point of

view

July 2017

Cyber risk management
Enhancing stakeholder confidence

pwc

Meeting the cyber risk challenge

- The cyber threat landscape continues to evolve, and managing cybersecurity risk is becoming more complex. Cyber threats have progressed from being primarily focused on theft of personal information to broader threats against intellectual property, ransomware, and denial-of-service attacks.

- Stakeholders are looking to gain confidence in companies' ability to effectively manage cyber risks. Boards are seeking information and metrics on how companies are addressing cybersecurity. Investors are trying to gauge how potential threats could impact companies' growth prospects. At the same time, governments' and regulators' scrutiny of companies' cyber risk is intensifying, as they seek to protect infrastructure, and consumers and their personal information.

- The AICPA recently released a voluntary cybersecurity reporting framework aimed at enhancing companies' communication about how they are managing cybersecurity risk. The reporting framework and related criteria apply to the performance of a cybersecurity risk management engagement. However, management can leverage the criteria to enhance communication with its board and external stakeholders about the company's cyber risk management efforts.

- It is imperative that companies have a comprehensive cyber risk management program. The program should address specific risks to the business, identify how management keeps current with new threats to its industry and the broader marketplace, and include a tested cyber incident response plan that contains robust communication and brand management protocols. While there are numerous frameworks and resources available to assist companies in their cyber risk management efforts, care should be taken in deciding which are suitable based on companies' cyber risk maturity level and stakeholder needs.

The cybersecurity challenge

Background

Cybersecurity remains a critical issue for governments and companies of all sizes. Managing cyber risk has become more complex, and is top of mind for business leaders. PwC's 2017 global CEO survey found it among the fastest-rising threats to companies' growth prospects. Cyber threats have evolved from being primarily focused on theft of customer personal information to broader threats against intellectual property such as trade secrets, product information, and negotiating strategies. Cyber threats also include use of ransomware and denial-of-service attacks. As a result, many companies' strategy has expanded from a focus on prevention to building resilience in the wake of a cyber breach. However, they may not be moving quickly enough. PwC's 2016 Global Economic Crime Survey revealed that only 37% of organizations have a cyber incident response plan in place.

In 2016, cybercrime rose to become the second most reported economic crime, affecting 32% of organizations.[1] The costs associated with a cyber attack can be staggering, and the impacts wide-ranging. Lost business, brand and reputational damage, legal, crisis communication and forensics costs, and service disruption are among some of the costs and impacts. The recent global malware attack, known as WannaCry, impacted more than 200,000 computers in 150 countries, causing mass disruption to banks, hospitals, and other organizations. Some estimate that cybercrime will cost businesses over $2 trillion by 2019.[2]

A tangled web

Technology continues to transform how businesses operate and interconnects them with their customers, suppliers, partners, and other third-parties. This raises the stakes for managing cyber risk. Outsourcing of services, such as IT and payroll, also increases cyber risk. Why? These services typically involve the transfer of, or access to, information, creating more access points for cyber criminals, and widening the potential impact of a breach.

The rise of the Internet of Things (IoT) has also increased cyber risks exponentially. IoT refers to increased machine-to-machine communication. It is the connectivity of physical devices, embedded with software, sensors, and network connectivity that enable these objects to collect and exchange data. This includes things like cars, medical devices, and security systems, which have risks individually, and create even higher risks when information is exchanged.

Cybercrime continues to escalate in a hyperconnected business ecosystem

Stakeholders want more confidence

Stakeholders are interested in understanding how companies manage cybersecurity risks. Boards and audit committees, which often are responsible for the oversight of cybersecurity, want more information from management on the effectiveness of a company's cybersecurity risk management programs. However, they may not be getting the information they need. Only 36% of directors are very comfortable that management provides the board with adequate reporting on security metrics.[3] Similarly, investors want more transparency into how cyber risks could impact a company's value and growth prospects. In our 2017 global investor survey, investors identified cybersecurity as a top 5 threat to the growth prospects of the companies they follow or invest in.

Regulatory landscape

As cyber threats evolve, regulators' scrutiny of companies' cyber risk is intensifying. For example, the New York State Department of Financial Services (NYSDFS) implemented a cybersecurity regulation that requires banks, insurance companies, and other financial services institutions to maintain a cybersecurity program. Effective March 1, 2017, companies must annually submit a Certification of compliance with the NYSDFS cybersecurity regulations.

[1] PwC, *Global Economic Crime survey*, 2016

[2] Juniper Research, *The Future of Cybercrime & Security, 2017*

[3] PwC, *Annual Corporate Directors Survey, 2016*

Responding to the marketplace

Legislation has also expanded across the US. In 2016, cyber-related legislation was enacted in fifteen states addressing:

- Protection of information in government agencies
- Exemptions from state Freedom of Information or public records acts for information that could jeopardize the security of critical information or infrastructure
- Cyber/computer crimes

Countries are also instituting laws and regulations to protect the personal data of their citizens. The proliferation of requirements can make it challenging for companies to determine which apply and how to interpret them.

