ITSecurityExpert.co.uk
Get Secure, Be Secure & Stay Secure

For Caught in the Crossfire of Cyberwarfare

Dr Sandra Bell, Head of Resilience Consulting EMEA, Sungard Availability Services

The 2019 National Cyber Security Centre's (NCSC) Annual Review does not shy away from naming the four key protagonists when it comes to state-based cyber threats against our country. The review sites China, Russia, North Korea and Iran as being actively engaged in cyber operations against our Critical National Infrastructure and other sectors of society. That being said, the main cyber threat to businesses and individual citizens remains organised crime. But with the capability of organised crime matching some state-based activity and the sharing (if not direct support) of state-based techniques with cyber criminals, how are we expected to defend ourselves against such sophisticated cyberattack means?

The answer offered by Ciaran Martin, CEO of the NCSC, in his Forward to the 2019 Review only scratches the surface of the cultural change we need to embrace if we are to become truly cyber resilient to these modern-day threats.

"Looking ahead, there is also the risk that advanced cyberattack techniques could find their way into the hands of new actors, through proliferation of such tools on the open market. Additionally, we must always be mindful of the risk of accidental impact from other attacks. Cyber security has moved away from the exclusive prevail of security and intelligence agencies towards one that needs the involvement of all of government, and indeed all of society."

There are a few key points to draw out from this statement. Firstly, there is an acceptance that all of us may be collateral damage in a broader state-on-state cyberattack. Secondly, we should accept also that we maybe the victims of very sophisticated cyberattacks that have their roots in state sponsored development. And finally, we must all accept that cyber security is a collective responsibility and, where businesses are concerned, this responsibility must be accepted and owned at the very top.

Modern life is now dependent on cyber security but we are yet to truly embrace the concept of a cyber secure culture. When we perceived terrorism as the major threat to our security, society quickly adopted a 'reporting culture' of anything suspicious, but have we seen the same mindset shift with regards to cyber threats? The man in the street may not be the intended target of a state-based or organised crime cyberattack but we can all easily become a victim, either accidentally as collateral damage or intentionally as low-hanging fruit. Either way we can all, individual citizens and businesses alike, fall victim to the new battleground of cyberwarfare.

What can business do in the face of such threats?

One could argue that becoming a victim of cybercrime is a when not an if. This can in turn bring about a sense of the inevitability. But what is clear when you see the magnitude of recent Information Commissioner's Office (ICO) fines, is that businesses cannot ignore cyber security issues. A business that embraces the idea of a cyber security culture within its organisation will not only be less likely to be hit with a fine from the ICO should things go horribly wrong, but are also less likely to fall victim in the first place. Cyber security is about doing the basics well and preparing your organisation to protect itself, and responding correctly when an incident occurs.

Protecting against a new kind of warfare

Organisations need to prepare to potentially become the unintended targets of broad-brush cyberattacks, protecting themselves against the impact they could have on their operations and customer services. With each attack growing in its complexity, businesses must in-tow respond in a swift and sophisticated manner. Defence mechanisms need to be as scalable as the nefarious incidents they may be up against. To give themselves the best chance of ensuring that an attack doesn't debilitate them and the country in which they operate, there are a few key things that businesses can do:

1) Act swiftly

A cyberattack requires an immediate response from every part of a business. Therefore, when faced with a potential breach, every individual must know how to react precisely and quickly. IT and business teams will need to locate and close any vulnerabilities in IT systems or business processes and switch over to Disaster Recovery arrangements if they believe there has been a data corruption. Business units need to invoke their Business Continuity Plans and the executive Crisis Management Team needs to assemble. This team needs to be rehearsed in cyber related crisis events and not just the more traditional Business Continuity type of crisis.

Both the speed and effectiveness of a response will be greatly improved if businesses have at their fingertips the results of a Data Protection Impact Assessment (DPIA) that details all the personal data collected, processed and stored, categorised by level of sensitivity. If companies are scrambling around, unsure of who should be taking charge and what exactly should be done, then the damage caused by the data encryption will only be intensified.

2) Isolate the threat

Value flows from business to business through networks and supply chains, but so do malware infections. Having adequate back-up resources not only brings back business availability in the wake of an attack, but it also serves to act as a barrier to further disruption in the network. The key element that cybercriminals and hacking groups have worked to iterate on is their delivery vector.

Phishing attempts are more effective if they're designed using the techniques employed in social engineering. A study conducted by IBM found that human error accounts for more than 95 per cent of security incidents. The majority of the most devastating attacks from recent years have been of the network-based variety, i.e. worms and bots.

Right now, we live in a highly connected world with hyper-extended networks comprised of a multitude of mobile devices and remote workers logging in from international locations. Having a crisis communication plan that sets out in advance who needs to be contacted should a breach occur will mean that important stakeholders based in different locations don't get forgotten in the heat of the moment.

3) Rely on resilience

Prevention is always better than cure. Rather than waiting until a data breach occurs to discover the hard way which threats and vulnerabilities are present in IT systems and business processes, act now.

It's good business practice to continuously monitor risk, including information risk, and ensure that the controls are adequate. However, in the fast-paced cyber world where the threats are constantly changing this can be difficult in practice.

With effective Disaster Recovery and cyber focused Business Continuity practices written into business contingency planning, organisations remain robust and ready to spring into action to minimise the impact of a data breach.

The most effective way to test business resilience without unconscious bias risking false-positive results is via evaluation by external security professionals. By conducting physical and logical penetration testing and regularly checking an organisation's susceptibility to social engineering, effective business continuity can be ensured, and back-up solutions can be rigorously tested.

Cyber Resilience must be woven into the fabric of business operations, including corporate culture itself. Crisis leadership training ensures the C-suite has the skills, competencies and psychological coping strategies that help lead an organisation through the complex, uncertain and unstable environment that is caused by a cyberattack, emerging the other side stronger and more competitive than ever before.

A look ahead to the future

A cyberattack is never insignificant, nor expected, but if a business suffers one it is important to inform those that are affected as quickly as possible. Given the scale at which these are being launched, this couldn't be truer. It's vital in the current age of state-backed attacks that businesses prioritise resilience lest they be caught in the crossfire. In a business landscape defined by hyper-extended supply chains, having a crisis communication plan that sets out in advance who needs to be contacted should a breach occur will mean that important stakeholders don't get forgotten in the heat of the moment and that the most important assets remain protected.