THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

# A STRATEGIC CYBER-ROADMAP FOR THE BOARD

## From Sit-Back to Lean-In Governance

By Andrea Bonime-Blanc

## INTRODUCTION

This *Directors Notes* reviews five director case studies of cyber-risk governance, compiled by The Conference Board Governance Center through interviews with board members who hold seats at a variety of public and non-public companies, including technology companies, Fortune 100 financial services companies, top 10 federally chartered credit union and professional associations. The case studies show examples of how boards are addressing their cyber oversight responsibilities including the formation of a board committee dedicated to technology, the importance of management reporting on cyber-risk, finding a director with cybersecurity governance skills and the importance of a third-party assessment of a company's cyber-strategy. Because there is significant risk exposure today for a cyber-breach, boards need to be fully informed and ready to address their cyber activities including understanding the company's crown jewels, their preparedness for an attack, company risk framework, current regulatory environment, etc.

DN-V7N8 | NOVEMBER 2016 | Subscribe for free at www.conferenceboard.org/directornotes
© 2016 The Conference Board, Inc. All rights reserved.

Recent surveys completed by PwC's Governance Insights Center and Spencer Stuart/ Corporate Board Member show that public company directors view cybersecurity as a serious threat that needs more attention. PwC's 2016 Annual Corporate Directors Survey reported that 81 percent are at least moderately engaged with overseeing the risk of cyber-attacks. However, about one in five directors say their management teams don't sufficiently, or at all, provide the board with adequate security metrics.

In Spencer Stuart's 2016 *What Directors Think* survey that appeared in *Corporate Board Member*, 35 percent of the directors surveyed agree that cyber risk is among the biggest corporate challenges. More than a third of those responding (38 percent) believe that although they are doing all they can to protect the company's data, most cybersecurity risk is really out of their hands. Eighty-three percent say it is at least somewhat important to consider IT/cyber expertise when selecting new board members.

In 2015, The Conference Board's report *Emerging Practices in Cyber-Risk Governance* (the "2015 Report").[1] zeroed in on what makes for an overall cyber-ready and resilient entity. The analysis translated into 10 key takeaways that global organizations (whether for profit, non-profit, academic or even governmental) should consider in developing their cyber-risk management and governance (see Appendix A). By profiling a new series of concrete cyber-governance cases, this *Director Notes* continues to discern today's most effective posture and practices on cyber-risk governance specifically at the board level and from the board's perspective.

The case studies are based on interviews conducted with five corporate board directors whose backgrounds and companies range from global technology and telecom to financial and the defense sectors, and from Fortune 100 to start-ups.[2]

The following are the principal lessons learned from this research and from the best practices shared by the five directors we interviewed:

1. All directors opined that the board must tackle the topic of cyber-security in a manner that is appropriate to its industry, footprint, geography, assets, and people.
2. Most directors said that the board should have either a committee, cyber expert, or both, tackling the issue of cybersecurity oversight as part of overall IT oversight. Such a technology or other committee should report to the board twice a year.
3. Most directors did not favor that the audit committee assume responsibility for cybersecurity oversight and some favored a technology (and cybersecurity) committee approach.
4. Several directors favored the inclusion of a cybersecurity savvy or knowledgeable director on the board.

---

1 Andrea Bonime-Blanc. *Emerging Practices in Cyber-Risk Governance*. The Conference Board 2015.

2 Of the five directors who agreed to share their experience and practices with us, three are on the record and two are off the record. In the latter two cases, we describe generically their role on their boards and the industry sectors of the companies whose boards they serve on.

5 Most directors felt that at least some board members engage in cybersecurity preparedness education and training.

Appendix B contains a summary of the key questions we posed to these five directors as part of our conversation with them.

## On the formation of a board committee dedicated to technology, including cyber-risk

**Dr. Anastassia Lauterbach,** Board Member, Technology Committee Chair, Dun & Bradstreet

According to Lauterbach, a European-based technology entrepreneur, director on various advisory boards and board member and chair of the Technology Committee of the Board of Directors of Dun & Bradstreet, the reliance on digital systems is why concern over cybersecurity is rising so rapidly with boards. In the face of an increasing onslaught of attacks and levels of sophistication, defenders are still relying on decades-old core security technologies. Most security professionals and practitioners would agree that total prevention is not possible. However, it is without doubt that a structured top down approach that embeds cybersecurity management throughout a company's infrastructure is highly desirable. The best approach is to establish a dedicated technology committee on the board. In addition to covering digital and technology issues generally, the mandate of such a committee will include the responsibility to review cybersecurity and ensure that discussion of this risk and opportunity reaches the overall board twice a year, following the same agenda and using benchmarking and key performance indicators (KPIs).

A board-level cybersecurity review blueprint should include subjects such as:

- reducing security risks from malicious and negligent employees,
- managing cybersecurity risks which might come from suppliers' and partners' products and applications,
- managing risks associated with third-party outsourcing,
- producing overviews on open source products and applications to increase transparency on cyber-risks,
- creating breach prevention processes and practices,
- analyzing risks due to introduction of IoT (Internet-of-things) products, forensic remediation practices, (simulations) of cyber incident response,
- creating guidelines on communication to shareholders, regulatory authorities and employees in case of an incident,
- taking out cybersecurity insurance, and
- implementing cybersecurity education for employees and executives/ board members.

Besides, boards should discuss cybersecurity in case of M&A and post-merger integration.

In Lauterbach's opinion, each board should have members with a profound understanding of technology, legacy IT and new technologies relevant to the business (e.g., artificial intelligence, IoT, cloud).

