Cybersecurity – starting with the basics

Ricky Liu explains six areas to consider for an effective cybersecurity programme

The rapid digital transformation in the Asia-Pacific region has been encouraging businesses to bring more of their services onto digital platforms. However, this hyper-connected ecosystem of businesses, service providers and consumers also creates a larger surface for cyber criminals to attack. Each entity, device and application within the ecosystem will have vulnerabilities and can potentially be an entry point for cybercriminals.

The cybersecurity ecosystem will continue to expand as business and technology evolve. For most organizations, there are hundreds of vulnerabilities that have to be protected, but a cyber attacker would only need to successfully exploit one to potentially compromise a system. To navigate through the complex and ever changing world of cybersecurity, organizations need to take a holistic approach to manage cybersecurity risks.

To successfully develop and maintain an effective cybersecurity programme, we propose six main areas for consideration.

Business alignment

The primary goal of information security is to enable your organization to meet its strategic objectives. Policies and controls need to be meaningful. Enterprises need to align themselves with these goals by understanding the enterprise's risk appetite, its core assets (including functions, processes, intangible and tangible assets) and the risks that these assets are exposed to.

A holistic approach must be taken when identifying risks: consider all connections, vendors, suppliers, outsourcing partners and other business partners. Attackers often use these external entities as indirect entry points in order to reach their intended target. In 2014, the United State's second-largest discount retailer, Target, was hacked. The attacker stole network credentials from a third party (a heating, ventilation and air conditioning provider) before gaining access to Target's system.

A system can never be risk-free and organizations do not have a blank cheque for cybersecurity costs. As such, a cybersecurity programme is about making businesses less of an easy target by prioritizing risks and putting safeguards and counter-measures in place within resource limits. The total cost of control should be less than the value of the asset it is trying to protect; highest to lowest levels of critical importance should be established, based on risk exposure against asset value, in order to avoid spending thousands of dollars on fixing a US$100 problem.

Resource

Cybersecurity is no longer just an IT issue, but a business risk. Effective cybersecurity requires ownership, accountability and skilled leaders at a senior level to drive the message out to the entire organization. Knowledgeable professionals are required to implement and maintain the programme. As the current shortage of cyber-experts continues, organizations need to identify the skill gap and commit to either developing the necessary skills internally or finding the right resources externally through third-party services.

Numerous global surveys have shown that most businesses leaders recognize the importance of cybersecurity. However, many are still reluctant to improve their security postures because they believe the costs are prohibitive. While cybersecurity will inevitably require investment, the benefits will far outweigh the potential damages. Not all risks are created equal, so prioritizing assets and risks plays an essential role in reducing unnecessary costs.

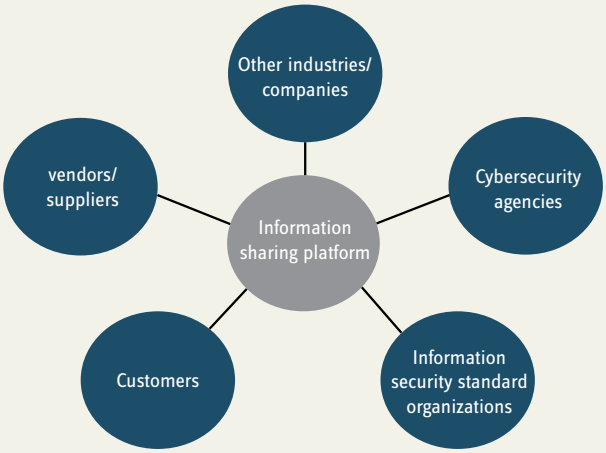
Fortification

When defining controls, there is no one-size-fits-all solution. Each industry and enterprise has a unique risk profile. The decision about which controls are required needs to be driven by business goals and a balance must be found between integrity, confidentiality and availability of data and systems.

Get the basics right first: start by focusing on a subset of critical controls that can be implemented, enforced and monitored in an automated fashion with the highest payoff.

For instance, details of new vulnerabilities appear in the public domain very quickly after discovery: exploit databases, such as Exploit-Database (hosted by Offensive Security) has nearly 37,000 entries. This information is available to anyone, including attackers. Fortunately, vendors frequently release fixes. To avoid a whole range of known vulnerabilities, enterprises simply need to stay "patched." The challenge comes when there are hundreds of devices and applications to keep track of, and this is when an automated patch-management system becomes useful.

Recognized information-security frameworks (such as the COBIT 5 ISO27000 series and NIST's SP 800 series) can be used as a blueprint to assist in defining the controls required and building security programmes in a structured and systematic way.



Developing a cybersecurity strategy is not a one-off effort; it needs to evolve within the ecosystem in which it exists.

An inherent risk assessment will help your enterprise understand its risk profile and expected maturity level for each area assessed. The result can be compared with an actual maturity assessment in order to identify any gaps in maturity levels. Any gaps identified should be used as a base to create a roadmap to the desired maturity levels.

Intelligence

Businesses are often reluctant to share information about security incidents, due to concerns about reputation damage, attacker retribution and legal ramifications. This thinking has to change because in the realm of security, organizations are always one or two steps behind the criminals.

Symantec's *2016 Internet Security Threat Report* identified that one new zero-day vulnerability was found every week in 2015, and more than 430 million new unique pieces of malware were discovered in the same year.

As cybercriminals become more collaborative, so should legitimate enterprises. Better information-sharing platforms will reduce the window of opportunity for attackers to re-use successful methods of attack on other victims: promoting innovation is a cyber-defence (see diagram above).

Preparedness

Achieving 100 percent security is impractical, as a determined and skilled hacker will eventually compromise a system to a certain extent. By the time a breach happens it is already too late – the cost is far more than that of being prepared in the first place. Organizations need tried-and-tested plans to detect, respond to and recover from security incidents. The consideration is not just a technical one. It also involves business continuity, reputation management, and legal and regulatory management.

In 2015, TalkTalk, a telecommunications provider based in the United Kingdom, suffered a significant and sustained cyberattack, during which the personal and banking details of up to four million customers were thought to have been accessed. The attacker exploited SQL injection vulnerability, a technique that had been well known for over two decades and for which fixes were available.

TalkTalk was fined £400,000 by the U.K. Information Commissioner's Office. However, the financial damage extended well beyond that: with the loss of 101,000 customers and a drop in its share price and revenue, TalkTalk's "exceptional costs" totalled over US$50 million as the company dealt with website restoration in addition to the public affairs and legal costs.

When devising these essential plans, organizations must not limit their thinking to within their boundaries. External relationships must be considered too. For instance, what if a third-party service provider is hacked and sensitive information is stolen, or their ability to provide services is disrupted? How will your organization deal with that?

Testing and training

No plan or control is going to survive the constantly changing landscape of cybersecurity. Every part of the security programme needs to be periodically tested, continuously monitored and frequently updated.

Employees are always going to be the weakest link in the security chain, simply because human and system interactions are inevitable and we cannot control human behaviour as far as we can automate systems and controls.

In the *2016 Cyber Security Intelligence Index*, IBM found that 60 percent of all attacks were carried out by insiders. Of these attacks, three-quarters involved malicious intent, and one-quarter involved inadvertent actors.

However, with appropriate human resources procedures, continuous awareness and technical training, users can also become a great preventive and detective mechanism, especially against social engineering attacks, and help spot unusual internal and external user activity.

Ricky Liu is Senior Manager of Risk Advisory at BDO.