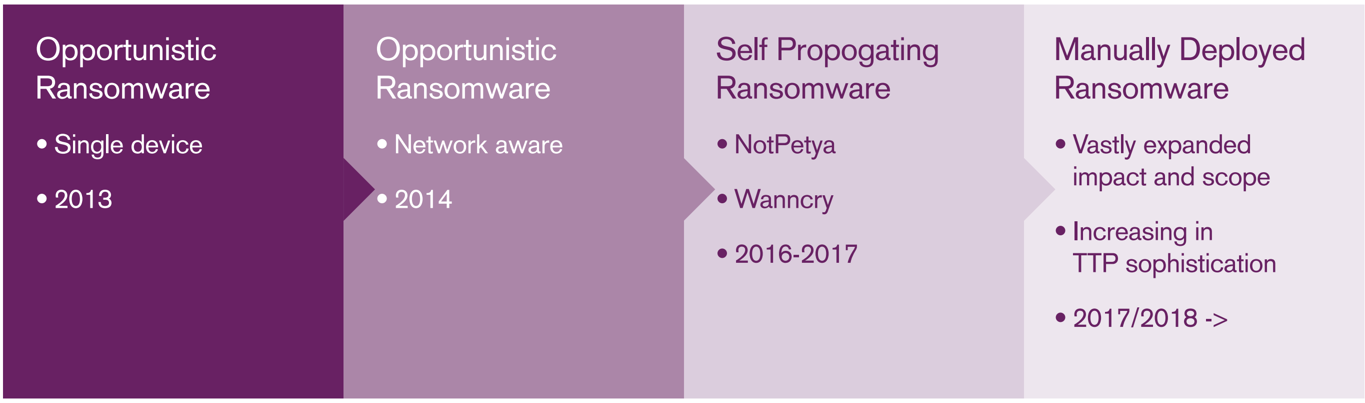
An NCC Group Publication

Building Resilience within Local Government

The rate of ransomware evolution has outpaced the security improvement efforts of many organisations, leading to resilience challenges cross-sectors. Local governments are no exception. Vastly expanded in their scope and impact, these attacks now target entire organisations through highly customised attacks, causing catastrophic and highly visible business disruption.



Opportunistic Ransomware

- Single device
- 2013

Opportunistic Ransomware

- Network aware
- 2014

Self Propogating Ransomware

- NotPetya
- Wanncry
- 2016-2017

Manually Deployed Ransomware

- Vastly expanded impact and scope
- Increasing in TTP sophistication
- 2017/2018 ->

Figure 1: the evolution of ransomware

Ransomware Evolution

A ransomware attack on a Local Authority in early 2020, which significantly disrupted its ability to maintain operations, brought into sharp focus the risk posed by cyber criminals and other malicious actors. The attack raised concerns that comparable organisations may have similar vulnerabilities caused by the same issues; historic underinvestment, the market-wide skills gap and mounting security debt, making them susceptible to ransomware attacks. The preparations for the response to the growing Covid-19 crisis, together with the importance of maintaining citizen services during the impending lockdown, made the need for operational resilience even more important. In response a central government sponsored 14-week remediation programme was initiated to rapidly establish the risk position in 27 organisations thought to be at the greatest risk of ransomware, and to make practical interventions to reduce the specific risks identified. The objectives were clear:

1. Reduce vulnerability of backups to Ransomware attack

2. Reduce the susceptibility of organisations to ransomware attacks

3. Improve the longer term resilience of each organisation

An initial view of the risk in key areas was established through targeted a questionnaire and workshops, with a programme of accelerated security improvement and remediation work initiated to quickly reduce risk across all organisations.

A Collaborative Approach

The joint programme between the Local Authorities (LA's), Ministry of Housing, Communities and Local Government (MHCLG), Cabinet Office (CO) and NCC Group had a number of challenges to overcome. The pace of the programme required a high degree of integration and collaboration across the very broad stakeholder group; there were multiple independent organisations each with different priorities. Making the required impact within the 14 weeks available called for a not only close collaboration, but a highly-transparent approach to programme planning, and most importantly, the flexibility of the remediation team to work around other operational priorities of each organisation. Further, the impact of the pandemic on remote working made the key imperatives of building trust, establishing relationships and delivering technology solutions more challenging.

A baseline of vulnerability exposure and security posture was established through a facilitated self-assessment approach, via a workshop, providing an indication of the risk present in each estate, however in most cases, a Cyber Threat Actor (CTA) emulation was required to truly understand the security posture of the organisation.