Such board members do not necessarily need to be current or existing chief security officers (CSO), chief information security officers (CISO) or chief technology officers (CTO) but someone with good judgment and good connections into the information technology (IT) ecosystem. That includes experience working within traditional and established technology companies (such as Amazon, Microsoft or Intel) and new technology companies such as start-ups or venture capitalists funding high-tech.

In terms of expectations from the board of management on cyber-risk management, the requirement is that the full board receives a full cybersecurity update twice a year and that the technology committee receives full updates quarterly including metrics and a dashboard from the CISO and his or her team. Additionally, if there is a serious incident, the technology committee chair would expect a direct report at any time it happens.

If a dedicated technology committee is not possible, cybersecurity should be integrated into the Audit or Risk committee agendas. A good practice might be to train all board members in cybersecurity (governance) basics, and brush up the training every 36 months to stay on top of technology trends and regulatory updates.

### Cyber-incident example

**FACTS**. Ransomware has been hitting a number of organizations hard, holding data hostage by encrypting it with an unknown key and demanding that the organization pay in order to have the data restored. If the organization has insufficient backups or the backup is also encrypted, the only way to restore the data may be to pay the ransom. In some cases, the decision to pay a ransom may need to be a board-level decision or at the very least discussed (ideally in advance of the attack).

**LESSON LEARNED**. According to the NACD Cyber-Risk Oversight Guidebook, the top control to reduce the risk of attack (including ransomware) is restricting user installation of applications (called "whitelisting" or "Trusted App Listing.") This excellent control is rarely implemented. Boards should ask organizations for their plans to implement this specific control.

## On the importance of management reporting on cyber-risk

**Robert A. Clyde,** Board Member, ISACA (Information Systems Audit and Control Association), White Cloud Security and Xbridge Systems, Advisory Board Member, HyTrust and BullGuard

Clyde is a technology expert by profession. He serves on various technology company boards and on the board of ISACA, a global IT and cybersecurity professional association with more than 140,000 members and certification-holders. Clyde believes that the single most important thing a board can do regarding cyber-risk oversight is to ask management for an accurate and externally validated report on the state of the organization with respect to cyber risk. The report should include a clear statement of the risks, gaps, and plans to address them.

In terms of how the board should be organized to meet the cyber challenge, Clyde believes that the board should include some members who are familiar with cyber issues and cyber security from a governance perspective, which does not necessarily mean that they must have deep technical or cyber technology skills.

As to where responsibility for cyber oversight should reside, Clyde advises that boards should carefully consider which committee will provide cyber oversight, and have that committee provide reports at each regular full board meeting. Additionally, boards should ensure that employees know how to report insider attacks, including those involving their managers.

The overall responsibility for cyber-risk governance rests with the entire board. Many boards have their audit committees provide oversight. However, this may overburden the audit committee and cause boards to appoint people to that committee who may be well-suited to cyber issues but less well-suited to traditional audit committee member responsibilities. The technology committee should not only consider risk, but also ensure that an organization is leveraging technology and cyber issues to their advantage and not falling behind competitively.

In Clyde's opinion, boards should include one or more technology-savvy board members with cyber expertise. In this day and age, there are many executives and potential board members with such knowledge. If the board cannot find someone like this to be a board member, then it should consider bringing in an outside cyber expert to assist the board. The CISO and Chief Risk Officer (CRO) should also be present for most cyber-related discussions.

In terms of best practice frameworks, Clyde recommends using the COBIT (Control Objectives for Information and Related Technologies) framework from ISACA, one of the leading governance and management frameworks for enterprise IT. COBIT is used by organizations across the globe as a governance framework for managing cyber risk. COBIT maps to the National Institute of Standards and Technology (NIST) cyber security framework recommended by the US government. COBIT 5 is the most recent version of the framework, which is now in its 20th year.

In terms of expectations from management, the CEO and CISO (CIO where there is no CISO) should communicate to the board and the relevant committee about cybersecurity. However, the CEO and management should promptly notify and brief the board on any material cyber-attack, new risk or new threat that may affect shareholders.

Cyber-risk governance will be an integral part of overall governance well into the future. Board members will become more conversant and knowledgeable about the subject. A best practice is to make sure that at least some board members engage in cyber-incident preparedness exercises, which not only will help prepare them for the incidents but also strengthen understanding of the process within the organization.

Another key ingredient in good cyber-risk governance that boards should be on top of is cyber insurance. Boards should review their coverage, or if their organization doesn't have cyber insurance, consider whether they should have such coverage.

## The State of Cyber-Risk Insurance[a]

The state of cyber-insurance continues to be in flux and is a moving target. There are many providers of this type of insurance but few standards that have been fully settled on so far. A lot of this has to do with the fact that organizations including companies have not quite figured out how to organize themselves around the issue of cyber-risk management.

That said, the National Association for Insurance Commissioners provides some useful guidance on where we are on this topic today and the key issues that might be covered by cyber liability policies (though this again depends on each particular carrier).

"Most businesses are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. However, most standard commercial lines policies do not cover many of the cyber risks mentioned below. To cover these unique cyber-risks through insurance requires the purchase of a special cyber liability policy.

However, cyber-risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Insurers compensate by relying on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber-risk are more customized and more costly than other risk insurance policies.

The type of business operation will dictate the type and cost of cyber liability coverage. The size and scope of the business will play a role in coverage needs and pricing, as will the number of customers, the presence on the Web, the type of data collected and stored, and other factors."

