Deloitte.
德勤

CFO Insights
Guarding against cyber threats

Although most cyber attacks do not make national headlines, they can hurt a business in any number of ways, from simply vandalizing its website to shutting down networks, perpetrating fraud, and stealing intellectual property. For many companies, the need to establish an enterprise-wide approach to preventing and responding to such attacks has required increasing attention from boards of directors and executives across the C-suite.

The U.S. Securities and Exchange Commission (SEC) recently weighed in on the issue, making it important for boards and CFOs as well to be part of the process in understanding how such policies work within an organization's broader strategies. A recent release by the SEC's Division of Corporation Finance included guidance intended to "assist registrants in assessing what, if any, disclosures should be provided about cybersecurity." The release, titled CF Disclosure Guidance: Topic No. 2 – Cybersecurity,[1] added that "as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."

Despite the fact that there is no similar guidance issued by authorities in China, many CFOs of non-SEC registrants are proactively seeking ways to beef up their cyber-security. And in this issue of *CFO Insights*, we examine how to take a more risk intelligent view of cyber threats and outline steps companies can take toward more effective cyber threat risk governance.

Taking a risk intelligent view of cyber threats

Those are the same questions that risk committees and organizations address across a broad range of areas—financial risk, reputational risk, regulatory risk, and others. When it comes to cyber risks, however, the term "cyber threat" is often misunderstood or a cyber threat may be underestimated, so these high-level questions may not produce answers that adequately address the threat.

Unless a company is already quite sophisticated in its cyber threat risk management practices, it may not yet have the risk management infrastructure and/or governance elements in place to support a meaningful conversation. For instance, leaders may not have agreed on risk definitions, risk tolerances, or metrics specific to cyber threat risk. Or a company might lack the technology tools to collect and report cyber threat-related information effectively. For many, the active involvement of senior management and board members well outside the information technology (IT) function may be critical.

If an organization is not yet in a position to discuss exposure and effectiveness as such, a first step is to ask the executive team four questions about specific information security practices that are essential to effective cyber threat risk management:

- How do we track what digital information is leaving our organization and where that information is going?
- How do we know who is really logging into our network, and from where?
- How do we control what software is running on our devices?
- How do we limit the information we voluntarily make available to a cyber adversary?

Highly effective cyber risk management processes are repeatable, clearly defined, well-documented, and aligned with an organisation's larger IT risk management (ITRM) and enterprise risk management (ERM) frameworks. The organisation may measure and monitor process effectiveness and efficiency, as well as apply continuous improvement techniques to enhance performance.

At many companies, cybersecurity practices are heavily weighted toward measures, such as firewalls and passwords, aimed at limiting access to the company's network. Even though these precautions are essential, they are not enough, however. Cybercriminals are becoming increasingly adept at infiltrating corporate networks without triggering an intruder alert. Once they are inside, they can easily siphon information off a network unnoticed unless a company is actively looking for signs of suspicious activity.

To help defeat cybercriminals who make it past the access controls, a cyber threat risk management program or set of protocols should include safeguards against unauthorised information distribution, as well as against unauthorised information access. To be effective, a cyber threat risk management program should employ techniques, technologies, and processes that monitor outbound information traffic for both content (is the information appropriate to share?) and destination (where is it being sent?). Destination, in particular, can be a red flag; if information is being sent to a country where a company has no operational presence, it is probably wise to look into who is sending it there and why. An effective program will also be able to restrict the transmission of suspicious communications until their legitimacy is verified, for example, with technologies that electronically "quarantine" the communication while appropriate checks take place.

Characteristics of a mature cyber threat risk management capability

Risk governance (board of directors):	**Communication:** Ongoing dialogue with management; critical metrics and key performance indicators (KPIs) agreed upon and monitored in real time.
Risk infrastructure (owned by executive management, which is responsible for implementing and maintaining the people, process, and technology elements needed to make risk management "work"):	**People:** Executive team has the background knowledge and current information to actively integrate cyber threat risk into broader ERM decisions; enterprise uses cyber threat intelligence to help manage risk in all classes (not just cyber threat risk) to within defined tolerance levels. **Process:** Processes addressed by continuous improvement efforts, including automation and other enabling technologies where appropriate; structured cyber threat risk management program integrated with broader IT risk management and enterprise risk management programs. **Technology:** Technology used to automate not just threat monitoring and alerts, but also other security processes such as malware, forensic analysis, and threat assessment.
Risk ownership (functions and business units):	In addition to the preceding attributes, incentives designed specifically to reward key personnel based on their cyber threat risk management performance.

Steps toward more effective cyber threat risk governance

The following 10 steps can provide a high-level guide for establishing a cyber threat risk governance program, and the approach discussed on the previous page (see "Characteristics of a mature cyber threat risk management capability") can provide a start toward understanding an organization's capabilities for managing and mitigating the ever-present risk that cyber threats pose today. However, neither is intended to substitute for a formal, rigorous IT security assessment performed by specialists.

1. Stay informed about cyber threats and their potential impact on your organisation.
2. Recognize that cyber threat Risk Intelligence is as valuable as traditional business intelligence.
3. Hold a C-level executive accountable for cyber threat risk management.
4. Provide sufficient resources for the organization's cyber threat risk management efforts.
5. Require management to make regular (e.g., quarterly), substantive reports on the organisation's top cyber threat risk management priorities.
6. Expect executives to establish continuous monitoring methods that can help the organisation predict and prevent cyber threat related issues.
7. Require internal audit to evaluate cyber threat risk management effectiveness as part of its quarterly reviews.
8. Expect executives to track and report metrics that quantify the business impact of cyber threat risk management efforts.
9. Monitor current and potential future cybersecurity-related legislation and regulation.
10. Recognize that effective cyber threat risk management can give your company more confidence to take certain "rewarded" risks (e.g., adopting cloud computing) to pursue new value.

Exploring cyber threat risk with an organization's executive team can yield value beyond helping to improve governance over this area of risk alone. It also can lead to a more productive dialogue between an organization's board and executives about IT risk management in general and greater engagement on all aspects of IT risk.

Endnotes

[1] CF Disclosure Guidance: Topic No. 2 – Cybersecurity, Division of Corporate Finance, U.S. Securities and Exchange Commission, October 13, 2011

[2] For more information, read Risk Intelligent Governance in the Age of Cyber Threats—What You Don't Know Could Hurt You

Deloitte CFO Insights are developed with the guidance of Dr. Ajit Kambil, Global Research Director, Deloitte CFO Program; and Lori Calabro, Senior Manager, CFO Education & Events and localised by Sammie Leung, Director of China CFO Program.

Deloitte's CFO Program harnesses the breadth of our capabilities to deliver forward-thinking perspectives and fresh insights to help CFOs manage the complexities of their role, drive more value in their organization, and adapt to the changing strategic shifts in the market.

For more information about Deloitte's CFO Program visit our website at www.deloitte.com/cn/en/cfocentre

Contacts

For more information, please contact:

Danny Lau
National Leader - China CFO Program
Deloitte Touche Tohmatsu
Tel: +852 2852 1015
Email: danlau@deloitte.com.hk

Sammie Leung
Director - China CFO Program
Deloitte Touche Tohmatsu
Tel: +852 2852 1620
Email: saleung@deloitte.com.hk