Insight Space

cyber insights programme

nccgroup

What's your legacy? The hidden ongoing security and resiliency cost

Technical Viewpoint

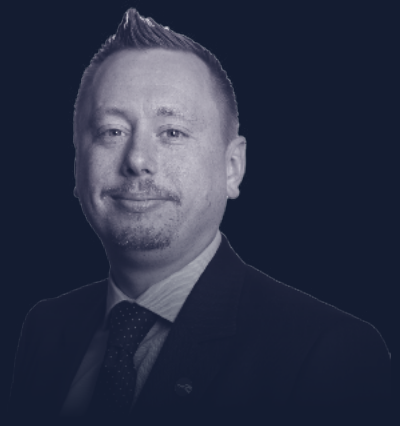
- What's your legacy? The hidden ongoing security and resiliency cost
- Legacy is not cheap or free - accumulating security debt
- Practical planning for cyber resilience

Ollie Whitehouse
CTO at NCC Group

Global. Transformative. Resilient.

What's your legacy?

The hidden ongoing security and resiliency cost



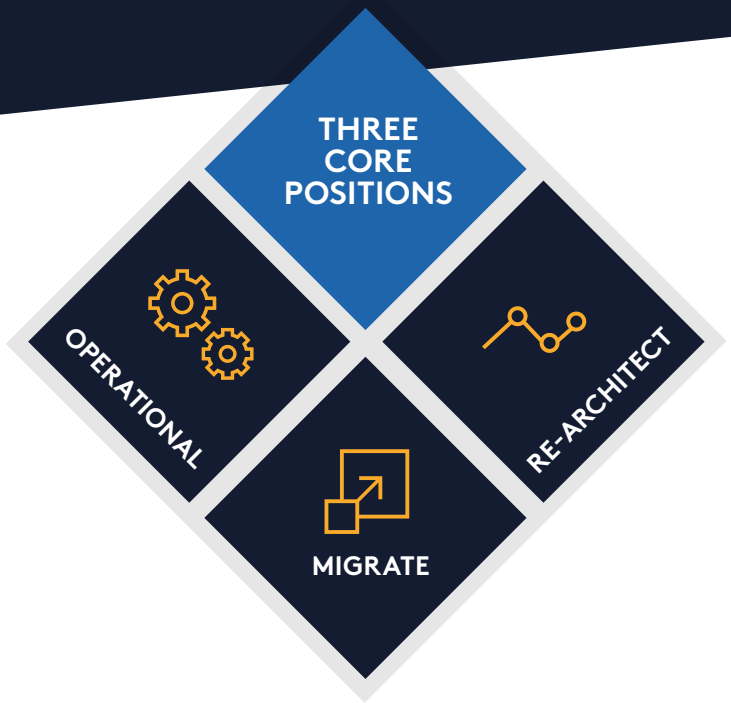
Ollie Whitehouse
CTO at NCC Group

When you are involved in cyber incident response it doesn't take long until you start to see in the thematic of successful attacks. A common theme, it may or may not surprise, is legacy. This can be for entry, lateral movement or privilege escalaton.

Legacy systems are prevalent in most organisations of a certain size and age. It might be networking equipment, embedded systems, operating systems, applications or custom line-of-business software. It's these systems that time and time again provide the point of entry an attacker is looking for through latent and known vulnerabilities – often exposing newer cloud-first environments in the process due to the interconnected nature say via Active Directory Federate Services or similar.

As we know organisations of all types have to wrestle with the trade-offs between either investing to keep them going, or investing for transformation when looking to pay down technical, security and compliance debt that these systems build up.

76%
of respondents temporarily increased their risk tolerances



Legacy is not cheap or free - accumulating security debt

And what do we mean by debt in this context?

In short - over time, systems and wider technology environments will often see a reduction in investment in their maintenance as organisations look to maximise their return. Cyber security maintenance is – for a lot of organisations – a manual process, so this reduction results is less proactive management of technical and compliance aspects, and in turn greater risk acceptance. Debt starts to accumulate.

We see three core positions taken when faced with a 'maintain or transformation' decision:

- Keep the legacy system operational and integrate
- Migrate the legacy system as part of a transformation
- Re-architect and re-platform the legacy system as part of a transformation.

Of these approaches, it is easy for a leadership team to rationalise the first and keep the legacy going on perceived cost efficiency grounds. But the problem is, the risks associated with this option are often not fully understood by technical and risk teams and therefore the full implications cannot be conveyed.

The fact is – legacy is not cheap or free when compared to modern platforms. In security terms those latent and known vulnerabilities – or simply a lack of maintenance – will be very costly when they result in an operational incident.

Legacy is not cheap or free - accumulating security debt

On the technical side, the debt manifests itself in a number of different ways, and the resulting symptoms will include:

Low levels of automation in all areas	Systems not monitored or monitorable	Teams can't meet security requirements or standards due to lack of functionality
Systems not managed or manageable	Systems not patched or patchable	Teams can't implement compensating controls or do so cost effectively

Over time these symptoms become systemic, even though the system may be business critical. This inevitably leads to situations where 'we must keep it going', but we know it is setup to fail.

55%
said they planned to increase security spending by up to thirty per cent

98%
of security decision makers said they currently use third parties to support or perform cybersecurity improvement or security remediation

Practical planning for cyber resilience

Here's the key takeaway: when organisations go through any sort of digital transformation, the impact of carrying any legacy issues into a new environment should be fully understood and challenged whenever possible. If you don't opt for re-architecture and re-platforming, we strongly recommend that proper care and consideration is given to how cyber resilience is factored in for the long-term. And the impact should be clearly articulated to the executive.

These considerations will exist at multiple levels, and include things like:

- Logical network access to exposed services
- Authentication and authorisation
- Monitoring
- Maintenance automation including vulnerability identification and patching
- Automation

Plan ahead and ensure that transformation isn't hampered by legacy and debt.

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 we can help you address legacy security issues to build your organisations's cyber resilience, speak to our team today.

+44 (0)161 209 5111
response@nccgroup.com
www.nccgroup.com