### KEY CYBER-INSURANCE POLICY ISSUES AS IDENTIFIED BY THE NAIC:

**Liability for security or privacy breaches**. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.

**The costs associated with a privacy breach**, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.

**The costs associated with restoring**, updating or replacing business assets stored electronically.

**Business interruption** and extra expense related to a security or privacy breach.

**Liability associated with libel, slander**, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.

**Expenses related to cyber-extortion** or cyber-terrorism.

**Coverage for expenses related to regulatory compliance** for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

---

[a] Most of the information in this Table was gleaned from the National Association of Insurance Commissioners, http://www.naic.org/cipr_topics/topic_cyber_risk.htm

## Finding a director with cybersecurity governance skills

**Bob Zukis,** Advisory Board, Firemon, Technology Consultant

To Bob Zukis, a technology executive, former Big 4 accounting firm advisory partner and current member of various technology company advisory boards, and a senior fellow at The Conference Board's Governance Center the single most important factor boards should consider is adding a director with cybersecurity governance skills to the board.

Zukis believes since cyber-risk governance is a component of overall enterprise risk management, it is not necessary for a separate committee of the board to be created as long as some directors have the cyber-governance skillset. However, Zukis is generally opposed to the overall topic of cybersecurity governance residing within the audit committee because (a) the cyber-risk governance is much broader than the audit committee's financial reporting focus and (b) the skillset needed is very different.

In terms of whether a board has a director with cyber-risk expertise or access to an external advisor or consultant, Zukis believes that the cybersecurity skills need to be a resident component of a high performing board. He posits that since cyber-risk is a systemic issue that covers people, process and technology that the skills need to be internalized to the board. Ultimately, cyber-risk is about business risk and continuity and a board without these skills is not fulfilling its duty of care around this pervasive issue.

As to the frameworks that Zukis recommends, there are quite a few that are readily available for adoption (e.g., COBIT, COSO, ISO ITIL, NIST, King III[3]), but they are simply under-applied and under-utilized in the corporate boardroom. Boards should have members with the right skills to ask and require management to explain what they aren't doing in this area as a regular part of the board agenda.

Zukis also considers developments in cyber insurance to be helpful in the fight against cyber breaches as insurers are examining the board's approach to cyber-risk governance as part of the underwriting process and considering this in how they set their premiums. Some legislators are also beginning to propose rules that may force boards to address the boardroom cybersecurity skills gap issue similarly to how the Sarbanes-Oxley legislation required boards to address the financial reporting skills gap on the board.

As a board member, Zukis expects management to understand that cyber-risk is an everyday issue and that governing it is a core responsibility that every board needs to meet.

3 See COBIT definition on Page 5 of this report. COSO is the Committee of Sponsoring Organizations of the Treadway Commission. It has published several risk management frameworks, including one on internal control—integrated reporting in 2013. ISO is international organization for standardization. ITIL is the Information Technology Infrastructure Library, which is a list of IT services guidelines. NIST is defined on Page 5 of this report. King III is the King Code of Governance Principles in South Africa. Its latest version focuses on IT governance.

Zukis is an advocate for boards to have a cybersecurity savvy director with the necessary skills who can govern the application of a comprehensive IT and cybersecurity governance framework. This is a simple step that will help every board fulfill its duty of care, and ultimately help companies adequately address cybersecurity risk.[4]

### Cyber-incident example

**FACTS**. Due to the adoption of technologies like cloud and virtualization, many IT administrators have tremendous power. If an IT administrator makes a mistake, goes rogue or has his or her account hacked, an organization may be surprised at the amount of damage that could be done without any additional collusion. For example, in the case of a large U.S. bank, one of the bank's administrators accidentally deleted thousands of virtual machines, which took down many key departments, like credit card services, for more than a day.

**LESSON LEARNED**. Boards should insist that management have a list of who the administrators are that could create such damage without collusion, and then ask management for a plan on how to add secondary approvals and other controls so that no single individual has that much power.

4 Bob Zukis recently wrote the chapter "Information Technology and Cyber-security Governance in a Digital World" in *The Handbook of Board Governance*, Wiley 2016, edited by Richard LeBlanc.

## The importance of a third-party assessment of a company's cyber-strategy

**Fortune 50** Financial Services Industry Board Member

This director of two financial services sector companies (one of which is a Fortune 50 company) and former Executive of a Fortune 100 Aerospace company, believes that the single most important thing a board should do is to request an independent third party assessment of the company's cyber strategy, approach and plan. The board (or an appropriate board committee) should be briefed on the results of the assessment. From these results, cyber heat maps should be created using the assessment as a factual baseline. This is an excellent way for the board to become educated about cybersecurity and prioritize the company's risks. The assessment, if done properly, can provide a foundational roadmap for future improvements.

In terms of how the board should be organized to deal with cyber-risk governance, this director suggests that the board request the CIO or CISO to brief the board on their strategy and approach to cyber. This should include a discussion of "crown jewels" or the data, systems or technology most sensitive to the company. With this backdrop, the board can decide how to organize itself—full board, working group of a committee, specific committee, etc. This director believes that much of this depends on the depth of cyber experience both on the board and within the company.

This director believes that one of the board committees—either audit or risk—should be charged with the responsibility for cyber oversight. This committee must have the time for "deep dives" into this topic and appropriate board expertise allowing the right questions to be asked. The full board should be provided with periodic updates (generally quarterly) from the committee and from the company relative to any changes in threat environment, business continuity plans, dry-run results and other similar topics.

Having the time for the appropriate "deep dives" is critical as the cyber threat is dynamic. Best practices consider both the current environment and any changes to technology or other items. Company best practices also call for CISO engagement with law enforcement, industry peer groups, and government where threat information and possible mitigating techniques can be discussed.

Cyber is a complex topic; so having board expertise is particularly useful. This should be augmented by internal/external expertise, as required. This expertise may be in terms of third-party reviews or may be to provide updates on the threat environment or other similar topics.

The board, too, benefits from hearing any key themes or shifts in the cyber threat. A recent U.S. law, the Cybersecurity Information Sharing Act, allows the government to provide threat information to industry groups and industry, in turn, provide information to the government. This is particularly important as the information might provide an early warning of the types of threats being seen by others, allowing proactive actions to be taken.

