THE CONFERENCE BOARD
Trusted Insights for Business Worldwide

Emerging Practices In Cyber Risk Governance

CEO STRATEGIC IMPLICATIONS

This publication is part of a suite of products on this issue. For additional resources visit:

www.conferenceboard.org/cyber-risk-governance

No business is completely immune from the risk of a breach in its cyber security. And this cyber risk is not a stand-alone or isolated issue. It cuts across many other major risks—including reputation risk—that can adversely affect an organization's strategy, business plan, and even survival.

Given cyber attackers' ever-broadening degree of sophistication, any entity—corporate, nonprofit, public—that does not have a well-formed, thought-through, and constantly tested cyber risk governance framework will find it increasingly difficult to manage, mitigate, and counter cyber risk.

The best cyber risk governance begins with the board but is only complete if it is in essence a triangular relationship that includes the C-suite, which has primary responsibility for cyber security strategy and risk management, and the top cyber security talent, which leads and implements the details of the cyber risk and security plan on a daily basis.

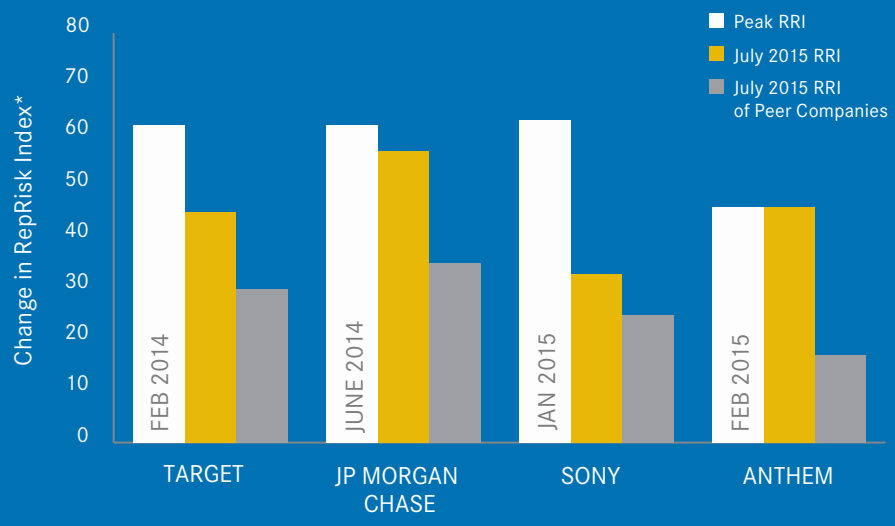
What Is Cyber Risk Governance?

"Cyber risk governance" is a framework an organization adopts to deal with the new and evolving risks relating to cyber space coming from within and without. In this framework, the key actors are the board, the C-suite or executive team, and frontline top management in charge of executing cyber risk management. This cyber risk governance team:

- Adopts, oversees, and promotes an appropriate, concerted, and coordinated philosophy or approach to cyber risk and cyber security for the organization;
- Develops the necessary and appropriate strategy (and budget, resources, and incentives) to execute on that philosophy or approach; and
- Implements that strategy in the most nimble and effective manner possible at an operational and tactical level.

R-1592-15-CEO

Reputation Risk Effects at the Four Companies Examined



TARGET

PEAK RRI Occurred at height of bad publicity and consequences of cyber breach becoming fully known

Current RRI Has recovered over time slowly but still relatively high for its peer group of companies, suggesting a longer-term reputational taint from this affair

JP MORGAN CHASE

PEAK RRI Occurred a couple of months prior to cyber breach being made public and potentially reflecting other bad publicity regarding multiple fines and litigation JP Morgan was dealing with at the time

Current RRI Not much lower and still relatively high compared to peer companies, reflecting the fact that from a reputation risk standpoint, JP Morgan continues to be very much in the crosshairs of regulators and the media

SONY

PEAK RRI Occurred as the fuller implications of the Sony Pictures Entertainment cyber hack became known, including major salacious inside Hollywood details revealed by hacked emails

