Feb 18, 2021 17:50 GMT

Spotlight on cyber security as a science

Ollie Whitehouse, global CTO at NCC Group

When you consider the history of cyber security – which stretches back to around 60 years – it's perhaps not surprising that it's not yet widely seen as a science. While it is ubiquitous in our everyday lives, today's cyber security practices remain at the same stage of maturity as medical practices were in the early Middle Ages.

In 2019, we explored an evidence-based approach to cyber resilience and

how a such approaches are emerging. Two years later, we're seeing further traction in the cyber security community – here, as part of our *Spotlight on...* series, we share some thoughts on what's needed to establish cyber security as a science.

Putting research into practice

As the capabilities and understanding of the global cyber security community expand – in line with the sophistication of techniques employed by threat actors – we will see a more evidence-based approach to cyber resilience. This more rigorous approach will be driven by various factors spanning governments, academia, insurers and the end-user buying community looking to understand return-on-investment.

In practice, this will mean a move away from solely vendor attestation as to solution efficacy. Instead, we will transition to a world where evidence is provided of efficacy in real-world operating conditions, against realistic threat scenarios and the associated costs, caveats and similar considerations.

For example, in the wake of the WannaCry and NotPetya attacks, many of our clients were concerned about the impact of such large-scale attacks. One CEO asked us what would happen if their company was hit by NotPetya – so our team sought to find out.

By launching a re-engineered and augmented NotPetya into their environment over the course of eight months and measuring the organisation's resilience and response capabilities, we were able to quantify the potential impact and show in the real-world what worked and what did not. Being able to accurately measure the effectiveness of different strategies

is crucial to the future evidence-based world.

What does the future hold?

With increasingly sophisticated environments, continuous integration pipelines and design experiments, the cyber security industry's ability to deliver evidence-based advice will only grow. Measurement is key, and with these tools and models of working in place, organisations will be able to understand which solutions are working well and make any improvements on a continuous basis.

When armed with this knowledge, businesses can not only increase their own resilience, but make better strategic decisions. A threat intelligence-informed approach – particularly when it's tailored to an individual organisation – ultimately empowers business leaders to understand their unique threat profile and make better decisions to remain secure amidst a changing threat landscape.

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