NCL

Ransomware Resilience Assessment

Arm yourself against the ever-growing threat of ransomware with an assessment that doesn't just tell you whether or not you're prepared, but also recommends, prioritises and maps out a robust security improvement plan.

Most ransomware preparedness assessments just tell you whether or not you're prepared. That's great, but what then?

Our Ransomware Resilience Assessment helps your organisation protect and respond to ransomware attacks by examining 11 key security aspects. We then, as standard, provide you with a security improvement plan including identified weaknesses, recommendations and corrective actions and a high level roadmap of prioritised recommendations to help you prepare, secure, detect and respond to ransomware events.

Ransomware is a type of malware that covertly encrypts your data, stopping you from accessing it and then demands payment for "safe" recovery. However recovery is not guaranteed; neither is confidentiality. Your data will most likely be stolen and could be sold or made publicly available.

After the USA, the UK is the second most targeted country, recording 14.6 million ransomware attacks. The cost of the attacks is also increasing, with the average cost of remediating a ransomware attack more than doubling in the last 12 months.

Ransomware is designed to not just hold your organisation's data ransom, but also to stop you, your customers and suppliers from accessing your systems - essentially stopping your business in its tracks. One of the reasons it's such a significant threat is that it is designed to impair your ability to recover both your systems and your data.

Being properly prepared is the best defence and our assessment focusses on the identification of weaknesses in your cybersecurity defences that ransomware threat actors can exploit and covers the following:

- Cybersecurity objectives and policies
- Access and authentication management
- Network and endpoint security
- Security monitoring
- Phishing defences
- Vulnerability management
- Employee education and awareness
- Backup and recovery
- Business continuity & disaster recovery (BCDR) Scenarios and plans
- Incident response planning, preparation and review
- Supply chain controls

Features & Benefits

Features

- Collaborative workshops, interviews and assessments
- Assesses your current security policies effectiveness against ransomware
- Reviews effectiveness of your security auditing, monitoring and detection capabilities
- Identifies shortfalls in user education and awareness
- Reviews supplier cybersecurity posture from context of your business
- Assesses security configurations to best practice security guidelines
- Highlights improvements within your existing incident response capabilities

Benefits

- Identifies security weaknesses
- Provides prioritised corrective actions to improve effectiveness
- Provides a ransomware resilience indication for your business
- Allows training and education needs to be planned in line with highest risk
- Identifies policy improvement
- Supports identity and access management planning
- Highlights where suppliers' security posture is misaligned to yours.
- Provides clarity on configurations to meet best practice
- Identifies corrective action to strengthen response capability and reduce impact

Service Delivery

1 Preparation.

- Identify information requirements
- Timetable activity based on availability
- Schedule scrum/end-of-week slots

2 Discovery Workshops.

- Initial information gathering
- Follow-up clarifications

3 Analysis & Recommendation.

- Identify areas of improvement and capture in security improvement plan
- Determine corrective actions to achieve improvement

4 Playback.

- Report & presentation
- Provide logical timeline for actions

- Our approach uses the MITRE ATT&CK® framework coupled with recognised good practice to perform a comprehensive evaluation covering perspectives of organisation, process, technology and people.
- The assessment is delivered as a combination of document reviews, interviews and collaborative workshops with technical teams and management.
- NCL cybersecurity consultants work with your staff to correctly classify asset criticality, relative vulnerability and determine remediation action and priority.
- The assessment can be tailored to your specific needs to cover a wider assessment of your readiness or focus on specific details or areas of concern.

MITRE | ATT&CK™

Service Levels, Reporting & Pricing

Delivery	The engagement can be undertaken remotely or as a combination of on-site and remote collaboration, review and analysis.
Data Retention	Data is retained for period of assessment and then securely deleted.
Pricing	P.O.A

Build a Solid Foundation to Protect Against Ransomware

In our experience, ransomware defence is founded on clear direction and support from senior management, coupled with robust and comprehensive security practices and supported by effective incident detection and response capabilities.

We can support the development of your cybersecurity defences through hardening systems, attack surface identification & reduction, protection of sensitive data, and responding to and recovering from an attack. Contact one of our team today and discover how we can help put your ransomware fears to bed.