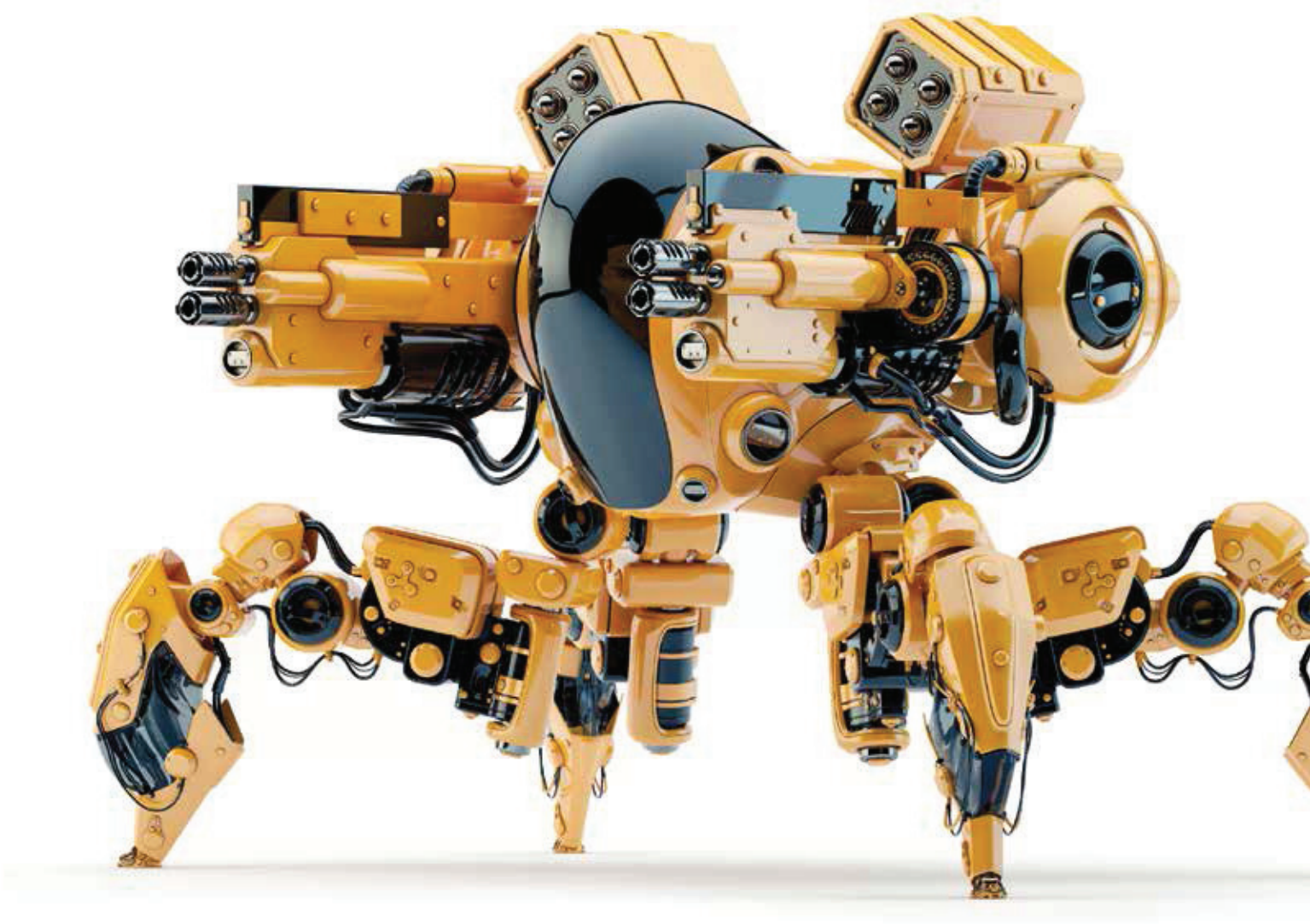
Global Cyber Executive Briefing

Lessons from the front line

Stéphane Hurtaud
Partner
Governance, Risk & Compliance
Deloitte Luxembourg

In a world increasingly driven by digital technologies and information, cyber-threat management is more than just a strategic imperative. It's a fundamental part of doing business. Yet for many senior executives and board members, the concept of cybersecurity remains vague and complex.



Yet for many senior executives and board members, the concept of cybersecurity remains vague and complex. Although it might be on your strategic agenda, what does it really mean? And what can your organisation do to shore up its defences and protect itself from cyber-threats?

