Deloitte.

Digital Directors: The board's role in the cyber world

Thio Tse Gan, Southeast Asia Leader - Cyber Security

Cyber security threats are not just for information technology specialists anymore. Today, cyber security is drawing attention from the very top, and it has become a huge concern for corporate boards. The reasons for this board level concern are not hard to understand – a number of organisations have been badly shaken by cyber security breaches and their boards are being held accountable. It is estimated that 1 billion records were compromised in 2014[1] and the average loss for each breach ranges between USD52 to USD87[2].

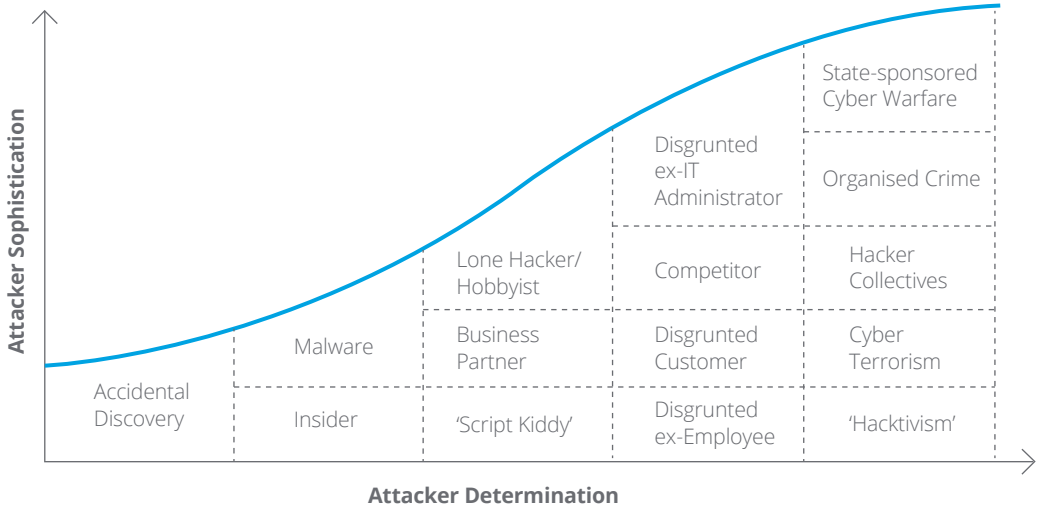
[1] **Gemalto's 2014 Breach level index**
[2] **Verizon's 2015 Data Breach Investigations Report**

So how can directors best conduct oversight and ensure their companies are adequately protected against cyber threats?

Boards, traditionally used to focusing on strategic and governance risks, now find themselves involved in the oversight of technology because the use of technology is critical in determining the success of business. Yet, the benefit that technology has brought to organisations also poses risks that need to be understood and managed.

This advancement of computing power in tandem with that of Moore's law[3], coupled by the level of sophistication of cyber criminals has resulted in exponential growth in the level of cyber threats. These threats are no longer random in nature.

Hence, to effectively provide oversight and governance, the board first need to understand the different types of actors that exist, their level of sophistication and their determination as shown in diagram 1. Cybercriminals strategises and targets organisations that maximises their return on investment, and the most demanding perpetrators are those where the end goal is monetisation of the records that they are able to compromise.



[3] Moore's law states that processor speeds, or overall processing power for computers will double every two years. http://www.mooreslaw.org/

Then as a next step, directors must recognise and understand the importance of their organisation's digital assets such as data, information, applications, and networks that exist within the organisation's walls. This also extends to their suppliers, vendors and other partners, and to data and information that reside in employees' mobile devices.

To gauge the vulnerabilities of these assets, directors might want to ask:

- What information is leaving the organisation, and how?
- What are the "crown jewels" that we must protect?
- What are the cyber threats that our organisation faces?
- How do we know our controls are operating effectively and have they been validated?

The answers to these questions will help set the tone for transparency and a two-way conversation between management and the board, setting up a "ladder" approach in which threats are categorised and managed according to their associated risk with the appropriate priority and resources.

Guarding against cyber threats is a mind-set change across the entire organisation and it should be devoted to achieving three things: Secure.Vigilant.Resilient™

- **Security** of data and systems centers on risk-prioritised policies, procedures, and controls, such as those for devices, e-mail, home-based data, and third-party data use which is important because of the increased number of vendor and outsourcing arrangements.
- **Vigilance** means rapidly flagging violations and suspicious occurrences, and responding appropriately. It also includes being adaptive - absorbing new threat information and adjusting to changes in the business and technology environment to keep eyes on what matters most.
- **Resilience** focuses on damage control and repair, and ensuring that post-attack recovery will be swift.

