Cyber attacks

Moving beyond prevention

Hugh Callaghan, Director, IT Risk and Assurance Services, EY
The reality is quite stark. Organisations must face the fact that cyber attacks are inevitable and that prevention measures alone are insufficient to protect the business. Companies will have to learn how to recognise the often-subtle signs of an attack as well as responding effectively and swiftly to limit the damage that security breaches could cause their businesses.

Although cyber security issues originate in technology, the consequences of an attack affect the entire business, by triggering potential breaches of regulatory compliance; operational disruption; direct financial loss; brand damage; and loss of investor confidence.

It is difficult to defend against cyber attacks, because they come in many guises. It could be an attack on the company web site, to disrupt digital customer channels. It could be the loss of critical files to ‘ransomware’, malicious software that deliberately locks up company data until the victim pays for the key. It could be silent infiltration of your most sensitive systems to steal intellectual property or strategic corporate information. Attacks could even cause expensive product recalls by disrupting a finely-tuned manufacturing process, industrial control or environmental system.

Many companies are sceptical of such threats, doubting their inevitability and questioning whether they would in fact be targeted by cyber villains. Others wonder whether the construction and maintenance of secure IT systems could really be such a complex task. Unfortunately such scepticism is misplaced.

Firstly, simple human error favours the attacker. The defenders of IT systems have to cover every possible angle of attack, whereas an adversary only has to find one way in through a missing patch or misplaced security setting.

Secondly, even if all of the known weaknesses are addressed, new software issues are constantly emerging and keeping up with these is an endless task. Cyber criminals also invest significant resources in finding new, undisclosed weaknesses which are then used to covertly break into systems (think of these as a skeleton key to your systems).

Finally, a combination of digital complexity and mass interconnectedness mean that interactions between users and technology often produce unexpected risks. For example, your Internet boundary can be well defined and protected, but mobile devices, email, web and social media applications cross that boundary regularly and each can provide an avenue of attack for cyber criminals.

It's also not enough to implement even the best of prevention measures and to assume that they won't fail. Security product and service vendors have themselves acknowledged this reality. Recently, a senior vice president of Symantec admitted to the Wall Street Journal that modern anti-virus software stops less than half of computer system attacks. He was further quoted as saying anti-virus software was ‘dead.’ Accordingly, the security industry would reconfigure to move away from anti-virus products as its main revenue stream. Recognising that breaches are inevitable, it will instead move into services to help businesses track and recover from intrusions, as well as provide advice on how to protect data.

In such a scenario, how should organisations protect themselves? Basic preventative measures – such as anti-virus; firewalls; web and e-mail content filtering; and a robust software update process – need to stay in place.

Beyond this, organisations need the ability to detect and respond to inevitable incidents. Companies need monitoring systems that function like burglar alarms, to help their business to spot the signs of intrusions. They need to assess their controls through regular penetration testing. Suspected intrusions need to be investigated quickly and companies need to prepare for intrusions by organising simulation exercises and cyber ‘war games’ exercises.

European companies can now also consider availing of insurance against cyber attack, an option which has been available in the US for a number of years. It may be possible to insure against adverse events including direct costs arising from cyber attacks; associated business disruption; the investigation of a data breach; regulatory fines; brand damage; and even the physical damage caused by a cyber attack. The market is still maturing but this is one of the few ways of reducing the impact of a cyber attack rather than just the likelihood of occurrence.