Cyber security
Time for a new paradigm

Stéphane Hurtaud
Partner
Information & Technology Risk
Deloitte

More than ever, cyberspace is a land of opportunity but also a dangerous world.

As public and private sector organisations continue to move into cyberspace, so do criminals. Cyber-crime, which is the collective term for criminal activities carried out by means of a computer or the Internet, has become increasingly sophisticated, making it difficult to detect and combat. Nowadays, cyber-crime cases appear in newspaper headlines on a regular basis, showing the extent and the ever-evolving nature of the cyber criminality landscape:

- *'US accuses China of new cyber attacks'* (The Guardian, 31 January 2013)
- *'NSA Prism program taps in to user data of Apple, Google and others'* (The Guardian, 7 June 2013)
- *'5 hackers charged in largest data-breach scheme'* (Bloomberg, 26 July 2013)
- *'LulzSec hackers sentenced for sophisticated global cyber-attacks'* (The Independent, 16 May 2013)

According to Deloitte's 2012 Global Financial Services Industry Security Study[1], about one-quarter of all banks were victims of a cyber breach in 2011. The cost of cyber-crime to the global economy to date may already be substantial. Some studies cite figures as high as US$388 billion[2] or US$1 trillion[3] , which is larger than the global black market in marijuana, cocaine and heroin combined (US$288 billion).

In this context, it goes without saying that cyber security is increasingly becoming a key concern among organisational leadership, including boards of directors. A biennial study of enterprise security governance practices by the Carnegie Mellon University CyLab found a sharp rise in board-level attention paid to the topic. Among companies surveyed in 2012, 48% have a board-level risk committee responsible for privacy and security, up from just 8% in 2008.

The cyber security threats landscape

The 2013 Data Breach Investigations Report (DBIR)[4] consolidates information of the data breach incidents in 2012 from diverse sources to facilitate analysing threats a particular industry is exposed to (a total of 47,000 security incidents with a focus on 621 incidents with confirmed data loss). Deloitte is one of the 19 contributing organisations to this report in light of its incident response and investigation services.

Which industries are at risk?

A definite relationship exists between a particular industry and attack motive, which is most likely a result of the data targeted (e.g. stealing payment cards from retailers and intellectual property from manufacturers):

- 37% of breaches affected financial organisations, mainly due to a large number of ATM skimming incidents
- 24% of breaches occurred in retail environments and restaurants
- 20% of network intrusions involved manufacturing, transportation and utilities

What are threat actors and what are their motivations?

There are four main categories of malicious actors in cyber security:

- State actor: the rise of state actors is significant and considered a great threat according to Deloitte. There are several countries that have openly participated in information warfare for the past several years targeting both private companies and governments

More than ever, cyberspace is a land of opportunity but also a dangerous world

1 http://www.deloitte.com
2 Norton Cybercrime Report 2011
3 The Global Industry Analysts; McAfee, 'Unsecured Economies: Protecting vital information' 2011
4 Verizon 2013 Data Breach Investigation Report

- Organised crime: as explained earlier in this article, cyber crime has surpassed the global drug trade in terms of revenue. This is not simply limited to credit card data, but anything of value
- Hacktivist/activist: the hacktivist movement is the newest addition to the threats list. Groups like Anonymous, Lords of Dharma, Team Poison and others have garnered a lot of media attention
- Insider: insiders can range from the negligent employee who loses a laptop to a completely malicious actor who releases confidential data in an act of vengeance

Most confirmed cases of data loss are perpetrated by outsiders, generally by organised crime groups or state-affiliated groups. The largest number of actors reportedly come from China, Romania, the United States, Bulgaria and Russia.

How do breaches occur (threat actions)?
Threat actions describe what the actor did to cause or to contribute to the breach, taking into consideration that every incident contains one or more actions.

- 52% used some form of hacking, including all attempts to intentionally access or harm information assets without (or in excess of) authorisation by circumventing or thwarting logical security mechanisms
- 76% of network intrusions exploited weak or stolen credentials
- 40% incorporated malware—malware is any malicious software, script or code added to an asset that alters its state or function without permission
- 35% involved physical attacks. Physical threats encompass deliberate actions that involve proximity, possession or force (ATM skimming operations, point-of-sale device tampering, stolen user devices, etc.)
- 29% adopted tactics such as phishing, bribery, extortion, etc.

What is the breach timeline?
Understanding the timeline of an incident can greatly increase the ability to assess and improve an organisation's lines of defence.

- In 84% of network intrusion cases, initial compromise (the time taken for the attacker to get his foot in the door) occurred within hours or less
- In 69% of network intrusion cases, initial compromise to data exfiltration (point when non-public information is first removed from the victim's environment) also occurred within hours or less
- In 66% of network intrusion cases, initial compromise to discovery (i.e. when the victim first learns of the incident) took months or more. In addition, approximately 70% of breaches were discovered by external parties who notified the victim

While these statistics highlight the need to improve prevention measures (ability of organisations to resist cyber-attacks), we must accept the fact that no barrier is impenetrable, and detection/response represents an extremely critical line of defence.

Cyber security risks are not new, so what is different?

The digital revolution is driving business innovation and growth, but also exposing organisations to new and emerging cyber threats. The threat landscape has changed, and the business case for more mature cyber security is better than before. Actually, new business goals and new ways of working are driving business innovation and growth, but these expose us to new and emerging cyber security threats:

- **Consumerisation** ('bring your own'): de-perimeterisation and loss of control of data and devices that have left the traditional data centre boundaries
- **Increased collaboration:** cross-channel, cross-platform sharing of large volumes of sensitive data
- **Technology innovation:** lack of understanding of risks introduced by new tools and processes
- **Commoditisation of IT** (e.g. cloud computing): business functions can procure IT services outside of internal controls
- **Market trust:** reputational damage of a cyber-attack destroys trust which is very hard to recover
- **Globalisation:** new threats arising from expansion into new markets and new ways of working

As organisations increasingly adopt cloud, mobile and social computing, IT environments are becoming more difficult to defend.