Current RRI Has dropped to within the range of peer companies, reflecting the fact that the cyber hack did not have long-term negative reputation risk consequences for the company

ANTHEM

PEAK RRI Occurred immediately upon revelation of the cyber hack and has continued to this day

Current RRI Continues through mid-2015, showing an ongoing high reputation risk impact and pressure on Anthem, with a very high RRI relative to its peer companies

* The RepRisk Index (RRI) captures criticism and quantifies a company's or project's exposure to controversial environmental, social, and governance issues. It does not measure overall reputation but rather is an indicator of reputational risk. The range is from 0 to 100, with 0 to 25 indicating low risk exposure, 25 to 50 indicating medium risk exposure, 50 to 75 indicating high risk exposure, and 75 to 100 indicating very high risk exposure. A "Peak RRI" signifies the highest level of criticism in two years. For more on this methodology, see: http://www.reprisk.com/methodology/.

Source: RepRisk AG

Cyber Risk Management Gone Wrong

We examined the qualitative and quantitative consequences of cyber breaches in the past two years on the financial and reputational well-being of four companies and their stakeholders—Target, JP Morgan, Anthem, and Sony—and found that the attacks had varying degrees of effect. In analyzing these cases, we used two sets of data—one relating to the financial impact of the cyber cases on the companies' stock performance and the other presenting a data-driven reputation risk index. In some cases, as in that of JP Morgan, the company's cyber risk readiness allowed it to emerge relatively unscathed. In other cases—such as those of Anthem and Target—lack of cyber risk preparedness was partly responsible for more serious financial and reputational consequences.

Examples of Proactive Cyber Risk Governance

We profiled five companies: an electric power company, a technology company with a presence in 100-plus countries, a global health care company, a global business process outsourcing and computing services company, and a Europe-based global insurance and financial company.

From sectors in which data privacy is king (the health care and business process outsourcing sectors) to sectors where physical security is paramount (protection of the electric grid), these companies provide a cross-section of leading and even best practices in cyber risk governance in the corporate world today.

Our review of the cyber risk governance framework of these companies zeroes in on several key questions, from which we derive some general findings:

When and why did cyber risk governance begin at the company?

Most of these companies started their cyber risk governance programs (or elements of it) before a major attack or threat occurred or was disclosed. Most of these companies were ahead of the game. They also had substantial cyber risk, enterprise risk management, and corporate security schemes in place prior to starting a more focused cyber risk approach.

How is cyber risk governance managed at the company today?

WHO OWNS CYBER RISK MANAGEMENT?

In most cases, early on, cyber risk management or information security (InfoSec) may have originated in the information technology function under the CIO or CTO, but in all cases, InfoSec has migrated to a different main function or to a multifunctional approach, and there is a strong interdisciplinary and cross-divisional approach to cyber risk management. In a couple of cases, an enhanced global corporate security function has taken lead responsibility for cyber risk management.

THE ROLE OF THE CEO & C-SUITE

In all cases, the CEO and the C-suite play an important role in leading the strategic discussion and overseeing the big picture implementation. Indeed, in the most advanced cases, the enhanced InfoSec functional leader—a global head of security in one case and a trio of high-level executives (including the chief risk officer) in another—reports at least monthly to the CEO and/or C-suite.

What is the role of the board in cyber risk oversight today?

THE BOARDS OF THESE COMPANIES HAVE SEVERAL KEY THEMES IN COMMON:

- They have moved from rare engagement on this issue (maybe once a year) to receiving periodic reporting (at least quarterly) and, in a couple of cases, crisis management scenario planning.
- In some cases, a committee has direct responsibility for tracking this risk, but in most cases, the entire board is engaged in cyber risk oversight.
- They regularly engage outside experts for updates, education, and benchmarking.