No industry or organisation is immune

A common myth is that cyber-attacks only happen to certain types of organisations, such as high-profile technology businesses. However, the cold, hard truth is that every organisation has valuable data to lose. In fact, the attacks that happen most frequently are completely indiscriminate - using scripted, automated tools that identify and exploit whatever weaknesses they happen to find. Cyber-attacks can be extremely harmful. Tangible costs range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for injured parties. However, what might hurt even more are the intangible costs - such as loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, loss of integrity due to compromised digital assets, and overall damage to an organisation's reputation and brand - all of which can send an organisation's share price plummeting, and in extreme cases can even drive a company out of business.

What is the potential impact to your business?

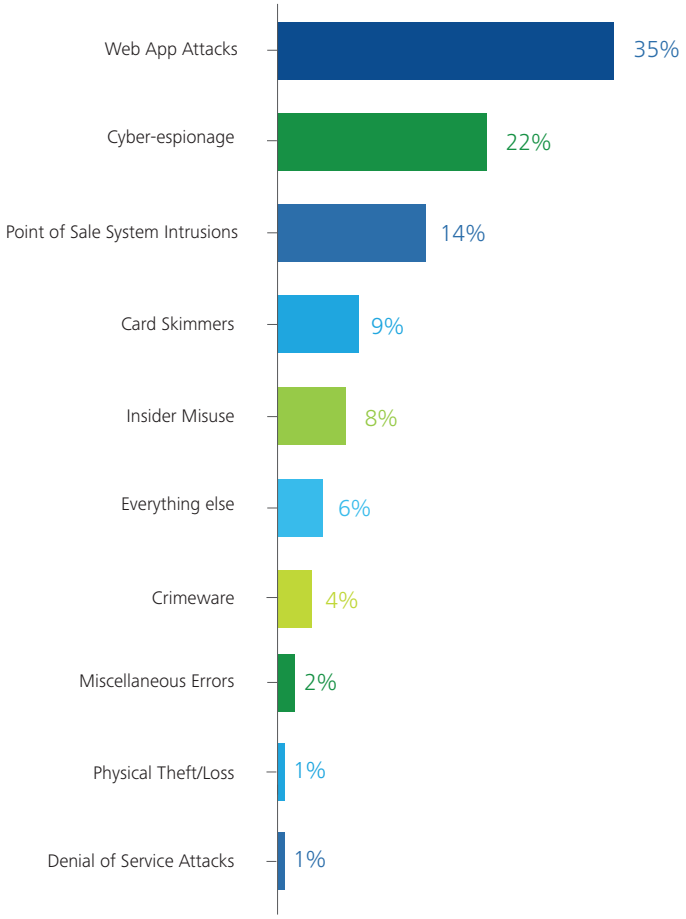
Being resilient to cyber-risks starts with awareness at the board and executive level; recognition that at some point your organisation will be attacked. You need to understand the biggest threats, and which assets are at greatest risk - the assets at the heart of your organisation's mission.

Who could potentially target your organisation, and for what reasons? Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack (see *Figure 1*), and what is the potential impact to your business?

Questions such as these can help determine how advanced and persistent the cyber-threats to your business are likely to be. This insight allows you, as a senior executive or board member, to determine your organisation's risk appetite and provide guidance that helps internal and external security professionals reduce your risk exposure to an acceptable level through a well-balanced cyber defence.

Who could potentially target your organisation, and for what reasons?

Figure 1: Frequency of incident classification patterns from 1367 breaches during 2013.



Source: Verizon 2014 Data Breach Investigations Report[1]

1 *www.verizonenterprise.com/DBIR/2014/*

The importance to understand the key cyber-threats for your industry sector

The Deloitte's 'Global Cyber Executive Briefing' report[2] is a starting point for organisations to understand their most important cyber-threats. It highlights the top threats for seven key industry sectors - retail, manufacturing, e-commerce & online payments, online media, high technology, telecommunications, and insurance - and offers real-world stories and practical insights to help your organisation begin to assess its threat profile and stay a step ahead of cyber-criminals. Follow-on reports will highlight the top cyber-threats in other major sectors that are also highly vulnerable.

For those key industry sectors, the main highlights of the report include:

High Tech

The high-tech sector is often ground zero for cyber-attacks because (i) it has very valuable information to be stolen and (ii) the nature of high-tech organisations themselves. High-tech companies - and their employees - generally have a higher risk appetite than their counterparts in other sectors. Also, they tend to be early adopters of new technologies that are still maturing and are therefore especially vulnerable to attacks and exploits. In addition, many high-tech organisations have open environments and corporate cultures that are designed to stimulate creativity and collaboration, but are more difficult to defend. As a result, high-tech organisations typically have a very large attack surface to protect.

