Insight Space

cyber insights
programme

How to prevent legacy derailing your transformation projects

Executive Viewpoint

- How to prevent legacy issues from derailing your transformation projects
- (Whole) life insurance
- Integrating total cost of ownership into transformation projects
- Apply the risk lens

Tim Rawlins
Director and Senior Advisor
at NCC Group

Global. Transformative. Resilient.

How to prevent legacy issues from derailing your transformation projects

Tim Rawlins
Director and Senior Advisor at NCC Group

Digital transformation is one of the biggest opportunities for organisations to grow, so it's not surprising that senior executives are always looking to invest in the shiniest new systems that can drive their business forward. In our experience, however, organisations are less enthusiastic about investing in those systems as they are replaced by newer products and become outdated over time.

Left unchecked, 'legacy systems' can present considerable security risks. As they age, cyber criminals will have spent longer looking for vulnerabilities that can be exploited within them. They know that they are more likely to find those vulnerabilities as developers and end users spend less money on updating and securing them as they move to end of life.

Unfortunately, these legacy security issues can seriously affect security postures: in our recent survey of 500 cyber security decision makers, 45% told us that their transformation projects had inherited legacy security issues. And exploiting those vulnerabilities to gain access to current and maintained systems is increasing, as we have seen in several attacks on supply chains recently.

With this in mind, you should account for the management of legacy systems as part of their 'total cost of ownership' before beginning transformation projects. Otherwise, your legacy systems could quickly end up costing you more than expected.

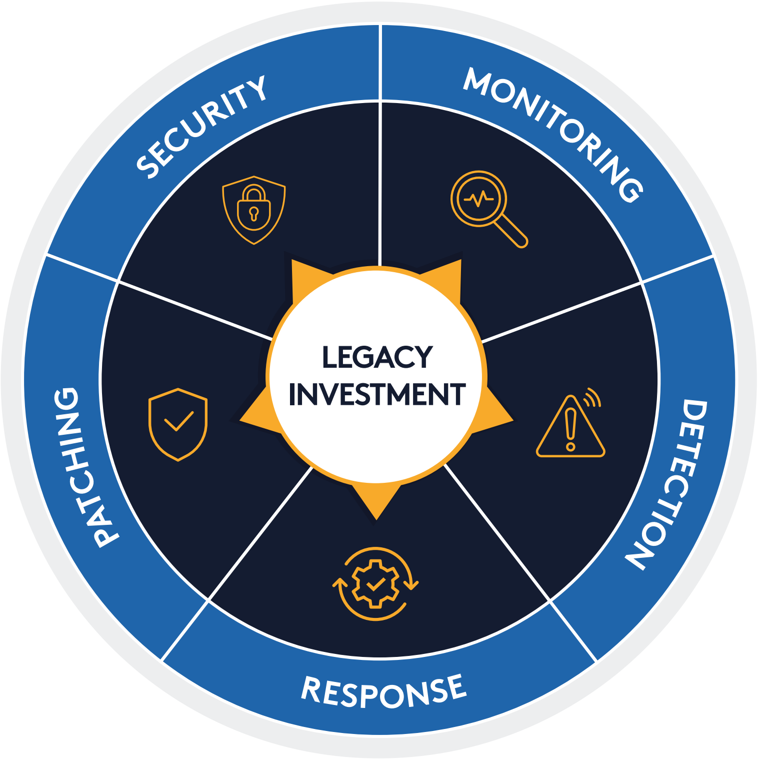
45%
said their transformation projects had inherited legacy security issues

(Whole) life insurance

But what does the total cost of ownership include?

Essentially, it means budgeting for securing legacy systems in the long term, or properly decommissioning them. This can be easier said than done when budgets are squeezed and there is already pressure on IT teams to deliver proactive security improvements alongside business as usual operations.

However, accounting for whole life costs will save you money in the long run by tangibly reducing your transformation projects' risk of falling victim to legacy security flaws, so it's well worth the investment up front. This investment should include the removal of common security issues around identity and access management, proper monitoring, detection and response and patching legacy systems on an ongoing basis.



Integrating total cost of ownership into transformation projects

We regularly see organisations that leave legacy systems running because they've forgotten about them or because they assume that they still need them for one operation or another. This isn't necessarily true in many cases, so ask your IT team about which legacy systems need to be kept operational to support your transformation projects. Once you've established this, you should implement an effective decommissioning process to remove all non-essential legacy systems from your estate. This process can take some time, so audit the health, life span and current status of all the assets on your estate on a regular basis. This will help you to identify and prioritise the legacy items that need to be decommissioned more urgently than others, such as those that are no longer supported with security patches yet still have access to the internet.

If you're already using legacy systems as part of an ongoing digital transformation project and are unable to turn them off, you should isolate them from the internet and other internal systems. By putting effective network segmentation in place, you can significantly reduce the risk that cyber criminals will be able to access and exploit the legacy systems. This could involve internal firewalls, jump boxes with additional privileged access controls, multi-factor authentication or data diodes to create that segmentation and improved security. Again, finding the budget for this is preferable to dealing with a major incident.

Apply the risk lens

As our survey highlighted, the COVID-19 pandemic put cyber security teams under considerable pressure: 76% of organisations admitted that they had increased their risk tolerances to cope with changes to their operating model in the last 18 months, with many still grappling with ongoing security challenges.

With these circumstances in mind, it's understandable that many organisations struggle to apply an effective 'risk lens' to their transformation projects. For example, we recently worked with one client that missed over 100 legacy Windows servers during its business as usual decommissioning process. By discovering them and bringing them into the decommissioning process, we helped it to reduce risk to its estate, save money and reduce its carbon footprint.

This ability to review your review business-as-usual activities and improve operational resilience across your IT department is a key benefit of engaging an external company to address your legacy security issues. Whether it's finding ways to reduce the vulnerabilities that exist, providing a spotlight on the good work that is already being undertaken or offering support to deliver transformation programmes with additional remediation resources, third party expertise can make a significant impact in reducing the risk to your estate. It is well worth the investment of your resources.

Top four actions to protect your transformation projects from legacy risks:

Establish the legacy systems that need to remain operational to support your transformation projects. 1

Implement an effective decommissioning process for all non-essential legacy systems. 2

Isolate essential legacy systems from the internet and other areas of your network by segmenting your network. 3

Engage third-party expertise to apply an independent 'risk lens' and remediation to your transformation projects. 4

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.

nccgroup

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