In terms of leading frameworks, this director believes that it is helpful if the company adopts a security framework, such as the one published by NIST for Improving Critical Infrastructure Cybersecurity, which is a collection of best practices, maturity frameworks in use by many third party assessors or other frameworks. Risk analysis, priorities and impacts can then be measured against this framework to understand the company's overall security posture. The Cybersecurity Information Sharing Act mandates that NIST periodically update best practices to keep them current against the evolving threat.

### One director's key recommendations

- Independent assessments can help the board evaluate the cyber plan and risks
- Board organization is a function of depth of experience in cyber-risk
- Boards should have a board committee with cyber-risk oversight
- Both internal and external expertise play key roles in addressing cyber threats
- The NIST cyber and other frameworks play a key role in analyzing and managing cyber risks
- The board should be kept informed of any significant cyber threats or breaches
- Cyber-risk management is everyone's responsibility
- Boards should be curious and ask questions
- Company best practices also call for CISO engagement with law enforcement, industry peer groups and government

## Keeping open communications about cyber-risk governance

**Chairman of the Board** of Top 10 US Federally Chartered Credit Union

According to this director, the single most important aspect of good cyber-risk governance is to have open, honest and transparent communication channels with management, including regular and candid discussions with top-level IT management. This director stresses that it must be acceptable to bring up and discuss vulnerabilities and less-than-perfect outcomes.

In terms of how the board should be organized for cyber-risk governance, this director believes that it depends on the board and the industry. In the case of the financial industry company where this director is chair, cyber-risk issues are handled at the full board level since that risk is a key element of both their product and their reputation.

A committee may be appropriate in some circumstances. The credit union for which this director is board chair chose not to place cyber-risk governance under a specific committee because the board believes it is so intertwined with other key strategic initiatives. The company keeps these conversations at the full board level. However, in this company's case, they also have an enterprise risk committee and an audit committee that occasionally do deep dives around audit follow-up, whether from internal or external auditors, compliance personnel, or regulators.

This chair believes that each board should bring in expertise as necessary. Cyber-risk is a broad topic, and specific expertise can become dated quickly.

The board should understand to what extent management is bringing in third-party experts to vet the security environment and make sure that the internal team's thinking is up to date. This board does not require that a particular framework be used to understand cyber-risk oversight. However, management is using frameworks expected by the company's financial regulators.

In terms of what this board expects of management, it is to issue regular dashboard reporting and candid dialogue at each board meeting. The dashboard should include some of the following elements: the architecture for cyber risk governance, a threat matrix complete with a heat map, a status report on technology and liability defenses, incident reports, and the cyber attack "crown jewels." (See Figure 1)

By regulation, the board meets monthly and is updated frequently. It is the board's practice that the executive leadership team (which includes the CISO who is also chief digital officer) attends the meeting in addition to the CEO. The board receives monthly status reports from each executive team member.

While this chair of the board does not believe that the company is practicing cutting edge cyber-risk governance, the chair believes strongly that the company is and should continue to practice "business as usual" cyber-hygiene (meaning applying systematic and fundamental cybersecurity technical and behavioral risk management), which is an issue for all boards. It is not different from audit, compensation, succession planning, corporate social responsibility, strategy, etc. It is part of the "new normal" of what boards need to pay attention.

Figure 1 **What's on your board's cyber risk governance dashboard?**

| Architecture of cyber risk governance | Budget & resources |
|---|---|
| How is the company positioned, organized, and deployed for cyber risk management<br>Is this the optimal approach? | What is being spent?<br>What is needed for proper cyber risk management? |
| **Threat matrix–substantive cyber-risk issues** | **Toolkit & proactive measures** |
| Top issues<br>Industry trends and benchmarking<br>Technology trends and benchmarking<br>Global heat map | Status report on the main policies and programs in place what is needed |
| **Technology & liability defenses in place** | **Internal technology talent & skills assessment** |
| Status report on what cyber defenses are in place: technological, assessments, audits, monitoring, testing, insurance | Review top expert executives<br>Review C-suite and CEO performance on cyber-risk management |
| **Incident reporting** | **External experts used/needed** |
| Statistical overview of all incidents at company<br>Specific mention of serious-to-material incidents | Are the right experts in place? Including for periodic board report |
| **Cyber attack crown jewels** | **Cyber actors & stakeholders matrix** |
| Know exactly what your company's crown jewels are--what are the perpetrators and potential perpetrators after? | Who are the potential perpetrators?<br>Who are the company stakeholders and potential victims? |

*Source:* Andrea Bonime-Blanc. 2015 Conference Board Emerging Practices in Cyber-Risk Governance,
© GEC Risk Advisory LLC 2016. All rights reserved.

## Cyber-incident example

**FACTS**. This firm has predictably huge seasonal spikes in customer usage of their on-line product, which is also dependent on a third party for completion of the transaction. Monitoring routines were established to ensure management has its "finger on the pulse" during these busy periods. However, clear triggers had not been established to require formal declaration of a crisis.

**LESSON LEARNED**. Although lots of people, including high-level managers, were watching the transaction flow, in the absence of clearly defined triggers, it was not clear when to declare a crisis and initiate the crisis management plan. It's not always easy to realize when a crisis has begun because instances can start slowly, involve different parts of the ecosystem, can appear to be fixable, and be quite out of hand by the time events have cascaded.

## Additional feedback from the five directors

1. **Do the company or companies you are a board member of have a separate cyber-risk committee or subcommittee (if so, please specify which)?**

   Of the five directors, four said no, one did not respond. The responses were varied: either cyber-security is handled by an existing standing committee, a technology committee or the entire board.