Important current and future cyber risk governance practices and opportunities

- Among the most advanced practices was the creation of a stand-alone business unit with direct reporting to the CEO and the board, freeing that business unit from having to ask for funding from the other main businesses and providing a degree of independence while maintaining a strong line of accountability to the highest levels of the organization.
- A strong, nimble, cross-disciplinary approach to cyber risk management led by top functional and technical experts is the wave of the future in keeping pace with the fast-changing nature of this pervasive and constantly metamorphosing threat.
- Two of the five companies have specifically turned this risk into an opportunity by developing new products and services from the very risk they are guarding against—in one case, cyber risk insurance and in the other case, cyber risk security software.
- Greater board engagement and expertise on risk management generally and cyber risk management in particular appear to facilitate an organization's ability to oversee and manage this risk.

10 Ways to Reduce Cyber Risk With Effective Governance

1 **Develop a triangular governance approach to cyber risk management**

The board must take a proactive approach to cyber risk oversight Whether the domain of one or more committees or of the entire board and/or its chairman, the board sets the tone from the top on cyber risk governance and must take the governance lead. Key elements the board should consider for cyber risk governance oversight include an update on the architecture of cyber risk management, the resources and budget allocated, and a list of company "crown jewels" from a cyber risk standpoint.

The CEO and the C-suite must take charge of cyber risk strategy and management Depending on the cyber risk readiness required at a given company, more or less direct CEO involvement on a regular basis is highly recommended. The more an organization is at risk, the more actual attention, leadership, and support will be needed from the very top of the executive food chain. Depending on the type of industry and other criteria that determine cyber risk intensity, the C-suite should consider whether to have a dedicated cyber risk/security executive at the executive table.

The CEO and the board must ensure that the right frontline talent and resources are deployed Cyber risk governance is complete when a company has the board engaged, the CEO and C-suite deployed, and the right balance of top technological and cyber expertise within its management ranks. This also entails getting the right outside experts in place for specific tasks, assessments, and reviews.

2 **Understand the reputation risk consequences to strategic cyber risk management gone wrong**

Cyber risk can often become a material risk with potential additional and amplifying reputation risk consequences; it is related to and potentially cuts across many other types of risks. For this reason, cyber risk should be at the top of many companies' risk prioritization, whether they have suffered from a major or material cyber attack (yet) or not. The strong reputational risk relationship to cyber security mandates board oversight and proper governance well in advance of a major incident.

3 **Know who your cyber risk actors and stakeholders are**

Critical to the success of a cyber risk governance framework is having a clear sense and inventory of who the key cyber risk actors are and who has the principal stake or interest in proper cyber risk governance. An understanding of these actors and especially the stakeholders allows an organization to gauge the downside risk of not meeting stakeholders' expectations, which is a clear indicator of increasing potential reputational risk as well.

4 **Have a deep understanding of the organization's "crown jewels"**

A successful triangular cyber risk governance framework necessitates a clear, in-depth understanding of the "crown jewels" residing within the organization that may be interesting to and targeted by cyber perpetrators—whether they are intellectual property, personally identifiable information, trade secrets, executive personal profiles, or government contract information. Knowing what cyber attackers may look for allows for stronger and more capable cyber risk oversight and management. No cyber risk governance program will work without a systematic and constantly updated inventory and protection of such matters and assets that would serve as targets for cyber attackers.

5 **Engage in a relevant cyber risk public-private partnership**

The US government's National Institute of Standards and Technology framework makes a relatively strong case for certain companies to consider joining a public-private partnership on cyber readiness, depending heavily on the type of business and overall characteristics of the company's footprint, products, and services. Austria, Germany, the Netherlands, Spain, and the United Kingdom have established formal public-private partnerships for cyber security, while both Japan and Malaysia have set up official partnerships.

6 **Develop a cross-disciplinary approach to cyber risk management**

There is a strong case to be made for proactive cross-disciplinary coordination and collaboration on cyber risk governance. This is partly in recognition of the complexity and novelty of cyber risk, where no one expert can really "own" the issue, as well as a recognition of the fast-moving aspect of cyber risk requiring the best and brightest minds from a variety of disciplines. In today's hypercomplex world, no risk management can be properly triangulated without the coordination of key interdisciplinary experts.

