Insight Space

cyber insights
programme

Legacy: the hidden ongoing security cost?

Webinar Write-Up

- How and why do legacy risks accumulate?
- How can organisations deal with legacy risk?
- How does legacy risk management fit into a security improvement plan?

Katy Winterborn
Principal Security Consultant
at NCC Group

Global. Transformative. Resilient.

Legacy: the hidden ongoing security cost?

When conducting penetration tests for our clients, legacy systems are one of the first things that we look for. Generally, these systems are outdated or unsupported by their manufacturers, but remain active in an organisation's IT environment. Legacy systems can present considerable risk if they are left unchecked, and they often provide the route for hackers or security testing teams to compromise an organisation's systems.

According to our **recent global survey** of 500 cyber security decision makers, this 'legacy risk' was exacerbated by COVID-19: 76% of respondents admitted that they had temporarily increased their risk tolerances to allow changes to their operating model during the pandemic. However, this appears to have negatively impacted security postures, with 45% reporting that their digital transformation projects have inherited legacy security issues.

In our latest The Big Three webinar, Tim Rawlins, Senior Advisor, Nigel Gibbons, Rebecca Fox, Interim IT Director and Nigel Gibbons, Director, joined me to discuss the issue of legacy risk in more detail. We asked how and why legacy risks accumulate, what organisations can do to deal with legacy, and how legacy risk management fits into a security improvement plan.

Katy Winterborn
Principal Security Consultant at NCC Group

45%
reported that their digital transformation projects have inherited legacy security issues

1 How and why do legacy risks accumulate?

According to our panel, many organisations do not account for the eventual decommissioning or securing of new systems when presenting a business case for them as part of a new transformation project.

As a result, IT environments become bloated with legacy systems that can present risks to that organisation.

As Tim highlights, these systems are often provided by third parties that have their own roadmaps and strategies around end of life support, taking legacy risk management out of the organisation's hands.

This can lead organisations to unknowingly run legacy products that are no longer supported by manufacturers because the risk management for that application or system was not accounted for in their own security roadmap.

Our panel also highlighted how legacy risks can also accumulate through M&A activity. By failing to conduct technical due diligence on an acquired company's systems and processes, organisations can absorb legacy systems without necessarily understanding the risks of doing so. In turn, this can disrupt the acquiring company's transformation projects as they attempt to implement the new systems and enable business continuity and growth.

76%
of respondents admitted they had temporarily increased their risk tolerances to allow changes to their operating model during the pandemic

2 How can organisations deal with legacy risk?

In our experience, organisations often have business-as-usual processes that are aimed at decommissioning outdated hardware and software, but these are rarely as comprehensive as they need to be, resulting in legacy systems being overlooked. In one example, Tim referenced a organisation that was using a Windows 7 laptop to create physical access control cards. The unpatched laptop was operating within the client's IT estate and presenting a risk to the organisation, but they only became aware of it after NCC Group conducted detailed security testing into the environment.

To mitigate these risks, organisations should clearly identify every asset that sists on their estate and the condition that they're in so that they can establish the actions that are required to secure those assets accordingly. They should also understand what systems are essential to the delivery of core business services or a transformation project, and work backwards to prioritise and mitigate risk around those systems. By doing so, organisations can optimise their overall management of risk rather than working through a long list of individual issues.

Our panel also advised that organisations should understand the threat to their organisation from their supply chain. Regulators are increasingly focusing on the risk presented by third parties, so decision makers should ensure that the terms of their contracts with suppliers provide adequate measures around end-of-life security, and challenge their vendors if they are not satisfied with the existing agreement.

3 How does legacy risk management fit into a security improvement plan?

Until recently, organisations were often left with long lists of security improvements that they needed to make following a security test or audit, without any real guidance on how they should prioritise or implement those improvements within their business. At NCC Group, we've been working with our clients to support them in creating a security improvement plan to effectively address those improvements.

Legacy risk management is a key aspect of an effective security improvement plan. By applying a unique risk lens, we've helped organisations to identify how they can drive legacy out of their IT estates within their existing strategies and policies. By doing so, organisations can get a better view of the short, medium and long-term improvements that are needed to keep legacy risk at bay, such as segmenting the network or isolating a legacy system if it can't be removed or decommissioned.

Ultimately, a security improvement plan must translate legacy risks into a common language that IT teams and board members can use to agree on an acceptable level of risk for their organisation, and make decisions accordingly. Every board member will view this acceptable level of risk in a different way so it's easier said than done, but finding common ground can go a long way to helping organisations address legacy risk.

Top three actions to reduce legacy risk:

Don't let it accumulate. Aim for a 'one in, two out' policy when introducing new systems. 1

Know your risk: Not every old piece of hardware or software will present a risk, so ensure that you know which assets to prioritise. 2

Account for a system's whole lifecycle: A product that is shiny and new today could be a legacy system tomorrow, so think about the entire existence of an asset and the assurance that you'll provide for it through to decommissioning. 3

To find out more about how you can reduce legacy risk in your organisation, watch the full webinar, 'Legacy: the hidden ongoing security cost?' here.

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 legacy risk, speak to our team.

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