2. **Do the company or companies you are a board member of have a specific crisis management plan in place for cyber-risk? If so, does the board train periodically on cyber-risk incident management?**

   Four of the five directors responded to this question and all in the affirmative – they either have cyber-security included in their crisis management plan and/or have a cyber-plan that is shared with the board.

## A STRATEGIC ROADMAP FOR EFFECTIVE CYBER-RISK GOVERNANCE

When it comes to cyber-risk oversight, boards must move from *sitting back to leaning in*.

What does this mean? It means going from what has been the norm—"sitting back" and absorbing information at best—to "leaning in:" learning, adding the right expertise to the board, asking the right questions and being trained on the implications of cyber-risk gone wrong in their enterprises.

Effectiveness in this case does not mean perfection—it means having the tools necessary to manage the inevitable cyber-crises that will come. And they will come. But so will the opportunities—to improve processes, to button down loose ends, to create clarity and awareness and to perhaps even improve products and services. Based on our discussions with the above directors, it is clear that they are giving a lot more time and attention to cyber-risk.

But the journey from sitting back to leaning in must be done judiciously and appropriately for the specific enterprise. As experienced board members know, there is an art to oversight and a delicate balance between leaning in and leaning in so far that the board ends up leaning over and managing or micro-managing. On the other hand, there is something special about cyber-risk—unlike most other risks confronting organizations today, it is a largely unknowable, multifaceted threat over which a company cannot be expected to be in complete control.

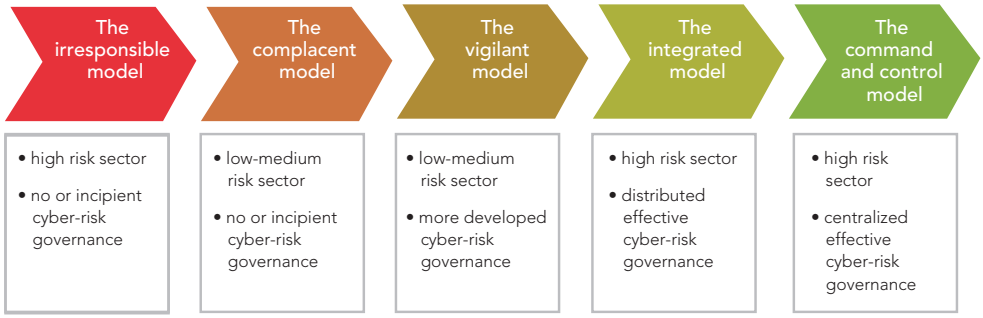
So, how can a board that is still sitting back or just about to embark into greater cyber-risk awareness effectively tackle this issue?

Below is a summary of the three-phased strategic cyber-roadmap to developing mature and responsible cyber-risk governance, It consists of 12 elements that are not only incremental but should always be part of fully mature cyber-risk governance; in other words, boards should always "Know the Basics" (Phase I), always "Oversee Preparedness" (Phase II) and always "Lean In" (Phase III) when it comes to cyber-risk governance. (For more detail, see Appendix C)

Figure 2

A Typology of Cyber-Risk Governance Readiness & Resilience

**The Evolutionary Spectrum**




© GEC Risk Advisory LLC 2016. All rights reserved.

## PHASE I – KNOW THE BASICS

This is the early stage at which a board is no longer in denial or ignorance (i.e., sitting back) and has realized that it needs to do something about cyber-risk governance. It includes several steps that not only need to be taken as a company decides to move forward to a more proactive cyber-risk governance stance but it also includes items that have to be covered on a regular and periodic basis no matter how advanced a company's cyber-risk governance.

## PHASE II – OVERSEE PREPAREDNESS

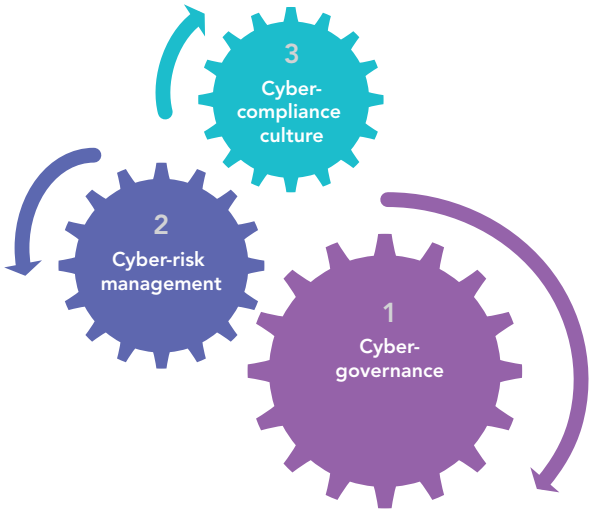
This second phase of the roadmap evidences that the board has moved from a pure "sit-back" approach to a more proactive, learning phase. The results of the evaluations and management discussion from the first phase should inform clearly what steps need to be taken to achieve more effective cyber-risk governance.

Those steps include:

- Having a keen understanding of how enterprise cyber-risk intersects with other key risks
- Having the right external and internal talent to assess and manage cyber-risk
- Adding one or more diverse and/or cyber expert board members
- Establishing what committee is responsible for cyber oversight
- Creating a special cyber-risk charter

Figure 3

**The Cyber-GRC Program**




© GEC Risk Advisory LLC 2016. All rights reserved.

Source: Andrea Bonime-Blanc "Deploying a Voluntary Cyber-Resilience Program: A Strategic Imperative", Chapter 15 in The Cyber-Security Social Contract. The Internet Security Alliance (2016).