Voluntary cybersecurity frameworks

In deciding on a comprehensive and effective cyber risk management structure, organizations have access to a variety of frameworks. These resources have been created by governments, industry specific groups, independent agencies, and other stakeholders. The frameworks can assist companies with designing cybersecurity controls specific to cybersecurity risks. Some commonly used voluntary frameworks include:

- National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity – A risk-based cybersecurity framework developed by a collaboration between industry and government. It includes five functional areas: Identify, Protect, Detect, Respond, and Recover.
- ISO/IEC 27001/27002- A group of standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). These standards provide guidance for securing financial information, intellectual property, employee data, and other information.
- SEC cybersecurity guidelines – Guidance for investment companies and advisers that includes steps to consider to address cyber risk. The SEC also issued guidance addressing the disclosure of cybersecurity risks and incidents.

These frameworks provide a baseline for companies in addressing cyber risk. However, they are only one of many resources available to companies as they evaluate their cybersecurity program.

Building effective cyber risk management

So what other steps can a company take to enhance its cyber risk management? While there is no one-size fits all plan, there are leading practices companies can consider. Among the most important is ensuring there is a commitment from the top of the organization to support investment in cyber risk management capabilities. Leadership support in this area demonstrates its importance, which helps to build a culture of risk mitigation.

As senior business leaders are becoming more engaged on the topic of cybersecurity, the need for a more practical and informed cybersecurity risk management capability is mounting

Husam Brohi, Director, Cybersecurity and privacy, PwC

Leading companies take a holistic view of business strategy, focusing on business continuity planning and crisis response in the event of a cyber attack. To do this, they leverage people from all functions who impact cybersecurity, including information security, product security, and data privacy. As part of this strategic focus, they also model cyber risk scenarios based on emerging threats. After understanding risk scenarios, a company can make more informed decisions to address the vulnerabilities that are identified.

Further, leading companies provide the board and senior management with cybermetrics that measure risk and performance. They also implement training programs and enhance processes, as necessary. And, they have a robust communication plan to provide transparency in the event of a cyber attack.

A new cybersecurity reporting framework

In April 2017, the AICPA released a cybersecurity risk management reporting framework. The framework enables organizations to communicate the effectiveness of their cybersecurity risk management programs and provides guidance for CPAs in attesting to management's assertions. The reporting framework also provides users with useful information about a company's cyber risk management program. Reports issued using the new framework include:

Building resilience and confidence

- Management's description of the company's cybersecurity risk management program aligned to suitable description criteria (e.g., NIST)
- Management's assertion - An assertion about whether the description is presented in accordance with the criteria, and whether the program's controls were effective in achieving the company's objectives based on the control criteria (e.g., Trust Services Criteria for security, availability, and confidentiality).
- The practitioner's opinion - An attestation opinion on the description of the company's cybersecurity risk management program and the effectiveness of the controls within the program.

Because the reporting framework is voluntary, companies have flexibility in implementing the framework's components. This is important because companies are at different levels of maturity in their cyber risk management journey, and may have different objectives.

"Cybersecurity threats are escalating, thereby unnerving boards of directors, managers, investors, and customers of businesses of all sizes..."

Sue Coffey, AICPA, April 26, 2017

Companies might not have a mature cyber risk management program or want to pursue an attestation-level report. However, they can still benefit from the framework. For example, a company may want to use the framework to improve the design of its controls or to establish a common approach when communicating with its board or other stakeholders.

In summary

Enhancing cyber risk management is a business imperative. We believe organizations have an opportunity to take a proactive, strategic approach to cyber risk management. This means having an effective cybersecurity strategy that addresses specific risks to the business, staying current with the threat landscape for the industry and the broader marketplace, and having a tested cyber incidence plan that includes a comprehensive communication plan.

Companies at all levels of cyber risk management sophistication can use available frameworks and resources to build a program that is suitable for their situation. This may mean conducting a readiness assessment, developing a remediation plan, or moving toward a cybersecurity attestation report. Ultimately, providing stakeholders with transparent information that demonstrates the effectiveness of the cyber risk program will build confidence in a company's ability to respond to cyber incidents.

Contact Information

To have a deeper discussion about our point of view on cyber risk management, please contact:

Grant Waterfall
Global Cybersecurity & Privacy Assurance Leader
Email: grant.waterfall@pwc.com

Beth Paul
US Strategic Thought Leader
National Accounting Services Group
Email: elizabeth.paul@pwc.com

Todd Bialick
Trust and Transparency Solutions Leader
Email: todd.bialick@pwc.com