Remediate by nccgroup

An NCC Group Publication

Are security legacy issues slowing your digital transformation down?

Dominic Carroll, Product Manager and Service Architect

When digital transformation projects are executed effectively, they enable you to drive your core business strategy forward. However, 45% of organisations claimed that their transformation projects had inherited legacy security issues that impacted their security posture in our recent survey. These issues, combined with the results of security assessments, can make it difficult to align security risk management with your organisation's priorities.

Often, these assessments uncover long lists of security improvements that need to be made, without any guidance on which improvements should be prioritised to have the most impact on your cyber resilience. In these circumstances, security risk management can become a blocker for business transformation if teams work through fixes without a clear roadmap.

To overcome this issue, risk owners should convert the results of an assessment into a structured Security Improvement Plan that prioritises remediations according to your short, medium and long-term business strategy. With that in mind, here are three ways that you can use a Security Improvement Plan to prevent legacy issues from slowing down your transformation agenda.

> "Holding on to legacy infrastructure can become a blocker for business transformation if teams work through fixes without a clear roadmap"

1. Resolve critical issues before embarking on your transformation agenda

Any Security Improvement Plan should be considered as a long-term roadmap to reduce your risk position. With cyber-attacks increasing in the last 12 months, it's important that your roadmap is flexible so that you can be agile enough to remediate critical security issues quickly, without jeopardizing imminent transformation projects.

By using a consistent measurement of risk, you can effectively prioritise vulnerabilities and create a backlog of critical fixes that need to be made. Then, external security partners can often remediate the vulnerabilities that are critical to your innovation agenda, working alongside your IT teams to enhance your immediate resilience against cyber threats while you focus on innovating at pace.

If there is a specific area of your transformation project that is of particular concern e.g. your Azure Active Directory configuration settings, then a 'find and fix' discovery option can be implemented to quickly remediate security risks in that area.

You'll also be working with hybrid (cloud and On-Prem) estates during your transformation project, so you should prioritise identity access management (IAM), multi-factor authentication (MFA) and the quality of passwords across your organisation to reduce risk here, in addition to securing your cloud environments.

By prioritising security fixes in this way, you can also address the legacy issues that are slowing your digital transformation down. Common examples of these legacy risks include:

- Unpatched apps and systems
- Systems that haven't been isolated from the internet or your network
- Supply chains that haven't been properly risk-assessed

2. Proactively accelerate key transformation priorities

When the most critical issues have been addressed, a Security Improvement Plan gives you the clarity, transparency and focus to proactively improve your mid-term security. By triaging and categorising vulnerabilities according to their potential impact on the business, you can gain a holistic view of your risk profile against your strategy and risk appetite.

Armed with this information, you can prioritise and proactively address issues that might impede business progress more effectively. For example, if you've identified critical issues in your legacy systems and are introducing a transformation project that connects to those systems, you can prevent any delay to that project by directly addressing known issues, or provisioning supporting technology to enhance resilience.

As part of your Security Improvement Plan, you should also understand the cost, time and resource required to remediate the key security risks that have been identified in your organisation. Again, this will give you a clearer picture of when you will need to scale up your resources to support the delivery of a transformation project, enabling you to proactively manage and mitigate risks before they result in a cyber incident. Having an upfront scope of the cost and effort required to reduce risk can also help you to build a business case for upgrades to your technology.

3. Embed a culture of security by design

To build a secure platform for growth and enable transformation projects in the future, it's important that your Security Improvement Plan includes longer-term strategic decisions to improve your security posture over time. Often, this involves examining your people, processes and technology to uncover the root causes of vulnerabilities that have already been remediated to stop them re-surfacing in the future.

DevSecOps is an effective means of adopting a collaborative approach to executing security transformation across an organisation, so Security Improvement Plans should facilitate the adoption of these methods. By integrating cyber security into the development cycle of systems and applications from the beginning, and during the growth of enterprise estates through transformation projects, you can ensure that risk management is an enabler rather than a blocker.

Targeted risk reduction in action

Remediate is NCC Group's security improvement and remediation service. It helps security teams rapidly reduce their cyber risk by prioritising and fixing security weaknesses without impacting business as usual operations.

Remediate has already accelerated the transformation agendas of various businesses, including:

Charity

Following a major incident, we stood up a hybrid access method in less than two days, enabling the organisation to become operational.

Global Organisations

Working collaboratively, we removed attack vectors at pace to eradicate and lock threat actors out after a cyber-attack.

Public Sector

By rebuilding an Active Directory domain controller in less than 3 days following a ransomware attack, we helped the client reassert control and rebuild its systems.

To discuss how we can help you to prevent legacy issues from delaying your business transformation, speak to our team today.

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

Conclusion

Penetration tests, red team exercises and security audits are all key pillars of good cyber hygiene, but the way in which you implement their recommendations can determine whether risk management supports or undermines your business strategy.

A strong Security Improvement Plan that has buy-in across your organisation can help you to position cyber security risk as an enabler within your organisation by unlocking transformation projects and business growth in the short, medium and long-terms.

Remediate by 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.

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