## PHASE III – LEAN IN

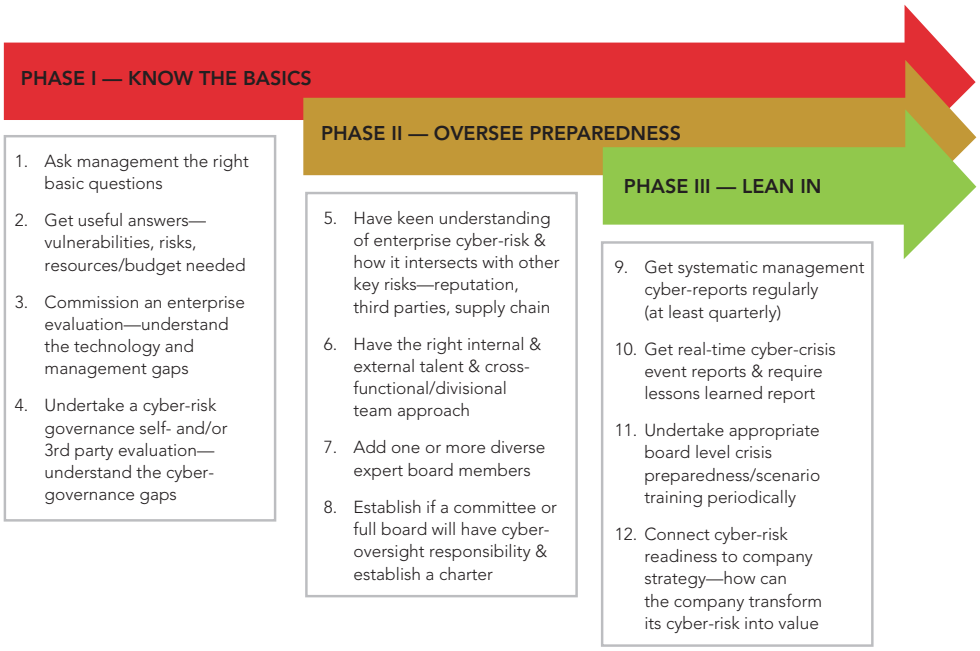
In the final phase of this strategic roadmap a board has reached a lean-in or mature level of cyber-risk oversight. The following four additional elements are critical to helping a board achieve this level of sophistication, which ultimately will serve the company and its stakeholders well: systematic management cyber reports, real time cyber crisis event reports, crisis preparedness/scenario training and connecting cyber risk readiness to company strategy.

Overall, boards need to ask: what are we doing to help the company build the organizational resilience that it needs to be ready for the routine and the extraordinary? By leaning in, a board can encourage management to equip the organization with defenses, risk management and opportunities. Figure 4 below represents an overview of what needs to happen within an enterprise to achieve that cyber-risk governance level of maturity – where cyber-risk governance (at the board level), cyber-risk management (at the executive level) and cyber-risk compliance and culture (at the employee, third party and supply chain levels) co-exist in a synchronous manner.[5]

Figure 4

A Strategic Cyber-Roadmap for the Board

**Building Effective Cyber-Risk Governance**




© GEC Risk Advisory LLC 2016. All rights reserved.

5 From: Andrea Bonime-Blanc. "Deploying a Voluntary Cyber-Resilience Program: A Strategic Imperative", Chapter 15 in The Cyber-Security Social Contract. The Internet Security Alliance (2016).

## CONCLUSION

Achieving effective cyber-risk governance overall is a difficult and complex task that at the end of the day requires attention, customization, nimbleness and willingness to change. While perfection in this area will never be achieved, it is very important for companies and all kinds of organizations (including non-profits, academia, the government) to adopt proper cyber-risk governance as part of overall cyber-resilience.

In the age of hyper-transparency and technological turbo-change, cyber-risk will not go away. It will only become more complicated and potentially dangerous. The very top of any organization (the board) not only has a responsibility and duty of care to the company and its stakeholders; it has one to itself as well. Boards that do not properly oversee and lean-in on the creation of effective cyber-risk governance along the lines of the strategic roadmap presented in this article will be at serious risk.

It is time for diversity of expertise toward cyber-risk oversight to be part of the global boardroom. With the addition of cyber-risk expertise and greater diversity of expertise and background on the board, properly overseeing the cybersecurity risk will not only better protect the company but could lead to more opportunity for those companies that take advantage of technological insights.

APPENDIX A

| Key Takeaways of the 2015 Emerging Practices In Cyber-Risk Governance Report | |
|---|---|
| **2015 Report - key take-away** | **Specific role of the board** |
| 1. Develop a triangular governance approach to cyber risk management | Supervise and oversee that such a triangular governance approach is taken |
| 2. Understand the reputation risk consequences to strategic cyber risk management gone wrong | Understand the strategic reputation risk implications of a cyber-event |
| 3. Know who your cyber risk actors and stake-holders are | Require management to provide a roadmap of principal actual & potential actors/perpetrators & of stakeholders & their company expectations |
| 4. Have a deep understanding of the organization's "crown jewels" | Require management to provide a clear and comprehensive map of company digital & physical crown jewels that are susceptible to cyber-attack |
| 5. Engage in a relevant cyber risk public-pri-vate partnership | Inquire/require that management participate in both private sector industry cyber-benchmarking/ sharing and appropriate industry/government initiatives |
| 6. Develop a cross-disciplinary approach to cyber risk management | Ask/require management whether and how cyber-risk management is taking place cross-disciplinarily within the organization |
| 7. Develop a cross-segmental/divisional approach to cyber risk management | Ask/require management whether/how cyber-risk management is taking place across the organization's divisions and business units |
| 8. Make cyber risk governance an essential part of your organization's resilience approach | Is management (and the board) incorporating cyber-scenarios and preparedness in the organization's overall crisis management, business continuity and data protection programs? Including scenario training? |
| 9. Choose one of the three effective cyber risk governance models | Consider where the organization fits within the five types of cyber-risk readiness and resilience typology (described above) and proactively demand movement in the appropriate direction if the organization is in an unprepared category |
| 10. Transform effective cyber risk governance into an opportunity for better business | Ask management what they are doing to find opportunity and even value in this risk: Is the cyber-risk preparedness of this company advanced enough that it can actually provide added bottom line improvement/revenue opportunity and value to the enterprise now or in the future? |

