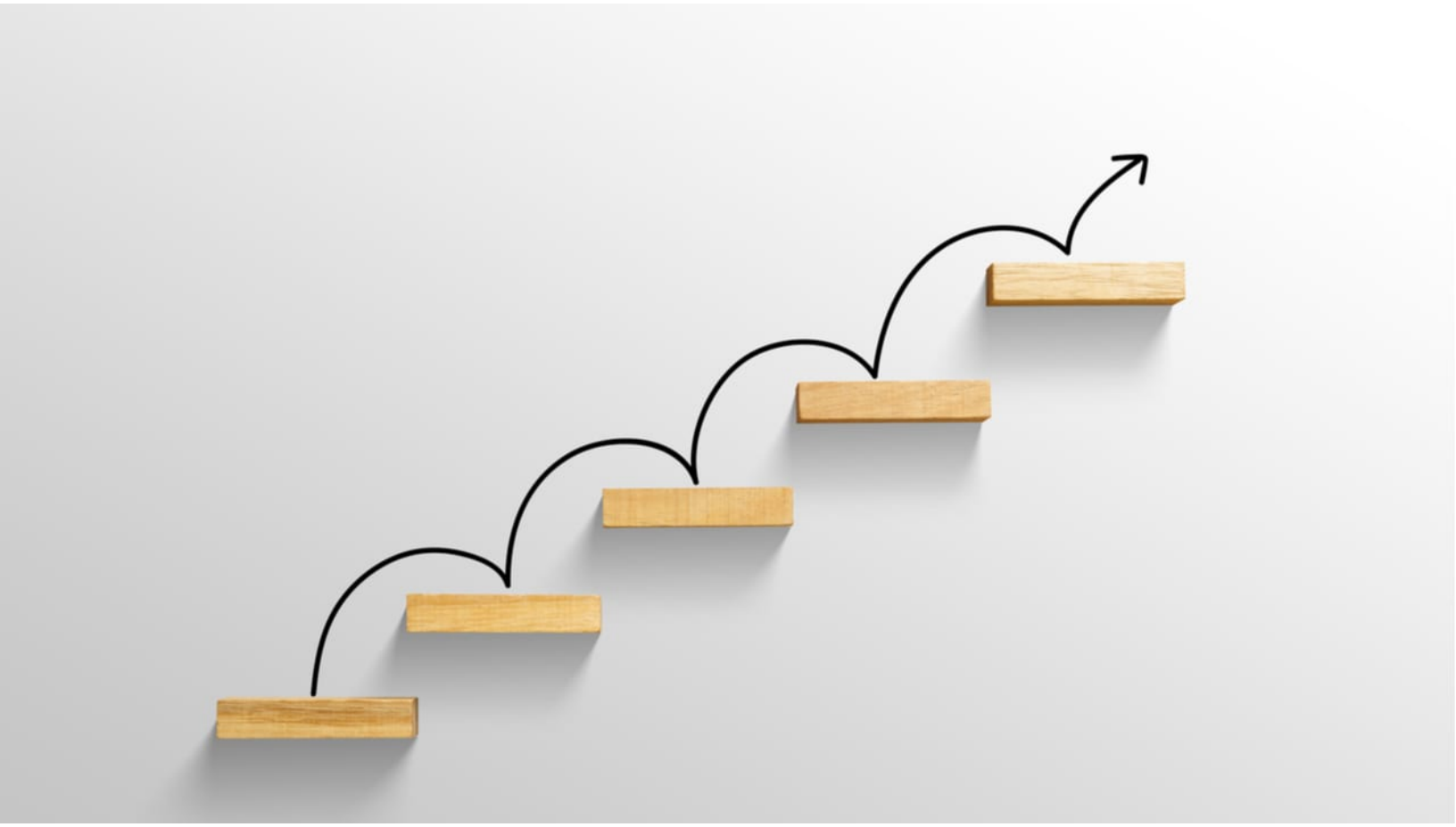
nccgroup



Dec 22, 2020 10:55 GMT

How can I materially improve my organisation's security posture?