The delivery of risk prioritised remediation at this scale was only achievable through a modular approach that delivered essential solutions to the organisations that needed them. These modules are continually updated based on the latest technology and threat information, and cover seven key security and resilience themes. Delivering the majority of activity in this modular approach allowed the programme to achieve consistency of delivery at scale for common risks, whilst taking a more flexible approach to unique risks where required.

During the programme a close working relationship was established between NCC Group, MHCLG, the CO, the LGA and LAs, at all levels, to share knowledge, troubleshoot and react to findings that may have potential impact on organisations in the wider public sector.

The characteristics of the team required to deliver a technical remediation programme of this nature were particularly important. The ability to converse at a detailed technology level, transferring the understanding into these organisations in a practical and reproducible way, was particularly important. The diversity of the team coming from a wide range of backgrounds, sectors, and professional areas of expertise, supported creativity and problem solving in overcoming local challenges. The multidisciplinary nature of the team supported all aspects of cyber resilience from practical security engineering through to processes and procedures, such as Business Continuity and Disaster Recovery.

Outcomes

The programme was a fantastic collaborative success; achieving its 3 key objectives. The programme quantifiably reduced the risk of the ransomware threat across a large number of organisations critical to the Government's Covid-19 response:

- All critical and high risks identified in relation to both the vulnerability of backups to ransomware and the broader susceptibility to ransomware were reduced to a controllable level;
- All organisations received a long-term security improvement plan detailing residual risk and recommendations for continuous improvement.
- 236 remediation modules were delivered across all organisations using multidisciplinary teams of cyber consultants and engineers;

Collectively delivering such a collaborative programme of work to achieve the objectives in such a time-pressured context was a huge success and one example of a number of excellent initiatives from the Ministry of Housing, Communities and Local Government (MHCLG), the Cabinet Office (CO) and from the Local Government Association (LGA).

Learnings

The programme delivered a realistic and practical insight into the challenges faced by public sector organisations when aiming improve security and resilience, whilst proving that the relationship between the private and public sector can bring benefits at scale.

Pete Cooper, Deputy Director Cyber Defence in the Cabinet Office commented;

> "The scale and criticality of the cyber security challenges we all face can only be tackled through a collaborative approach that embraces diverse teams and perspectives across both public and private sector. It's not easy, but the benefits in understanding and reducing risk are significant."

The programme used both controls-based self-assessment and practical CTA emulation approaches to establish the baseline for security posture in the LAs. The latter provided a highly practical and effective way to evaluate the efficacy of security controls in place and as such, suggests that a minimum cyber resilience position criteria should be introduced to support investment cases and the resilience of the sector overall.

Long-term improvement programmes and embedding best practice were common challenges, due to the immediate operational challenges faced by these organisations. There was also an imbalance between understanding the risks and technology that underpins the organisation and delivering compliance, which again directly links to the day to-day resourcing challenges. Further, there were a number of more specific learnings that can be applied when aiming to reduce cyber security risk very quickly across large and de-centralised organisations:

- Modular interventions allowed a consistent approach to remediation at scale and was a cornerstone of the programme delivery methodology;
- Practical interventions proved to be more effective in remediating the vulnerabilities found during the CTA emulation;
- Close collaboration, transparency and constant communication with all stakeholder groups ensured that pace was maintained and created a sustainable long-term impact.
- The 14 week intervention was a reasonable period of time for focussed remediation of specific risks, but systemic issues require a longer programme of knowledge transfer to be embedded within each organisation;
- Facilitated self-assessments combined with CTA emulation provided a robust foundation for improving practical cyber resilience and facilitated a significant improvement over the course of the programme;
- A less compressed programme timeline would have enabled more cycles of continuous improvement and learning and could enable even greater sustainable impact.

An innovative approach to building resilience within local government

The challenge

☒ Ransomware evolution has outpaced security improvement efforts.

☒ 236 vulnerabilities rated critical or high across 27 local authorities

☒ Historic underinvestment, the market-wide skills gap and mounting security debt

Cyber remediation focus areas

☑ Internal and External Infrastructure

☑ Identity Access Management

☑ End User Compute

☑ Core Network & AD

☑ Protective Monitoring

☑ Governance, Risk and Compliance

☑ Backup Resilience

Outcomes

☒ Critical and high risks reduced to controllable levels

☒ Long-term security improvement plans implemented

☒ 236 remediation modules delivered

Achieving sustainable cyber security resilience

What **needs** to be in place?

- The desire to tackle deep-seated challenges
- Understanding the technology is vital rather than simply executing compliance
- The importance of long-term improvement programmes
- A minimum cyber resilience criteria to support investment

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 clients 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 identify, assess, mitigate and respond to 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 over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

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