7 **Develop a cross-segmental/divisional approach to cyber risk management**

Another useful and cutting-edge trend entails deploying an integrated cross-disciplinary and cross-divisional team to keep a steady eye on cyber risk management within the company. Whether this means that overall cyber risk management is done in a single global command-and-control structure or more of a distributed model, where each segment or division has a version of the global cyber risk structure, is up to the company, its culture, and its history. The most successful companies addressing this issue have created some form of mixed interdisciplinary and cross-segmental teams.

8 **Make cyber risk governance an essential part of your organization's resilience approach**

A practice at leading companies is to have cyber risk fully embedded in and part of what some call the "resilience triangle": crisis management, business continuity, and disaster recovery planning. For those that perceived their cyber risk as high to very high (for example, utilities and global technology companies), that means performing cyber security-related crisis management drills on a periodic and even surprise basis, mainly with executives but sometimes including board members. To be properly handled, all risk—and especially cyber risk, which can imperil and paralyze an entity within seconds—must be taken into account in the crisis management and business continuity context.

9 **Choose one of the three effective cyber risk governance models**

The most effective models of cyber risk governance depend on leadership that is engaged, knowledgeable, and vigilant on cyber risk issues. In the **Vigilant Model**, the entity has a relatively low to medium exposure to cyber risk; in the **Integrated Model,** there is effective, integrated cyber risk management and governance at a largely decentralized, medium to high exposure organization; in the **Command & Control Model**, the most evolved cyber risk governance model, cyber risk management is organized in a centralized, command-and-control manner for a more centralized organization that has medium to high cyber risk exposure.

10 **Transform effective cyber risk governance into an opportunity for better business**

Some leading companies are transforming their cyber risk into possible additional value in the form of new products and services. While not every company can actually develop new revenue streams from better cyber risk readiness and governance, all companies can create more efficient, streamlined, and cost-effective approaches to cyber risk governance. This approach will undoubtedly save companies both financial and reputational capital if a cyber incident occurs.

READER SURVEY Please take a few moments to answer two questions Click here

CONNECT with our experts, your peers, and more thought leadership on this topic:
www.conference-board.org/cyber-risk-governance

Follow/join the conversation on Twitter #tcbCyber

OUR EXPERT

Andrea Bonime-Blanc is the CEO and founder of GEC Risk Advisory LLC, the global governance, risk, integrity, reputation, and crisis advisory firm serving executives, boards, investors, and advisors in diverse sectors worldwide.

Bonime-Blanc spent two decades as a senior executive in companies ranging from start-ups to Fortune 250, leading governance, legal, ethics, compliance, risk, crisis management, internal audit, information security, external affairs, and corporate responsibility functions, including at Bertelsmann, the global media company; Verint Systems, a "big data" technology company; and PSEG Global, a division of PSEG, the leading US 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 The GlobalEthicist for *Ethical Corporation Magazine*. Recognized as an Ethisphere 2014 100 Most Influential People in Business Ethics and a 2014 Top 100 Thought Leader in Trustworthy Business, she recently also 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 New York University and a frequent international keynote speaker.

Email: abonimeblanc@gecrisk.com
Twitter: @GlobalEthicist

LEARN MORE

RELATED RESOURCES FROM THE CONFERENCE BOARD

CEO and Executive Compensation Practices: 2015 Edition
August 2015

The Next Frontier for Boards: Oversight of Risk Culture
Director Notes, June 2015

Big Data Doesn't Mean 'Big Brother' (Implications for Legal and Risk Officers)
May 2015

The Board's Role in Cybersecurity
Director Notes, March 2014

WEBCASTS

Governance Watch, hosted in collaboration with Cleary Gottlieb Steen & Hamilton
December 17, 2015

Cyber Risk Communications (on-demand webcast)
April 23, 2015

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

PUBLISHING TEAM
Sara Churchville, Peter Drubin, Kathleen Mercandetti, Marta Rodin

R-1592-15-CEO

ISBN: 978-0-8237-1194-9