governance

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

II. Human Factors

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

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 table-top 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?

KPMG

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

Communication

Direction

- 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)

Communication

Direction

- 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 cybersecurity

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 cybersecurity 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 cybersecurity risk at the company and how it can be better managed in the future.

The company hired KPMG Cyber 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 Cyber 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 Cyber 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 cybersecurity is a required C-level activity.
- A cybersecurity 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.

KPMG

About KPMG Cyber

KPMG Cyber assists global organizations in transforming their security, privacy, and continuity controls into business-enabling platforms while maintaining the confidentiality, integrity, and availability of critical business functions. The KPMG Cyber approach strategically aligns with our clients' business priorities and compliance needs.

Contact us

Greg Bell
Principal, KPMG Cyber – US Leader
T: 404-222-7197
E: rgregbell@kpmg.com

Tony Buffomante
Principal, KPMG Cyber – Strategy & Governance Lead
T: 312-665-1748
E: abuffomante@kpmg.com

KPMG's Cyber Emergency Hotline
855-444-0087

kpmg.com/us/cyber

kpmg.com/socialmedia