The balance of investment in secure, vigilant, and resilient capabilities will vary between organisations, and will need to be applied differently to the various areas within an organisation but that said cyber security programs have some common characteristics:

- **They are executive-led.** Executive leaders must set the stage by defining cyber risk management priorities, appetite, and mechanisms of accountability. Support from the top is essential in ensuring that diverse groups and departments collaborate. The Board Risk Committee's charter should also be expanded to include the mandate of how the organisation should be allocating resources to managing cyber risks. Directors can also lead by creating a board cyber chair to oversee management activities on cyber; and ensuring that the appropriate senior management is focused on cyber.

- **They involve everyone.** Although specific roles need to be defined, the program is not the sole responsibility of a single part of the organisation. It requires broad horizontal and vertical participation, and behavioural change throughout the organisation to ensure success.

- **They are programs, not projects.** Although it usually requires a series of projects to get off the ground, such programs require continuous review and improvement cycles to adapt to changes in the business risk and threat landscapes.

- **They are comprehensive and integrated.** The secure, vigilant, and resilient elements are not distinct silos of activity; they are a set of lenses through which every essential business process and growth initiative should be evaluated or planned. Each involves people, process and technology components. And done well, each will improve the others.

- **They reach beyond your walls.** Your ecosystem includes various partners, suppliers, and vendors; significant cyber incidents directly impacting them may also substantially affect you.

Becoming secure, vigilant, and resilient requires that the organisation embrace a fundamentally different view of what we have previously called "security." Yesterday's security program was often perceived as a burden – an externally-imposed set of restrictions, rules, and procedural hurdles that impeded business initiatives. In the pace of today's climate, organisations cannot afford to be slow simply because it cannot be perfectly secured. You cannot secure everything equally. Being secure means focusing protection around the risk-sensitive assets at the heart of your organisation's mission.

Essential truths

01. No industry is immune. Every company's information network will be compromised. It is not a question of if you will be at risk but when and how you manage.

02. Cyber damages go beyond dollars. The long term effects on reputation, brand and morale, are significant and take their toll on organisations.

03. Speed of attack is increasing and response times are shrinking. Small highly skilled groups exact disproportionate damage and threat rate is increasing while response window shrinking.

04. Everything cannot be protected equally. Understanding the need to define 'crown jewels' allow you to make better risk decisions without getting caught up in noise.

05. Traditional controls are necessary but not adequate. Your protection networks and firewalls are probably high enough but it is always important to look at detective controls and new technologies.

06. Regulators and government are important stakeholders. Various privacy rules, guidelines, executive orders, consumer protection are increasing and it is important to keep updated.

Many boards hear from the chief information officer, chief technology officer, chief information security officers or others who are tasked with monitoring the cyber risk. Some company boards engage cyber security experts to speak with them about the risk, how to mitigate it, and signs that may signal a breach. However, Boards should also consider seeking feedback from key partners and customers.

Either way, boards should proactively ask questions of management, champion education and awareness programs company-wide, and treat risk as a priority, because the financial, operational, legal, security, and reputational risks posed by cyber threats are far too serious to ignore. The peril of cyber threat will continue to be present and the first step to averting it lies with the board and their commitment towards managing cyber risk.

Contacts

SEA and Singapore

Thio Tse Gan
Executive Director
+65 6216 3158
tgthio@deloitte.com

Eric Lee
Executive Director
+65 6800 2100
ewklee@deloitte.com

Victor Keong
Executive Director
+65 6216 3222
vkeong@deloitte.com

Siah Weng Yew
Executive Director
+65 6216 3112
wysiah@deloitte.com

Edna Yap
Director
+65 6531 5016
edyap@deloitte.com

Leslie Moller
Director
+65 6800 2333
lesmoller@deloitte.com

Indonesia

Sigit Kwa
Associate Director
+65 6800 2903
skwa@deloitte.com

Malaysia

Megat Mohammad Faisal
Executive Director
+60 3 7610 8863
mkhirjohari@deloitte.com

Ho Siew Kei
Senior Manager
+603 7610 8040
sieho@deloitte.com

Philippines

Maria Carmela Migrino
Director
+63 2 581 9000
cmigrino@deloitte.com

Thailand

Parichart Jiravachara
Executive Director
+66 2676 5700 ext. 11913
pjiravachara@deloitte.com

Pinyo Treepetcharaporn
Director
+66 2676 5700 ext. 11946
ptreepetcharaporn@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/sg/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte Southeast Asia
Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising 290 partners and over 7,400 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region.

All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

About Deloitte Singapore
In Singapore, services are provided by Deloitte & Touche LLP and its subsidiaries and affiliates.

© 2017 Deloitte & Touche Enterprise Risk Services Pte Ltd