nccgroup

Shutterstock: Dean Drobot

Oct 21, 2019 23:30 BST

Disperse the fear, uncertainty and doubt and take charge of your cyber risk

Is the cyber security threat landscape based on fact or fiction? It's just one question we posed to our own security experts Tim Anderson and Graham McElroy as we chatted to them to find out more about their thoughts on how organisations can reduce their cyber risk.

"There's been a lot of fear, uncertainty and doubt (or FUD as it is known) around cyber security for a number of years, from poor marketing and sales to a largely uneducated market place," says Tim who heads up our global Managed Detection and Response (MDR) practice. "And while the market has

matured somewhat over the past seven to 10 years, this quackery has sadly continued and can still dupe the innocent business."

"Yes, I agree," says Graham, Managed Security Services technical director. "And to answer your question – the cyber security threat landscape is based on fact by reputable cyber security firms. It is an industry term often used to describe the current types of attacks favoured by cyber criminals and other more serious attackers – like cyber espionage and nation state attacks."

"One of the issues though," adds Tim, "is the more evidence-based research pieces such as the Ponemon Study, and the Symantec Internet Threat Report can be unbelievable to medium sized businesses. For example the average cost of a breach according to the recent Ponemon Cost of a Data Breach Report is circa $3.92m – some medium sized companies don't turn over that amount so this can be interpreted as FUD"

"While the cost may not often be believed, the research and insights shared can help provide valuable insight into real-world incidents/breaches and how they occur," says Graham. "If appropriately acted on this information can help an organisation make the right choices to improve its security posture?"

Making it relevant to an individual business to deal with the risk appropriately is actually one of the biggest challenges when trying to protect against this threat landscape. Graham elaborates: "Understanding the potential threats and risks applicable to your industry or sector and the methods of attacks currently 'in the wild' through curated threat intelligence will better prepare you. Better preparation enables a more effective defence, which reduces the risk of an attack being successful."

This leads to the second biggest challenge, which is articulating that risk to the Board and budget controllers. Not being able to make threat intelligence relevant leads to the team being unable to quantify the full impact of a cyber-attack. Graham highlights that for many businesses having a team large enough to cope with potential demands on a 24x7 basis with the levels of skills and budgets they have is simply unrealistic. And ultimately they have a business to run first and foremost.

A broad team is important adds Tim but the bigger challenge facing organisations is keeping them: "Entry level Security Operations Centre (SOC) analysis work can be, in the long-term unchallenging and analysts quickly

become frustrated by this. We've actually addressed this as we use the SOC as a progression into more sophisticated security work and can continually attract new talent because of this."

As we've already touched on it – threat intelligence needs to be specific and actionable if it is to be valuable to an organisation. "Our threat intelligence comes from various sources – from our researchers, pen test findings, threat intelligence units, incident response engagements – but it's just information," says Tim.

In its simplest form – an organisation has intelligence to suggest an attack is coming from a particular IP address and exploits certain technical weaknesses which is passed to the client. The client has no idea what to do with it. And this is why you need to know what you are paying for stresses Graham: "You need someone that can take intelligence, turn it into actions and explain the risks. And you need to be assured you are supported in incident response, technical security consulting and be confident that there is a continued investment in skills, knowledge and services."

This all sounds great but where do you start. "Before you buy, start by understanding your risk, the likelihood (who, what and how) and then the impact (cost). With this information you can look at appropriate controls to mitigate," advises Tim.

"I think you have to see cyber security not as a single outcome but actually a longer-term series of improvements and capabilities, it's a journey not a destination– each of which improve your ability to either predict, prevent, detect, respond and recover from a specific incident or threat," adds Graham.

This means for some organisations it might be ensuring devices are patched and updated, for another it might be using threat intelligence to spot user names and passwords shared on the web which could be used to form an attack. And for others it could be identifying where there is a risk of compromise through either credentials being in the public domain through external breaches or inappropriate dev/ops activity 'leaking' credentials to GitHub.

When you are faced with cost challenges, what's the motivation to invest in cyber security? "Quite simply I see it as a duty of care – a responsibility to protect your stakeholders when engaging with your business. You just need

to look at the news to see that even the biggest companies with significant investment can experience a cyber-attack," says Tim.

Of course, with national cyber security being higher on the agenda for a lot of governments, the choice to invest isn't always there. Look at GDPR for example, which has forced organisations to take action and cost of non-compliance being quite significant in both financial and reputational terms.

As the threat landscape and technology becomes more sophisticated, techniques used in the past are not as robust as they were, evidenced by the fact the number of breaches are climbing not falling. So what's the answer?

"Quite simply get ahead of the threat actors," exclaims Tim. "Traditionally," adds Graham, "the focus was on keeping the enemy out of the protected environment by maintaining a strong 'barrier' around the perimeter, but it's no longer enough and a new approach is needed to deal with these threats."

"You can think of it as a castle," says Tim. "As the attacker builds taller ladders to scale the walls, we build the walls higher. How about if we left the castle and went into the forest and monitored the attacker cutting down the trees, watched the ladders being built, worked out how tall they were and took action before the attack? And in addition we could ask the Castle protectors to walk around inside looking for anything suspicious, interrogating and detaining when needed. This is essentially what an MDR service offers you."

So you get it, you need to be on the front foot to get ahead of the threat landscape and it's got to be relevant to your business/sector to be of value. But how do you know how much money to invest? "There are wide statements, like GDPR, which suggest the controls should be appropriate – but many organisations don't understand what appropriate means to them," says Tim.

"Often businesses haven't really considered how reliant they are on technology as it's so ubiquitous and embedded in most business operations. You need to look at both financial and reputational costs. How reliant are you on technology to operate and what is the impact to your supply chain and customers if you weren't able to work? Do you have back up to operate manually? It all comes down to the complexity of your business so there's no magic formula for that," agrees Graham.

In conclusion both Tim and Graham agree that cyber security isn't just about preventing an attack. It's about limiting the potential scope and damage of an attack, minimising the impact on the business and enabling the organisation to continue to operate or recover quickly. This is often described as making the organisation cyber resilient.

By accepting that an attacker may gain a foothold, the key is to have a service in place that isolates the attack so it can't cause damage and introduces alternative controls for you. "This capability enables even smaller organisations to have effective security protection that would not be affordable or achievable (skills, knowledge and experience) if they tried to deliver in-house," concludes Tim.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970

NCC Group - Financial Media Enquiries
Press Contact
Maitland AMO
Financial Results Media Enquiries
+44 (0)20 7379 5151

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750

Regional Press Office - Europe
Press Contact
foxit@mcspr.nl
+31 (0)23 562 8208