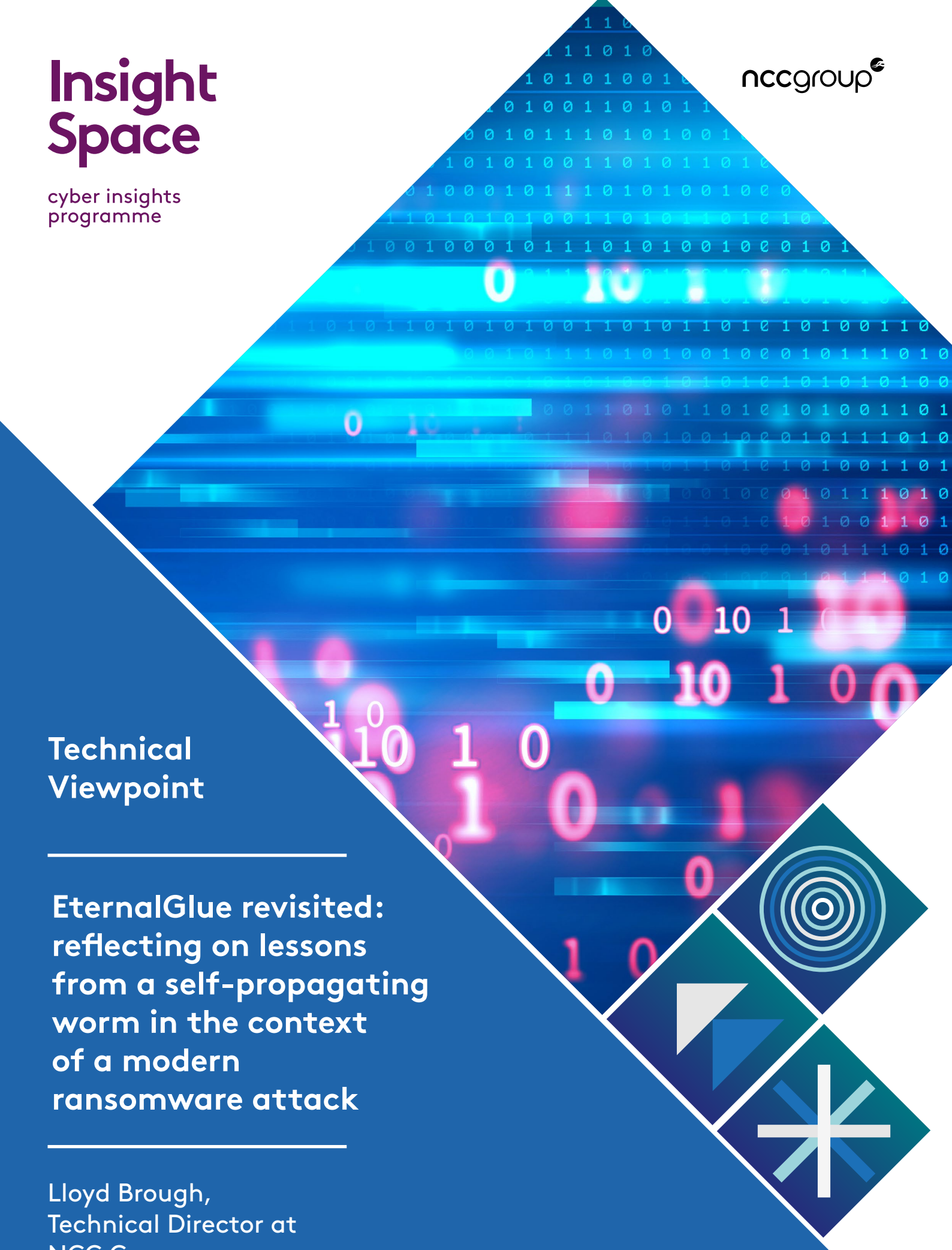
Insight Space

cyber insights programme

nccgroup



Technical Viewpoint

EternalGlue revisited: reflecting on lessons from a self-propagating worm in the context of a modern ransomware attack

