Cyber security experts are keen on using military analogies and terminology. It is easy to see why: Cyber security increasingly resembles an arms race in which cyber threat actors are constantly developing new tactics, techniques and procedures, and businesses are forced to counter these new threats. However, leading enterprises are not content to be merely reactive. They are trying to stay one step ahead of their adversaries, by understanding and anticipating future attacks, and actively defending themselves.

This article examines the changing cyber threat environment and the factors that are driving its evolution. We further analyze how leading organizations are responding to these new challenges and what this means for you.

The evolving threat environment

Not a week passes without headlines describing a major cyber-attack or some new strain of malware or insidious social engineering technique being used to attack businesses. Amongst this constant flux and change, it is possible to discern certain trends which can help us to make sense of what we are seeing:

Cyber threats are proliferating, facilitated by the Dark Web

Barriers to entry for would-be cyber criminals are falling rapidly, as malware and malware-as-a-service become more easily and cheaply available through the Dark Web. This is a major factor to the current epidemic of ransomware.

Ransomware is malware which restricts access to the infected computer system, usually by encrypting files on a hard drive in order for the criminals responsible to extort a ransom for restoring access. Criminal vendors put ransomware campaigns within easy reach by offering ransomware-as-a-service packages on the Dark Web, often on a commission payment basis.

These packages may include rental of the malware, server capacity through which to launch the campaign, and even an administrative interface through which to monitor and control it.

The Dark Web also provides a market place for stolen financial and personally identifiable information (PII), from bank and credit card credentials to personal health information. This has two mutually-reinforcing effects. Stolen data is used for further cyber-crimes, including identity theft and sophisticated social engineering campaigns. For example, spear phishing emails can be made to appear more credible to their recipients if they include stolen PII or personal health information. In turn, demand is created for yet more stolen data. This means that even organizations which do not hold financial assets cannot afford to be complacent as client, employee or corporate data are also targets for cyber criminals.
Unsophisticated attackers (script kiddies)

You are attacked because you have a vulnerability on the internet and have information of value.

Sophisticated attackers (hackers)

You are attacked because you are on the internet and have information of value.

Corporate espionage (malicious insiders)

Your current or former employee seeks financial gain from stealing something of value that can be sold.

Organized crime (criminal gangs)

You are attacked because you have money or something else of value that can be sold.

State sponsored attacks: Advanced Persistent Threat (APT)

You are targeted because of who you are, what you do, or the value of your intellectual property.

Source: EY, 2016

Cyber criminals are becoming increasingly sophisticated.

Two recent examples demonstrate how cyber threats are evolving:

The cyber theft of US$81 million from the Bank of Bangladesh in February 2016 was not only for its scale and audacity; the criminals also demonstrated highly-developed “Tradeoff” skills. They hid their tracks and delayed detection by deploying customized malware, which diverted transactions from the SWIFT database, altered transaction records, and manipulated confirmation messages that would normally be printed on paper.

The rapid development of banking malware demonstrates sophisticated cybercriminals’ ability to learn and adapt. The Android/Spy.Agent.SI mobile malware, discovered in early 2016 in Australia, masqueraded as a Flash Player upgrade. In fact it was a banking Trojan which overlaid fake sites over the websites of several major banks, enabling the theft of banking credentials. The Trojan also attempted to overcome the banks’ two-factor authentication procedures by intercepting and redirecting SMS text messages intended for customers.

We anticipate that technological innovation in the financial services industry will continue to drive criminal ingenuity. For example, smart phones have a number of known vulnerabilities for which, until now, cyber criminals have not had a financial incentive to exploit. Innovations such as banks’ introduction of payment through mobile phones will create motivation for cyber criminals to take advantage of these known vulnerabilities, as well as to find and exploit other weaknesses.

Such attacks may involve protracted reconnaissance and, having gained an initial foothold, maintaining a presence for several months on the target’s systems, conducting reconnaissance, before exfiltrating stolen data.

Greater connectivity increases an organisation’s number of points of potential vulnerability, collectively known as its “attack surface.” New business models, driven by an increasingly mobile workforce, greater digitization and connectivity with customers and the supply chain, mean that enterprises’ attack surfaces are rapidly expanding.

And this will only accelerate as we enter the era of the Internet of Things, with industry experts estimating that there will be anywhere up to 75 billion connected devices by 2020, from smart white goods to connected vehicles.

The cyber theft of US$81 million from the Bank of Bangladesh in February 2016 was not only for its scale and audacity; the criminals also demonstrated highly-developed “Tradeoff” skills. They hid their tracks and delayed detection by deploying customized malware, which diverted transactions from the SWIFT database, altered transaction records, and manipulated confirmation messages that would normally be printed on paper.

The rapid development of banking malware demonstrates sophisticated cybercriminals’ ability to learn and adapt. The Android/Spy.Agent.SI mobile malware, discovered in early 2016 in Australia, masqueraded as a Flash Player upgrade. In fact it was a banking Trojan which overlaid fake sites over the websites of several major banks, enabling the theft of banking credentials. The Trojan also attempted to overcome the banks’ two-factor authentication procedures by intercepting and redirecting SMS text messages intended for customers.