In this article from the latest issue of our Insight Space series, Technical Associate Director Lloyd Brough explains how security teams can rapidly reduce their cyber risk by prioritising and fixing security weaknesses and make high-quality security improvements.

When approaching improvements to your organisation's security posture, knowing where to begin can be overwhelming – particularly when you have a complex set of user requirements and service level agreements, and then you are presented with complicated post-security test reports.

This difficulty, coupled with resource challenges and the wealth of advice available to businesses on every security subject, can make it significantly harder to know what security risks to prioritise, which can result in basic issues not receiving the attention they need.

Even if you don't have a security improvement plan in place, it's important to take a structured approach to remediating security issues. Doing this gives you the space to contextualise and prioritise, plan, and execute high-quality improvements that can significantly strengthen your security posture.

Taking a step back

Whether you've received recommendations following a cyber security assessment or want to proactively reduce your cyber risk, it's important to take a step back and prioritise what needs to be done to protect your business. Being proactive provides the necessary breathing space to map out the issues you or the assessment has identified, and most importantly, prioritise these.

While there will be a number of 'sticking plaster' tactical fixes that can be implemented across your organisation, you should generally use these as a method of reducing the current risk to an acceptable level, whilst you ensure that medium-term enhancements and long-term strategic priorities are not forgotten.

To make this process as straightforward as possible, bucket the issues identified through the cyber assessment in order of priority and identify the phases in which these issues should be addressed.

What issues can you address now?

Quick fixes shouldn't need to involve complex change requests and should take a minimal number of days to plan, check and implement.

When prioritising these issues, it's important to think about how easy this issue could be to exploit and the impact on the network. However, it's also crucial that you don't forget to consider the compound risk. The outcomes of a red team or incident response are often dramatically higher in impact than a list of the issues would appear. The attack chain can be either broken, or at

minimum monitored at key points, but this should be part of the immediate risk reduction.

What is needed to enhance your posture in the medium-term?

While medium-term enhancements should involve a high-level design and user acceptance testing, they should still be part of your company's rapid change programme. This may require you to decommission legacy systems and bring in new ones.

Other impactful changes could include implementing robust application whitelisting across endpoints or EDR implementation.

What strategic solutions will contribute to your future resilience?

Longer-term strategic decisions will require new design, hardware and software – this will take some time to design and implement, given the complex changes and interdependencies involved.

Too often, cyber security is applied too late in the development cycle of systems or applications, and in some cases, isn't applied at all during the organic growth of an enterprise estate.

Unpicking the interdependencies and designing a new system as part of a longer-term strategic security improvement is an ideal opportunity to change this. When you make security a consideration from the start, you're preventing it from becoming a blocker in the future.

Taking Ownership

All of this can only be achieved when buy-in is secured across the board – without full understanding and commitment, whoever is responsible for driving the security strategy forward will struggle to make any tangible improvements. This is where having a clear improvement plan in place is critical.

Applying the fundamentals of security

Despite end-user awareness and security education improving over the last few years, many businesses still fall into the trap of forgetting how effective the basics can be.

Multi-factor authentication on your internet-facing resources is a must. Too often we see poor quality and reused passwords being the trigger for catastrophic breaches. Internal systems should have the same rigour applied to them as those on the obvious frontline.

These fundamentals are even more important as the future of work continues to evolve. Earlier this year, we published a piece on the eight security fundamentals that all organisations, working remotely or not, should work towards.

The UK's National Cyber Security Centre (NCSC) also has a range of resources available for organisations, including advice on how to achieve the best possible security across networks, systems and information, as well as guidance for boards on how they can establish a baseline of security across their organisations.

The benefits

Having a defined security strategy that breaks down the quick fixes, medium and long-term issues is crucial to improving your security posture via rapid risk reduction transitioning into strategic improvement.

By understanding your existing security challenges and risk profile, developing, implementing and measuring a structured improvement plan and upskilling your team to defend and monitor your network in the long term, you can make reducing cyber risk a much easier process.

For more information about improving your security posture by prioritising and fixing security weaknesses as part of a defined security strategy, download the full issue of *Reducing risk alongside BAU*here

ENDS

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 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia 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