Lloyd Brough,
Technical Director at
NCC Group

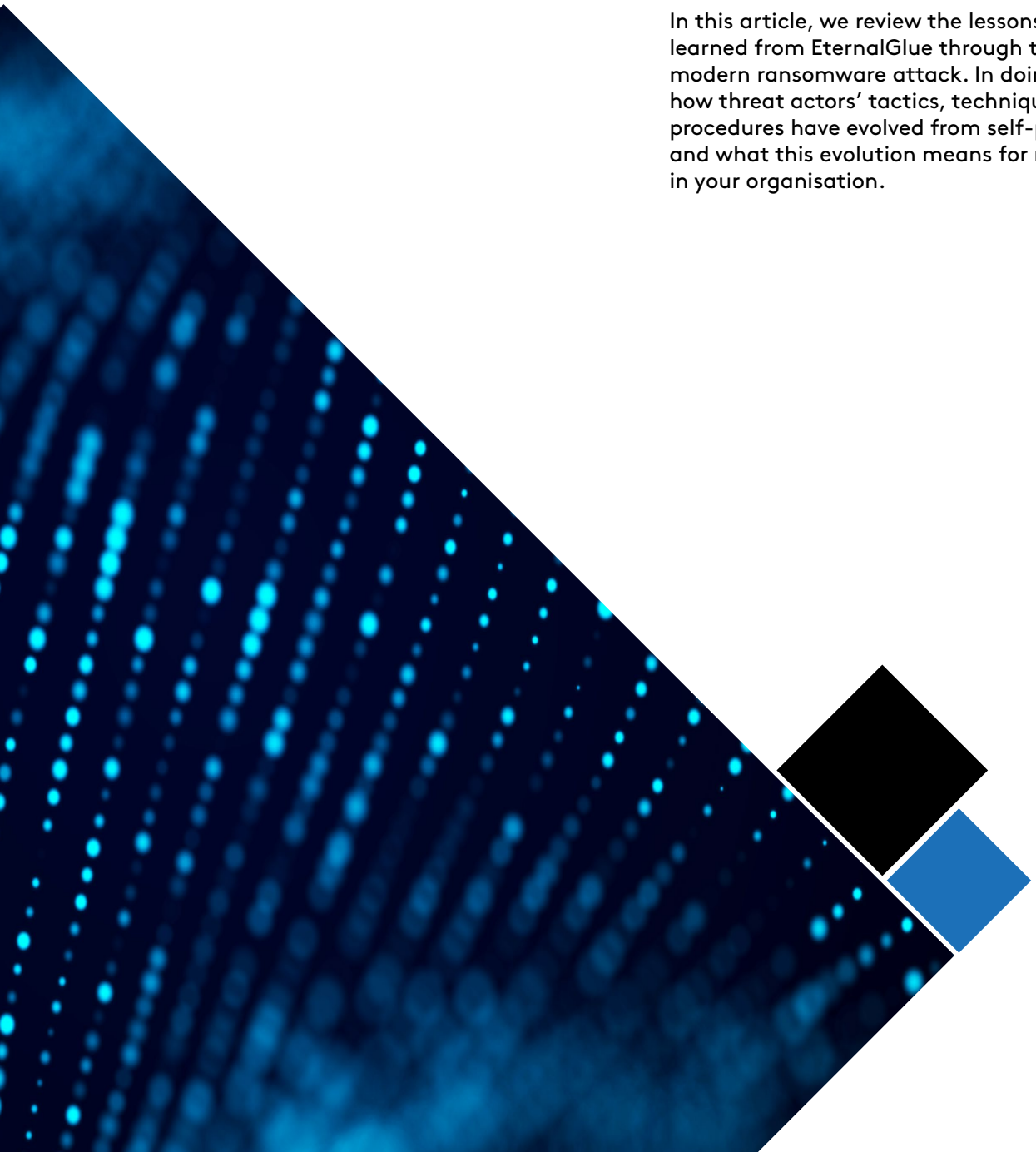
Introduction

In June 2017, the NotPetya worm alerted boards, technical staff and the general public around the world to the threat of ransomware.