Online Media

The online media sector might have the greatest exposure to cyber-threats. Since its organisations operate online, they have a huge attack surface to protect. Also, since its products are in high demand and completely digital, there is a high risk of being infiltrated and robbed of valuable content - both by individuals and organised crime groups.

Telecommunications

Facing increased, sophisticated attacks, including by Government agencies using Advanced Persistent Threats (APT) to establish covert surveillance for long periods of time. Another critical threat unique to the telecommunications sector is the attack on leased infrastructure equipment, such as home routers from Internet Service Providers (ISPs).

E-Commerce & Online payments

Database breach (i.e. loss of customer data, including names, physical addresses, phone numbers) and online payment systems are vulnerable areas often attacked. Denial of service attacks also top the list, particularly by hacktivists who want to disrupt an organisation in a highly visible way.

Insurance

The sector typically has a lot of sensitive data to protect. Cyber-attacks are growing exponentially as insurance companies migrate toward digital channels with sophisticated attacks combing advanced malware with other techniques such as social engineering. While current attacks appear short-term, the report predicts the number of long-term attacks may be silently growing.

Manufacturing

Increasing in the amount of attacks by hackers and cyber-criminals as well as through corporate espionage. Types of cyber-attacks in manufacturing vary widely from phishing to advanced malware, targeting not only IT but also connected Industrial Control Systems.

Retail

Credit card data is the new currency for hackers and criminals. Insider threats in retail are increasing, giving rise to a new breed of criminals that focus on stealing information - especially the valuable cardholder data that flows between consumers and retailers.

2 *Full report available on: www2.deloitte.com/content/www/global/en/pages/risk/articles/Global-Cyber-Briefing.html*

Breaches occur at all organisations - not because they are badly managed, but because hackers and cyber-criminals are getting smarter every day. By sharing information about breaches, we can learn how to better protect ourselves - an imperative being promoted by the Partnering for Cyber-Resilience[3] initiative of the World Economic Forum.

The stories clearly show that breaches are inevitable: your organisation will be hacked someday. They also show that we all depend on each other for a resilient cyber-space. For example, online media can be used to spread malware; vulnerabilities in the high-tech sector affect other industries that use digital technology; and disruption in online payments impact e-commerce.

By sharing and understanding these cases and taking responsibility at the executive and board level, we can all work together towards a safer cyber-space.

Need for an effective and well balanced cyber-defence

The bad news, and as explained earlier in this article, is that cyber-attacks can result in significant tangible and intangible costs. The good news is that cyber-threats are a manageable problem. To be effective and well balanced, a cyber-defence must have three key characteristics: it must be secure, vigilant, and resilient:

- **Secure:** Being secure means focusing protection around the risk sensitive assets at the heart of your organisation's mission - the ones that both you and your adversaries are likely to agree are the most valuable.
- **Vigilant:** Being vigilant means establishing threat awareness throughout the organisation, and developing the capacity to detect patterns of behaviour that may indicate, or even predict, compromise of critical assets.
- **Resilient:** Being resilient means having the capacity to rapidly contain the damage, and mobilise the diverse resources needed to minimise impact - including direct costs and business disruption, as well as reputation and brand damage.

Although it is not possible for any organisation to be 100% secure, by focusing on these three key attributes, it is entirely possible to manage and mitigate cyber threats in a way that reduces their impact and minimises the potential for business disruption.

3 www.weforum.org/issues/partnering-cyber-resilience-pcr

To summarise, here are five takeaway questions to reflect on through the lens of a secure, vigilant, and resilient approach to cyber security:

1 **Are we focused on the right things?**
Often asked, but difficult to accomplish. Understand how value is created in your organisation, where your critical assets are, how they are vulnerable to key threats. Practice defence in depth.

2 **Do we have the right talent?**
Quality over quantity. There may not be enough talent to do everything in-house, so take a strategic approach to sourcing decisions. Are the security teams focused on the real business areas?

3 **Are we proactive or reactive?**
Retrofitting for security is very expensive. Build it upfront in your management processes, applications, and infrastructure.

4 **Are we incentivising openness and collaboration?**
Build strong relationships with partners, law enforcement, regulators, and vendors. Foster internal co-operation across groups and functions, and ensure that people are not hiding risks to protect themselves.

5 **Are we adapting to change?**
Policy reviews, assessments, and rehearsals of crisis response processes should be regularised to establish a culture of perpetual adaptation to the threat and risk landscape.

Which assets are attackers likely to view as most valuable? What are the possible scenarios for attack?