Building digital services upon a secure foundation

Organisations can no longer stand still in the face of continuing and new cyberthreats. What can, and should boards do?

By
TAN WEN SZE
Assistant Director, Strategy, Cyber Security Agency of Singapore

Cyber threat is borderless. Companies are vulnerable to the increasingly sophisticated cyber crime syndicates and nation-state hackers.

These groups of attackers are developing cheaper and better ways to exploit security loopholes. At the same time, new networked technologies may increase the attack surface. For example, cloud-based transactions and remote access to enterprise systems can be new channels for breaches, so a comprehensive risk assessment is important when deploying them.

Time to get your defences up

Cyber security strategies have to evolve in tandem with technological change. The Singapore government, as many others around the world, is responding to the growing threat (see box, "What Singapore is doing in cybersecurity").

What Singapore is doing in cybersecurity

Many governments are putting in resources to strengthen the countries' resilience against cyberattacks. In Singapore, Dr Yaacob Ibrahim, Minister-in-charge of Cyber Security, has stated that the government will increase cybersecurity expenditure as a share of its IT budget to at least eight per cent in the long term.

Recognising the lack of skilled resources is a challenge faced by many companies, the Government is developing schemes to expand the cybersecurity manpower pool and level up technical competencies.

With the introduction of cybersecurity diplomas by Ngee Ann and Republic Polytechnics, all five polytechnics now offer cybersecurity courses. The universities also offer cybersecurity specialisations such as National University of Singapore's Bachelor of Computing in Information Security and Singapore Institute for Technology's Bachelor of Engineering in Information Security.

Schemes have been launched to help fresh graduates and mid-career professionals enter the cybersecurity profession. For example, the Cyber Security Associates and Technologists Programme (CSAT) developed by CSA and IDA help new entrants up-skill through on-the-job training programmes led by companies which are CSAT training partners.

Government agencies are partnering leading industry players to enhance Singapore's cybersecurity capability development. For instance, FireEye's Asia Pacific Centre of Excellence, in collaboration with Infocomm Development Authority of Singapore, provides manpower training programmes for expert level skills in the area of cyber threat intelligence. The Association of Information Security Professionals and CREST International are partnering the Cyber Security Agency of Singapore to set up a local certification centre to raise professional standards in penetration testing and incident response.

Companies have to follow suit. The good news is more organisations are aware of cyber risks and are increasing their cybersecurity budgets. According to the PwC, CIO and CSO Global State of Information Security Survey 2016, firms worldwide increased their cybersecurity budgets by 24 per cent in 2015.

A well-architected system gives defence tools a better security return on investment. Companies should start by architecting the system to the defenders' advantage and ensuring that cyber defenders understand their own network and activity better than the adversary.

Good practices include maintaining an authorised inventory of assets to enable monitoring, restricting administrative privileges, performing continuous monitoring and ensuring timely patching to remove vulnerabilities.

Organisations should be cognizant of the need for a layered defence. Security cannot be built on the assumption that systems have well-defined boundaries which can be defended by perimeter security tools such as firewalls.

Additional defences have to be placed around more granular assets at the application and data

levels. Examples include data encryption and application control.

Cyber defences also have to be continually updated against new threats. For example, recent high profile cases were dominated by data loss. In 2015, cyber criminals using data modification for ransom was trending.

Bringing cybersecurity from the backroom to the boardroom

A company that raises its defences sufficiently to change the cost equation of a threat actor can reduce, although not eliminate, its own cyber risk. In managing risks, the board is the fourth line of defence for the company.

The board can be more active and proactive in cybersecurity:

1. The board can elevate cyber risk from an IT risk to an enterprise risk. Cyber breaches can result in financial and reputational damage that can set back a company's strategic goals and undermine the confidence of customers, investors and business partners. Addressing cyber risks requires a systematic approach at the enterprise level as these risks are found across the company – from the online shop-front to the networked supply chain, from internal enterprise systems to outsourced cloud services, from traditional computer networks to smart office automation systems. The PwC-CIO-CSO *Global State of Information Security Survey 2016* indicates that there was boards are increasingly involved, with around 45 per cent of the survey participants' boards taking part in the overall security strategy.

2. Directors should increase their level of cyber security literacy. Business units can be called upon to provide cyber risk assessments and reviews of their current policies, processes and budgets to protect key assets to the board. The expertise of enterprise risk management and internal audit teams can be leveraged to provide a macro view of cyber risks specific to the company and facilitate discussions on interdependencies, prioritisation, resourcing, controls and overall resilience. Industry experts can be engaged to provide broad technology and cybersecurity trend briefings.

3. The board can advocate a mindset of "assuming breaches". While good cyber defences can prevent and stop most cyber incidents, they can still be breached by determined and sophisticated attackers, who will continually hunt for weaknesses to exploit. Furthermore, malware can operate quietly in the background until the opportune time, at which point the successful cyberattack may cause widespread damage across the networks more quickly than typical crises. Poorly thought through responses may result in more damage than the actual attack. Whether investors and customers retain confidence in the company depends on the company's communication as much as it does the severity of the attack. Time and resources should be invested to construct and test incident response plans.

4. The board should continuously engage management on cybersecurity. This will help the management and staff recognise that the board is concerned. While no universal set of questions can unearth all vulnerabilities, those listed in the box, "Cybersecurity questions that directors should ask of management" will be a good way for directors to engage with management.

Becoming cyber resilient

Successful cyberattacks are inevitable – even the most technologically sophisticated countries and organisations have fallen victims to this first-world invention. Petty cyber incidents are a fact of (digitally-enabled) life. Nonetheless, if we keep keeping on, improving our cybersecurity strategies and staying vigilant, we can cyber risk and ultimately strengthen our resilience in the event of successful cyberattacks. ■

Cybersecurity questions that directors should ask of management

Assessing risks

- What are the cybersecurity risks of top revenue generating assets?
- What are the cyber risks that our vendors and third-party service providers expose us to? Do our contracts with them have cybersecurity requirements?
- What are the implications of successful breaches – business continuity, legal, financial, reputational?

Assessing cybersecurity maturity

- What is our budget for cybersecurity?
- How is cybersecurity governance managed within the company?
- Does our cybersecurity programme cover technology, people and processes?
- What are the guidelines and processes to ensure that security is considered when we acquire, design, implement, and modify systems?
- What are the different tiers of security for our systems? How are they applied to critical assets?
- How do we configure our systems for security? For example, do we use a whitelist rather than blacklist approach for applications and users? Do we have an effective policy for restricting administrator privileges? Do we know our systems well enough to detect suspicious activity?
- What are the processes for maintaining security? For example, do we close newly discovered vulnerabilities through timely and regular patching?
- How do we validate the security posture of our systems?
- How has our cyber defence model evolved to address new technologies and emerging threats?

Planning ahead

- When building new services on next-generation digital infrastructure, what are the potential cyber risks?
- Does the roadmap for investing in next-generation services include cybersecurity measures?

Incident response

- When was the last time we had a cyber incident, or, what was our most significant near miss? How was it discovered, and how did we respond?
- Do we have cyber incident response drawer plans? Have these been tested?
- When and what will we communicate to investors and customers after a cyber incident has occurred?
- When and how do we engage government regulators and/or law enforcement agencies after a cyber incident has occurred?