We anticipate that technological innovation in the financial services industry will continue to drive criminal ingenuity. For example, smart phones have a number of known vulnerabilities for which, until now, cyber criminals have not had a financial incentive to exploit. Innovations such as banks’ introduction of payment through mobile phones will create motivation for cyber criminals to take advantage of these known vulnerabilities, as well as to find and exploit other weaknesses.

Such attacks may involve protracted reconnaissance and, having gained an initial foothold, maintaining a presence for several months on the target’s systems, conducting reconnaissance, before exfiltrating stolen data.

Greater connectivity increases an organisation’s number of points of potential vulnerability, collectively known as its “attack surface.” New business models, driven by an increasingly mobile workforce, greater digitization and connectivity with customers and the supply chain, mean that enterprises’ attack surfaces are rapidly expanding.

And this will only accelerate as we enter the era of the Internet of Things, with industry experts estimating that there will be anywhere up to 75 billion connected devices by 2020, from smart white goods to connected vehicles.

Proliferating adversaries, increasingly sophisticated threats and an expanding attack surface: how can any organization, let alone a financial institution entrusted with billions of dollars in customers’ funds and personal data, stay ahead? Cyber-attacks are integral to the greater connectivity demanded by new business models. But this is not a counsel of despair: leading organizations are responding actively and with agility.

Attacks launched through connected “things,” many of which are poorly protected, are already here. In June 2016 the website of a jewellery store was hit by a Distributed Denial of Service (DDoS) attack, whereby adversaries attempted to crash the website through flooding it with traffic from a number of zombie devices under their control (a “botnet”). Interestingly, closer inspection revealed that the botnet was not composed of computers, but rather more than 25,000 internet-enabled CCTV cameras spread across over 100 countries.

Counts military campaigns have demonstrated that timely, actionable intelligence can make a decisive difference, often acting as a force-multipier against numerically superior forces. Similarly, leading organizations use threat intelligence to inform and enhance their cyber defences and strategic decision-making.

Leading organizations leverage cyber threat intelligence and other security competencies to build countermeasures, hunt hidden intruders and bolster defences. Active defence missions focus on the most likely attackers and are conducted with operational discipline (plan, execute, review). These may include:

Targeted countermeasures:
Countermeasures are planned and deployed against the key threat scenarios identified through threat modelling.

Hunting:
Intelligence-led, focused investigation for malicious activity by adversaries on the organization’s network and endpoints, that cannot be detected by automated security tools.

Trapping and coercion:
Network and endpoint conditions are altered to provoke a hidden adversary into engaging in malicious activity that is likely to be detected by targeted monitoring.

Deception:
Deception technologies create fake systems and vulnerabilities to attract an adversary and stall and disrupt the progress of the attack. These missions are enabled by intelligence, which informs the location and type of deceits that are most likely to succeed against the attacker.
Cyber security is a type of asymmetric warfare: each organization faces a multitude of cyber adversaries, and their ranks are growing and becoming more sophisticated. The new reality is that you cannot prevent all cyber-attacks: a sufficiently capable and motivated attacker will get through. Leading enterprises are meeting this challenge by using cyber threat intelligence as a force multiplier, ensuring that their leadership teams are fully engaged, and using active defense to detect and respond to emerging threats. The cyber threat landscape is evolving – and so must your cyber security strategy.

This article was originally written by EY for the 2016 Thomson Reuters ASEAN Regulatory Summit.

The following are some suggestions for how the Board and C-suite can become more deeply engaged with cyber security:

**Intelligence briefings**

The Board and C-suite should demand regular briefings from their information security team on such matters as emerging threats which have affected comparable businesses, the changing regulatory landscape, or reporting on attacks against key third parties or M&A targets.

**Drills/war-games**

Regular tabletop simulations of credible cyber-attack scenarios are a relatively small financial and time investment. However, they can pay significant dividends in helping the Board and C-suite develop the skills and “muscle memory” required to lead the response to, and recovery from, a serious cyber incident. Simulations often expose the need to update crisis management, business continuity and communications plans, or to create new, cyber-specific plans and policies.

**Information security performance reporting**

Performance reporting is very often a series of dry metrics, with little business context or meaning for the Board and C-suite. An intelligence-led approach can deepen engagement by explaining how security operations have prevented specific adversary campaigns and how this has benefitted the business by preventing theft of data or disruption to IT services.
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organisation, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organisation, please visit ey.com.

© 2016 Ernst & Young, Australia.
All Rights Reserved.
EYG 02022-164GBL
PH1629725

This communication provides general information which is current at the time of production. The information contained in this communication does not constitute advice and should not be relied on as such. Professional advice should be sought prior to any action being taken in reliance on any of the information. Ernst & Young disclaims all responsibility and liability (including, without limitation, for any direct or indirect or consequential costs, loss or damage or loss of profits) arising from anything done or omitted to be done by any party in reliance, whether wholly or partially, on any of the information. Any party that relies on the information does so at its own risk. Liability limited by a scheme approved under Professional Standards Legislation.

ey.com