Insight Space

cyber insights programme

nccgroup

Crunch time:

Unpaid cyber debts are increasing the risk of attacks – and threatening to disrupt digital transformation projects

Market Research Report

Organisations plan to increase cyber security spending this year, but will it be enough to tackle long-term security issues?

Global. Transformative. Resilient.

Introduction

Most of us know how easy it is to avoid dealing with a growing problem. This head-in-the-sand approach (or "avoidance" behaviour as psychologists term it), can also occur in business, especially when resources are stretched thinly.

Recently, many organisations have trimmed security spending on older IT systems that are expensive to maintain and are replaced by newer versions over time. However, these cuts have had unintended consequences, including the creation of security flaws that make those organisations vulnerable to hacking.

This problem accelerated during the COVID-19 pandemic as organisations around the world cut security spending, froze recruitment of security professionals and rushed to move services online to support home working.

Our latest research – which interviewed 500 IT security decision makers – suggests that this "legacy" security problem is growing. It also found that security decision makers are tolerating higher levels of security vulnerability than they are comfortable with.

Most worryingly, our research found that companies' underlying security problems are threatening to disrupt nearly half (45%) of organisations' digital transformation projects.

Any security breaches in digital transformation – one of the top priorities for companies of all sizes and types worldwide – would cause financial damage and harm an organisation's reputation.

It's not all gloom, though. Security executives told us that they are planning to increase spending on security this year. As our research shows, the challenge will be to ensure that this spending tackles the legacy security problems that are emerging as the hidden costs of cyber debts that are still being paid off.

We interviewed 500 IT security decision makers – suggests that this **"legacy"** security problem is growing.

45%

of companies' underlying security problems are threatening to disrupt nearly half of organisations' digital transformation projects.

Risky business

The combination of ongoing cyber security challenges for organisations means that many have been forced to accept a lower standard of IT security.

Three in four (76%) of respondents said that they had to temporarily increase some of their risk tolerances to allow changes to their operating model (such as remote working), to tackle the risk of unresolved issues due to the pandemic. Eleven per cent said that the higher risk tolerances would be permanent.

76%

of respondents said they had to temporarily increase some of their risk tolerances to allow changes to their operating model.

45%

of organisations' digital transformation projects have inherited legacy security issues.

Excess baggage

However, these increased risk tolerances appear to have negatively impacted security postures.

Forty-five per cent of organisations' digital transformation projects have inherited legacy security issues. According to our research, this is partly because organisations have struggled to manage business-as-usual improvements to their security while prioritising risks and coping with a growing volume and complexity of security improvements.

Missing connections

Silos within business are notoriously difficult to eradicate, and this includes IT departments.

Our research found that seven in ten digital transformation projects do not have security fully integrated in them. When we asked security decision makers if cyber security and major programs in their organisation such as digital transformation were integrated, only one in three (30%) said they were. Thirty-nine per cent said that there was partial integration, while twenty one per cent said that there was no integration but "ad hoc" cooperation.

30%

said that cyber security and major programs in their organisation such as digital transformation were integrated.

Security spending is rising

After cutting spending on cyber security in the past year during the pandemic, including four in ten companies freezing recruitment of security staff, most companies plan to increase spending on it this year.

More than half (55%) of those questioned said that they planned to increase security spending by up to thirty per cent. Ten per cent said that they planned to cut security spending by less than thirty per cent.

However, amid a widespread shortage of security skills, and about six in ten companies relying on internal assessments of the effectiveness of their security, it is unclear whether any increase in spending will be enough to fix companies' long-standing security weaknesses.

Many organisations feel overwhelmed by the scale and variety of cyber security threats, and are struggling to make substantial improvements to their security. Forty-four per cent of those surveyed said that "we need to make security improvements, but finding and fixing issues is getting lost among business-as-usual."

Twenty-three per cent agreed with the statement "we know we have security weaknesses, but time and skills shortages are getting in the way." Eighteen per cent agreed with the statement "we need to quickly reduce cyber risk."

Importantly, only one in four (24%) of organisations we questioned said that they have a "security improvement plan" in place, suggesting that there is room for organisations to allocate their spending more strategically.

55%

said that they planned to increase security spending by up to thirty per cent.

24%

of organisations said they have a **"security improvement plan"** in place.

> "We know we have security weaknesses, but time and skills shortages are getting in the way."

Security challenges

Companies' biggest security challenges, according to our research, include balancing proactive improvements in security with everyday operations (49%); deciding which security risks to tackle first; and the "volume, and complexity of assessment reports from third parties" (joint second at 42%).

Tackling these problems alone is too much for even the biggest organisations. Almost all (98%) of security decision makers we surveyed said that they currently use third parties to support or perform cybersecurity improvement or security remediation (taking proactive and long-term improvements to security).

The most common types of third-party security service that those questioned said they would consider buying were ones that support the "long-term leadership of the delivery of our security improvement program"; "ongoing/long-term support to our security improvement program" and help with "longer-term strategic improvements" in cyber security.

SECURITY CHALLENGES

49%

balancing proactive improvements in security with everyday operations.

42%

deciding which security risks to tackle first.

98%

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

Summary

1. Organisations' digital transformations programmes are vulnerable to cyber-attacks after they increased risk tolerances and are still grappling with ongoing cyber security challenges, according to new research by NCC Group.

2. The research, which earlier this year questioned 500 IT security decision makers in the private and public sectors, found that forty five per cent of organisations' digital transformation projects have inherited "legacy" security issues.

3. Seven in ten digital transformation projects do not have security fully integrated in them, the research also found.

4. Organisations plan to increase security spending in the next year, but are struggling to cope with the scale and ever-changing variety of cyber-security threats.

Global. Transformative. Resilient.

The Big Three Virtual Event -

10th November 2021 at 12pm

Join our free upcoming virtual event, 'The Big Three,' where we'll discuss the three key questions that you should be asking about legacy security:

1. How and why do legacy risks accumulate?
2. How can organisations deal with legacy risk?
3. How does legacy risk management fit into a Security Improvement Plan?

Katy Winterborn
Principal Security Consultant

Nigel Gibbons
Director Partner

Rebecca Fox
CIO NCC Group

Tim Rawlins
Senior Advisor NCC Group

In this exclusive event, we'll provide practical advice on how you can budget effectively to mitigate legacy risk and pay down cyber debt to increase your overall resilience. We'll also explain how you can secure essential legacy systems to keep your active transformation projects running and minimise disruption to your business-as-usual operations.

REGISTER HERE FOR VIRTUAL EVENT >

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 organisation's cyber resilience, speak to our team today.

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