Unlike previous strains that encrypted data which could be recovered if paid for, NotPetya destroyed any of the hosts it was able to infect. It also propagated itself from one unpatched machine to another without relying on human or technical errors, enabling it to rapidly spread across entire networks and causing more than $10 billion in estimated damages around the world.

Following NotPetya, boards and technical staff began to question how resilient their organisation was against such an attack. With that in mind, one client asked if we could create a simulation of NotPetya and deploy it within its network so that it could quantify its risk against this new threat. The result was EternalGlue, a safe and controllable self-propagating malware worm.

In this article, we review the lessons that we learned from EternalGlue through the lens of a modern ransomware attack. In doing so, we outline how threat actors' tactics, techniques and procedures have evolved from self-propagation, and what this evolution means for ransomware risk in your organisation.



Launching EternalGlue in a live environment

The first live test of EternalGlue took place on a section of the customer's engineering network that was isolated from its corporate systems. After being deployed on a single machine with low privileges, EternalGlue found three unpatched machines and obtained system level access.

Within ten minutes, it spread itself through the entire departmental network using recovered or stolen credentials. Two minutes later, the domain controller was infected. When the client initiated the kill switch after 45 minutes, EternalGlue had compromised all 107 hosts on the isolated network.

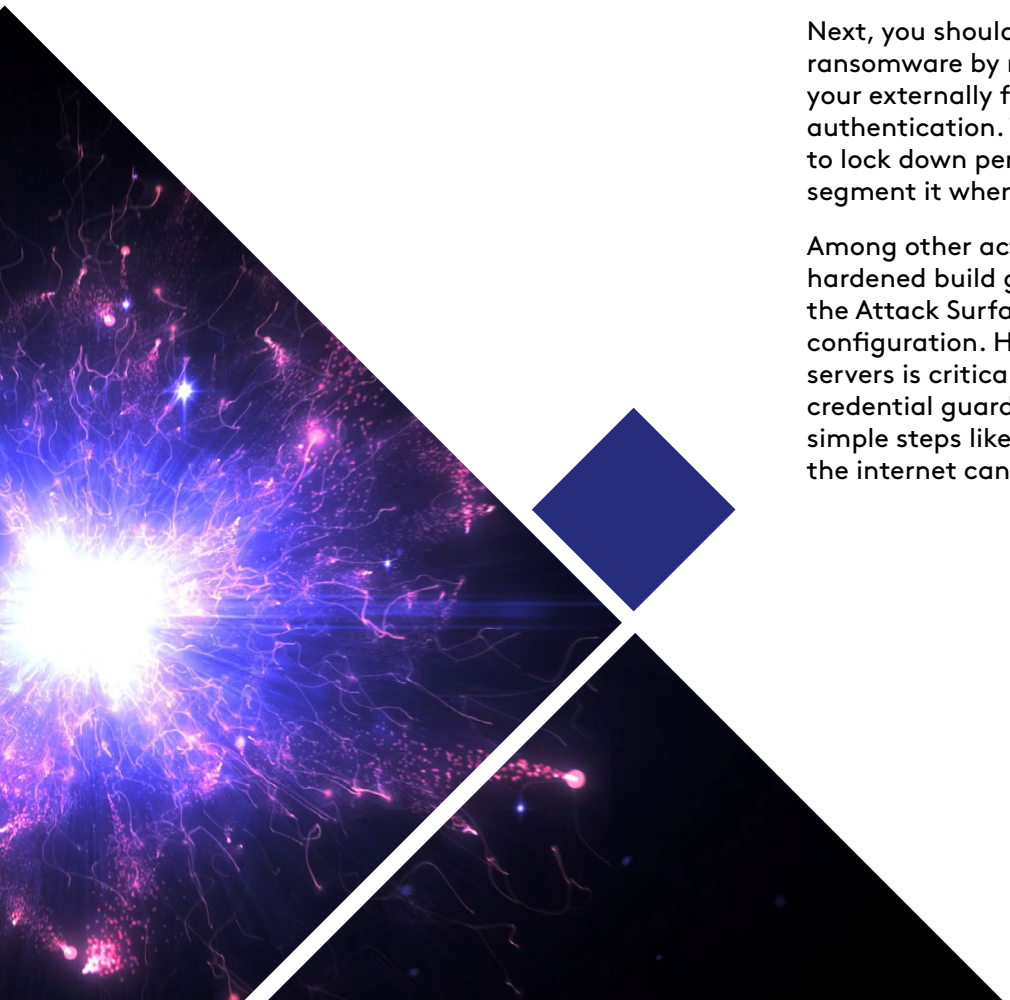
The test was a success, but some of EternalGlue's exploit payloads were still being detected by the client's antivirus. After tweaking it so that the antivirus would fail to detect EternalGlue even when it recognised a previous incident or similar behaviours, we tested it in the client's corporate environment. After thirty minutes, EternalGlue compromised an unpatched computer in Switzerland before gaining privileges. Although it was initially prevented from propagating quickly by a security configuration, a misconfiguration in a software development network enabled it to compromise over 200 of the customer's hosts in just 15 minutes.