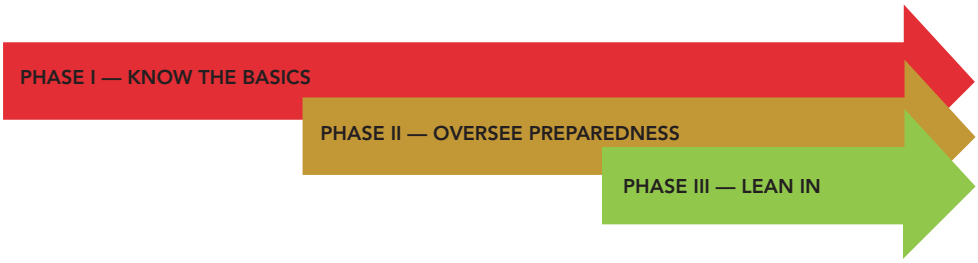
## APPENDIX B

### What we asked the five directors

- What is the single most important thing a board can do to be cyber-risk governance ready?
- How should the board be organized to meet the challenge of cyber-security?
- Where should primary responsibility for cyber-risk governance reside on the board?
- Should the board have a technology and/or cyber committee in charge of such oversight or is it the full board's responsibility?
- Should the board have a cyber-expert director or should the board bring in an external expert?
- Is there a particular practice, framework, guidance or system that your company has deployed on cyber-risk management that you as a board director find to be helpful or a best practice?
- What do you expect from the CEO and management when it comes to cyber-risk management?
- How often should management report to the board, how and with what information?
- What is the future of cyber-risk governance on corporate boards?
- What practice is your board engaging in at this time that is cutting edge and that other boards should consider adopting?

APPENDIX C

## A Strategic Cyber-Roadmap for the Board
## Building Effective Cyber-Risk Governance




© GEC Risk Advisory LLC 2016. All rights reserved.

### PHASE I –Know the basics

**Get useful answers from management – on vulnerabilities, risks, budget, resources, etc.** Critically important at this stage (and subsequently periodically) is to make sure that management has an opportunity to present what they know, what they have done, their talent and budgetary resources (or lack thereof), what their go forward needs are, etc. This is critically important especially in view of what might be needed with regard to the next two elements.

**Commission an enterprise cyber-security evaluation – understand the technology & management talent gaps** Even if management has provided useful answers it is probably advisable (unless management has already commissioned an evaluation) for the board to engage an independent technology gap assessment or an independent review of one that has already been conducted.

**Undertake a cyber-risk governance evaluation–understand the board level gaps** this is a critical element of the first phase of cyber-governance awareness (and something that should be undergone from time to time thereafter) because most boards (at least for now) do not have cyber-risk or governance, risk and/or compliance directors on board, so evaluating the needs and gaps at the board level itself is a necessary step to Phase II and the ability of the board to "Oversee Preparedness."

### PHASE II – Oversee preparedness

**Have a keen understanding of enterprise cyber-risk and how it intersects with other key risks** Most experts will acknowledge that while cyber is a special kind of risk, its management belongs squarely within a company's enterprise risk management framework. A more mature level of risk management within an enterprise will make it easier for management to manage and report and the board to oversee cyber-risk within that larger framework also because cyber-risk is not a stand alone risk but one that intersects with several other key risks including reputation risk, third party and supply chain risk, employee risk and others.

**Have the right internal and external talent and a cross-functional / divisional team approach** This element requires that there be both internal and external recognized experts, issue owners and cross-functional and cross-divisional teams handling the more day to day routine cyber-risk management and preparing for the more exceptional crises that will inevitably come.

**Add one or more diverse and /or expert board members** This point seems to be well established among board directors experienced with this issue as our review of the five director case studies clearly underlined. Whether the new board member or members to be brought in to help with cyber-risk oversight are strictly technology/cyber experts, or more broadly experienced governance, risk and compliance experts, companies need to include one or more of such board members depending on the size, footprint, sector, vulnerability, etc., of their particular enterprise.

**Establish what committee or if full board will have cyber-oversight responsibility and establish a charter** While there is a range of opinions on this theme, it is clear that boards need to either assign a specific existing committee to oversee cyber, establish a new technology or risk committee to include cyber, or ensure that if they will not anoint a committee as cyber-lead for the board, that the full board indeed undertake the full responsibility and burden of exercising proactive cyber-risk oversight. This said, all savvy board members agree on one thing: the entire board has a duty of care to oversee cyber-risk for their enterprise. Another key step in underlining responsibility and oversight whether to the full board or a committee is to establish a set of principles and tasks via a cyber-governance charter.

## PHASE III – Lean in

**Get systematic management cyber-reports regularly (quarterly)** The more cyber-sophisticated boards will receive routine reports from management not once in a while but systematically (at least quarterly) and will have an appropriate dashboard of metrics and other information that they will grow accustomed to seeing and asking questions about. See Figure 1 for an example of some of the information that might fit on such a dashboard.

**Get real-time cyber-crisis event reports (through committee or board member w/designated expertise) & require lessons learned exercise** The more sophisticated boards will also have a system by which the designated committee or board member (expert or chair) will be advised when and if a cyber-event occurs at the company. Specific tie-in with a company's crisis management and business continuity programs will be required for this to be effective.

