
Apr 06, 2021 21:02 BST

# Webinar playback: Is there a cyber debt left by Covid-19?

*Ade Clewlow, Senior Advisor, NCC Group*

With rapid digital transformation, financial pressures, and a mass shift to remote working, many organisations have struggled to maintain their previous levels of cyber resilience over the last year.

This has built up a cyber debt that is affecting a wide range of businesses. To truly understand its scale and impact, we spoke to 290 cyber security decision makers from across public and private sector organisations about the challenges that they've faced this year.

We found that budget cuts have significantly affected cyber spend over the last 12 months. Three out of ten businesses experienced delays or a cancellation of their cyber resilience projects, while one in five had to furlough staff responsible for cyber resilience programmes.

This reduction in resources has already had an impact on business resilience. Of those that reported cuts to budget, 70% also stated that they'd seen an increase in cyber attacks, while two-thirds of businesses reported internal skills shortages and an increase in insider-related incidents.

These issues have been exacerbated by changing working habits over the last twelve months. 21% of organisations expect staff to use more of their own devices while working in 2021, which makes effective security monitoring far more difficult. Meanwhile, digital transformation and cloud solutions are here to stay, which can contribute to a build-up of cyber debt.

To discuss the scale of today's cyber debt, and how it can be paid off, I was joined on our latest 'Big Three' webinar by cyber experts Mark Ward, global chief information security officer at Interserve IT, Katharina Sommer, head of public affairs at NCC Group, and Tim Anderson, group commercial director – managed detection and response at NCC Group.

Here's the key topics we discussed:

**QUANTIFYING CYBER DEBT**

Quantifying cyber debt is extremely complex. With changing working habits, it's hard for organisations to understand what the future could look like – and therefore, how their level of cyber debt might change.

However, it's important for organisations to understand their current risk profile and adapt their operations where necessary. Threat actors are seeking to take advantage of security weaknesses, while business leaders' focuses are on other operational concerns – which introduces a new element to existing threats.
Understanding any current vulnerabilities and areas for improvement is the first step towards quantifying cyber debt. A Cyber Security Review is a useful way of benchmarking your organisation's resilience against peers, and provides clear actions that can help your business begin addressing this cyber debt.

## RESPONSIBILITY FOR CYBER DEBT

Many security decision makers are already aware of the importance of increased security investment. Our research found that two-thirds of organisations plan to increase cyber security budgets this year, and that the amount spent on outsourcing security expertise will increase.

For many organisations, showing a return on investment on security efforts remains a challenge. 90% of respondents highlighted that they struggle to quantify the cost versus benefit of cyber security. For IT leaders, articulating security risk in terms of business priorities is key.

It's also important for all employees to take ownership of this issue of cyber debt. This can be achieved by ensuring that all staff are aware of what they can do to maintain cyber resilience. A safety-first culture, an effective technology strategy, and investment in both internal and outsourced skills can all make a significant difference.

## RESTRUCTURING CYBER DEBT

To begin paying down this cyber debt, organisations must first understand their own risk profile and strategic priorities.

Once businesses understand the level of risk they face – and the level of risk they are willing to accept – it's possible to build a list of priorities as part of a security improvement plan, and begin working through these. This type of plan maps out the short, medium and long-term strategic measures that can significantly improve your security posture.

While organisations may not be debt free in a matter of months, now is the perfect time for business leaders to address the issues that have built up over the last year, and begin paying off their cyber debt.

*To find out more about how your business can quantify and address cyber debt, you can watch the full webinar, 'The Big Three: Is there a cyber debt left by Covid-19?', on-demand here.*

Watch video on YouTube 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 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