Self-propagation vs enhanced hybrid evolution

Since EternalGlue, ransomware has evolved beyond self-propagation. Many of the attacks that we've seen in recent years have been manually deployed by a human and used bespoke tactics to encrypt, destroy and steal data from entire organisations.

However, recent developments including exploits of 0days, the compromise of managed service providers and automation for lateral movement and privilege escalation indicate that threat actors are continuing to evolve their methods of attack.

Although the tactics, techniques and procedures have evolved since EternalGlue, the consequences of a successful ransomware attack remain the same: catastrophic damage and highly visible disruption. As such, the prevention of access to your network remains the best and only defence against modern ransomware attacks. With that in mind, here are the three key steps that you should take to reduce your risk:



PATCH

Patching is the first line of defence against ransomware. EternalGlue and almost every major ransomware attack started by infecting an unpatched device before spreading laterally across a network, so it's crucial that you include regular patching as part of a good cyber hygiene program.

Creating an inventory of every device and system on your network and monitoring its status can help you to patch promptly as part of everyday operations and prevent threat actors from gaining an initial access vector in your organisation.

HARDEN AND SECURE

Next, you should reduce your susceptibility to ransomware by mandating that access to all of your externally facing systems requires multi-factor authentication. Then, apply least privilege concepts to lock down permissions across your network and segment it where appropriate.

Among other actions, you should also apply hardened build guides, including settings like the Attack Surface Reduction (ASR) Microsoft configuration. Hardening your endpoints and servers is critical. This includes application control, credential guard and exploit protection. Even simple steps like preventing servers from routing to the internet can help to derail an attacker.