**Undertake appropriate board level crisis preparedness/scenario training periodically (yearly)** A key ingredient in achieving effective cyber-risk governance at the board level is for the board itself to be trained in cyber-event scenario planning or at a minimum up to date cyber-risk education. While this does not have to occur often, it should occur periodically and involve all board members, not just the oversight committee.

**Connect cyber-risk readiness to company strategy** To complete the full picture on cyber-risk oversight and preparedness, the board should also take some time to understand how cyber might affect business strategy, whether cyber (and related technologies such as machine learning/artificial intelligence/the cloud etc.) can also have a value-added effect on the business and whether there are opportunities for the company to transform its cyber-risk into value.

## ABOUT THE AUTHOR

**Andrea Bonime-Blanc** is the lead cyber-risk governance author and researcher for The Conference Board. She is the CEO of GEC Risk Advisory LLC, the global governance, risk, ethics, compliance, reputation, and crisis advisory firm, serving executives, boards, investors, and advisors in diverse sectors worldwide.

Prior to founding GEC Risk Advisory in 2013, Dr. Bonime-Blanc spent two decades as a senior executive in companies ranging from start-ups to Fortune 250 companies, leading governance, legal, ethics, compliance, risk, crisis management, internal audit, external affairs, and corporate responsibility functions, including positions at Bertelsmann, the global media company; Verint Systems, a "big data" technology company; and PSEG Global, a division of PSEG, the leading U.S. energy and utility company. She began her career as an international project finance lawyer at Cleary Gottlieb Steen & Hamilton and has served as chair, audit committee chair, and a member of several boards for the past 25 years.

Bonime-Blanc is the author of *The Reputation Risk Handbook: Surviving and Thriving in the Age of Hyper-Transparency*, which the Wall Street Journal calls "The book on reputation risk." She writes a periodic column for Ethical Corporation Magazine and tweets @GlobalEthicist. Recognized in both 2015 and 2014 as one of Ethisphere's *100 Most Influential People in Business Ethics* and a *2014 Top 100 Thought Leader in Trustworthy Business*, she recently joined the Advisory Board of Spain's leading think tank, *Corporate Excellence: Centre for Reputation Leadership*, and is a life member of the Council on Foreign Relations.

Bonime-Blanc was born and raised in Europe and holds a Joint JD in Law and PhD in Political Science from Columbia University; she is an adjunct professor at NYU and a frequent international keynote speaker. She is an exhibited artist and photographer and lives with her family in New York City.

## ABOUT DIRECTOR NOTES

*Director Notes* is a series of online publications in which The Conference Board engages experts from several disciplines of business leadership, including corporate governance, risk oversight, and sustainability, in an open dialogue about topical issues of concern to member companies. The opinions expressed in this report are those of the author(s) only and do not necessarily reflect the views of The Conference Board. The Conference Board makes no representation as to the accuracy and completeness of the content. This report is not intended to provide legal advice with respect to any particular situation, and no legal or business decision should be based solely on its content.

## ABOUT THE SERIES DIRECTOR

**Matteo Tonello** is managing director of corporate leadership at The Conference Board in New York. In his role, Tonello advises members of The Conference Board on issues of corporate governance, regulatory compliance, and risk management. He regularly participates as a speaker and moderator in educational programs on governance best practices and conducts analyses and research in collaboration with leading corporations, institutional investors and professional firms. He is the author of several publications, including *Corporate Governance Handbook: Legal Standards and Board Practices*, the annual *U.S. Directors' Compensation and Board Practices* and *Institutional Investment reports, and Sustainability in the Boardrooom*. Recently, he served as the co-chair of The Conference Board Expert Committee on Shareholder Activism and on the Technical Advisory Board to The Conference Board Task Force on Executive Compensation. He is a member of the Network for Sustainable Financial Markets. Prior to joining The Conference Board, he practiced corporate law at Davis Polk & Wardwell. Tonello is a graduate of Harvard Law School and the University of Bologna.

## ABOUT THE EXECUTIVE EDITOR

**Gary Larkin** is a research associate in the corporate leadership department at The Conference Board in New York. His research focuses on corporate governance, including succession planning, board composition, and shareholder activism. Larkin serves as executive editor of *Director Notes*, an online publication published by The Conference Board for corporate board members and business executives that covers issues such as governance, risk, and sustainability. He is also the editor of the Governance Center Blog. Prior to joining The Conference Board, he was the editor and writer of PwC's *Governance Insights* Center's biweekly newsletter and editor and writer of KPMG's *Audit Committee Insights* biweekly newsletter. Larkin has served as managing editor of The Bond Buyer and editor in chief of the Hartford Business Journal.

THE CONFERENCE BOARD is a global, independent business membership and research association working in the public interest. Our mission is unique: to provide the world's leading organizations with the practical knowledge they need to improve their performance *and* better serve society. The Conference Board is a non-advocacy, not-for-profit entity, holding 501(c)(3) tax-exempt status in the USA.

**THE CONFERENCE BOARD, INC.** | www.conferenceboard.org

AMERICAS
+1 212 759 0900 | customer.service@conferenceboard.org

ASIA
+65 6325 3121 | service.ap@conferenceboard.org

EUROPE, MIDDLE EAST, AFRICA
+32 2 675 54 05 | brussels@conferenceboard.org

THE COMMITTEE FOR ECONOMIC DEVELOPMENT
OF THE CONFERENCE BOARD
+1 202 469 7286 | www.ced.org

THE DEMAND INSTITUTE
A Division of THE CONFERENCE BOARD
+1 212 759 0900

**THE CONFERENCE BOARD OF CANADA** | +1 613 526 3280 | www.conferenceboard.ca

To learn more about The Conference Board corporate membership, please email us at membership@conferenceboard.org