Most confirmed cases of data loss are perpetrated by outsiders, generally by organised crime groups or state-affiliated groups

The need for a cyber resilient organisation

As illustrated earlier in this article, the adoption of new technologies and the emergence of new threats result in a more complex risk landscape. In this context, many organisations may not be as effective at managing cyber threat risk as they are at managing risk in other areas.

Cyber resilience requires that organisations have the agility to prevent, detect and respond quickly and effectively, not just to incidents, but also to the consequences of the incidents.

First of all, it's essential to understand the cyber threats to your organisation before you can develop an effective cyber security strategy. For example, cyber risks can be mapped according to three factors:

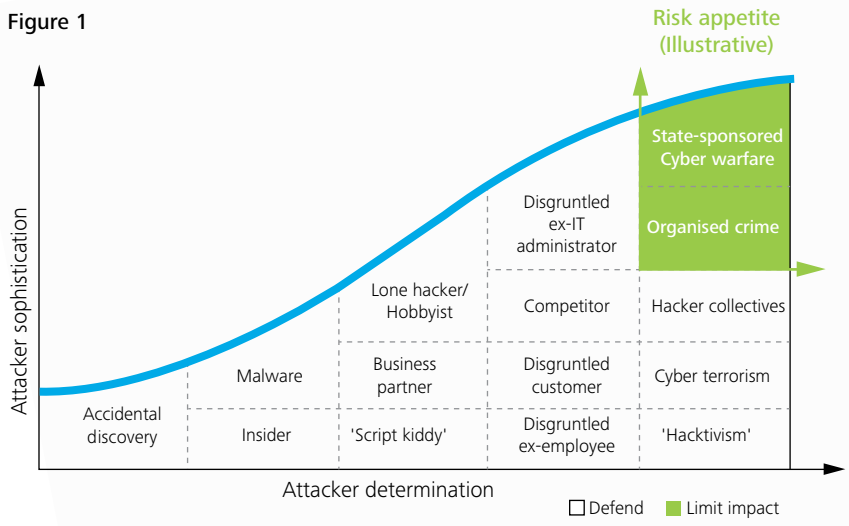
- Does the organisation focus on preventing the risk or detecting and responding to it if it occurs?
- Is the risk known and understood (does it relate to a current threat?), or unknown with little or no understanding (a future threat)?
- What level of concern does the risk pose?

The maturity of an attacker can be measured by their sophistication and determination. Those that are more mature are harder to stop, and there is a decreasing ROI on controls that prevent the most mature attackers. Depending on your risk appetite and the threat landscape for your organisation, one option may be to focus on preventing less mature attackers and detecting and responding to more mature attackers (see figure).

Based on this preliminary cyber threat assessment, the next step is to determine the scope of cyber security for your organisation and the underlying security capability model. The prevalence and sophistication of recent cyber-attacks on public and private organisations highlights a number of capabilities that are essential to becoming an effective cyber-resilient organisation:

- **Preparation:** prepare your organisation to effectively manage cyber risks by ensuring it has the right governance structures in place to enhance and maintain its preventative and detective security capabilities
- **Prevention:** defend your organisation against successful cyber-attacks by continuing to invest in enhancing and maintaining measures that protect your digital assets such as (i) next generation security controls (IDM, NAC, etc.), (ii) hardening of critical information infrastructure, (iii) secure services (secure SDLC, vulnerability and patch management, etc.) and (iv) secure workforce and cyber awareness
- **Detection:** leverage the wealth of threat intelligence and develop your own capabilities to ensure you are aware of the internal and external threats to your organisation and can pro-actively mitigate them
- **Response:** in anticipation of a cyber-attack, ensure you have the ability to rapidly respond to an incident in order to limit any adverse impact on your organisation

Figure 1



The five commandments for a successful cyber security strategy

In conclusion, five key principles should underpin cyber security and promote a cohesive approach to protection from cyber threats:

- **Understand your risk appetite:** only when you have fully understood your assets, the risks that threaten them and how these fit into the overall threat landscape can you determine what level of threat maturity you need to defend against and where you draw the line to focus on limiting the impact of a successful attack
- **Ensure close alignment with business goals:** ensure that your strategic direction for cyber security is in close alignment with business goals and the organisation's strategy for achieving these. Focus efforts on defending the most strategically important parts of the business, or those that carry most operational risk
- **Prepare for the worst:** it is not practical to prevent all forms of cyber-attack, especially those that are particularly sophisticated and targeted (advanced persistent threats or APTs). You should ensure you have the organisational and technical capability to rapidly detect and respond to a successful attack in order to limit its impact

Cyber resilience requires that organisations have the agility to prevent, detect and respond quickly and effectively, not just to incidents, but also to the consequences of the incidents

- **Share intelligence:** collaborate and share intelligence with industry and national and international cyber threat intelligence organisations. By sharing intelligence with other organisations you will be in a position to receive the benefit of shared wisdom
- **Instil a broad awareness of cyber security:** your security is only as strong as the weakest link. Ensure that the risks associated with cyber security and the steps your organisation is taking to combat these risks are understood across the organisation, from the board and senior management, to all staff, partners and third parties