Self-propagation vs enhanced hybrid evolution

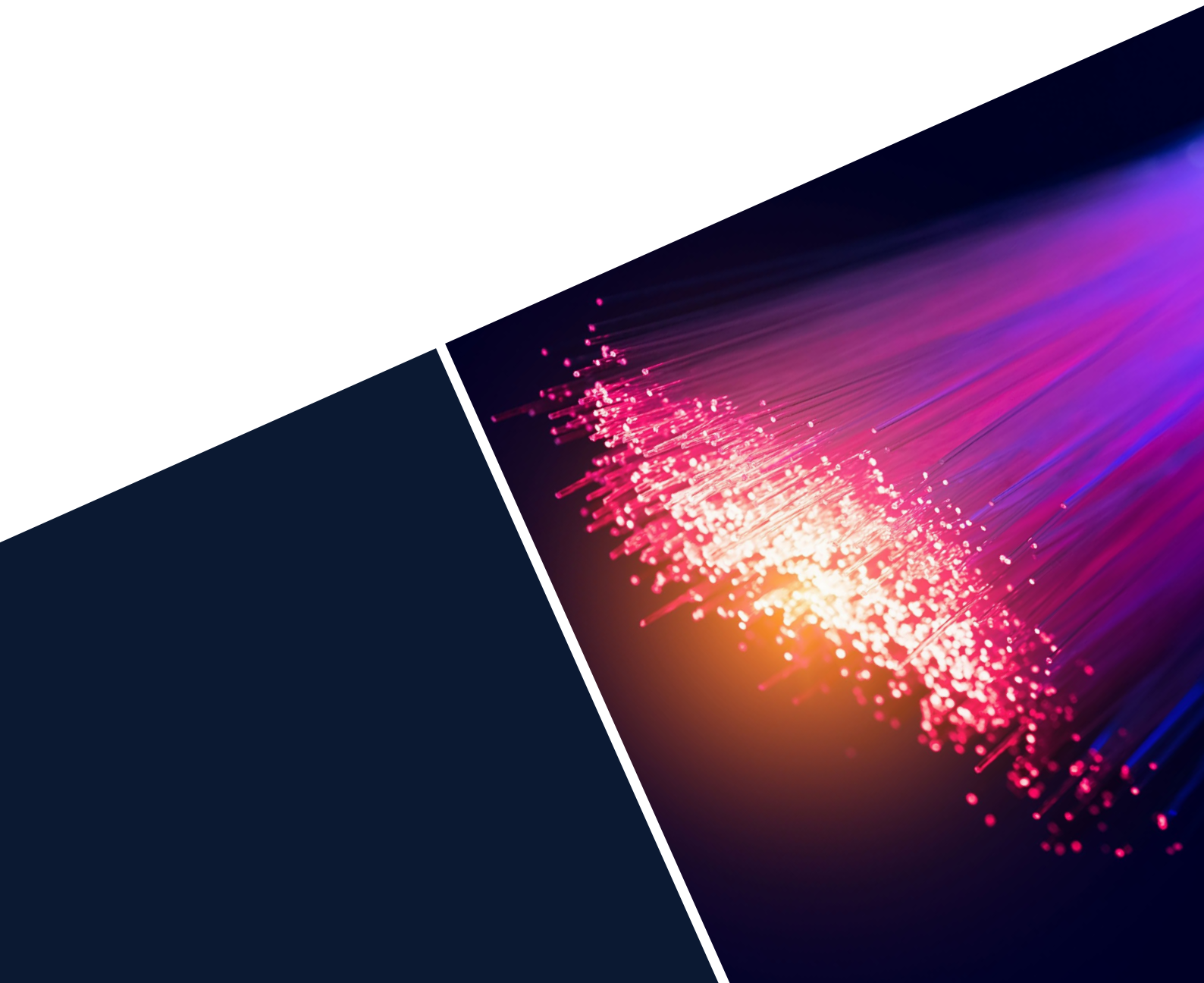
CREATE A CULTURE OF RESILIENCE

To create ongoing resilience against an attack, ensure that you have a tested continuity and disaster recovery plan. You should also create an incident management policy and supporting procedures that consider the operational impact of lost data and systems and empowers people to make decisions like calling in external help in the event of an attack.

Finally, ensure good cyber hygiene across your organisation by training your employees to identify modern phishing emails and enable them to flag suspicious activity with your IT team.

Preparing for the next big ransomware attack

Ransomware is a profitable crime, so threat actors will continue to develop new ways of infecting organisations with it. As such, it's highly likely that even more devastating attacks will occur in the future using a combination of new and existing techniques, potentially including a self-propagating strain like EternalGlue and human deployment. Prevention is the best form of defence, so it's essential that you act on the steps outlined in this article to maintain a low profile of risk.



Insight Space

cyber insights programme

nccgroup

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 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 assess, develop and manage 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 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.

To discuss how you can reduce your ransomware risk, speak to our team today.

+44 (0)161 209 5111

response@nccgroup.com

www.nccgroup.com