+44 345 094 0945
www.waterstons.com
Article

Protecting critical national infrastructure through cyber resilience

Breadcrumb

Insight navigation

Download PDF

Oct 2022

Protecting critical national infrastructure through cyber resilience

Operating within the UK's 13 critical national infrastructure (CNI) sectors comes with a tremendous responsibility to protect the nation's vital interests from cyberattacks, disruption from which could be detrimental to the daily life of ordinary citizens.

Categories

Oct 2022

As the number of cyber threats organisations must now protect against grows exponentially, and amid unstable geopolitical backdrop, nation state and organised crime adversaries continuing to become increasingly capable defeating most traditional security controls with relative ease, the conditions of a 'cyber arms race' have been created.

Organisations must now continue to invest in technical controls at a greater pace than the threats are emerging, however such a strategy is not sustainable, with weaknesses in cyber defences likely to continue to emerge overtime, meaning organisations must focus ever more on protecting through cyber resilience.

Cyber resilience

In today's ever-evolving landscape of sophisticated malware/ransomware, supply chain attacks and deep-rooted vulnerabilities, at some point all organisations are likely to suffer a cyberattack. As such, the perspective of cyber security must move beyond defending against cyber threats, to a state of readiness where incidents can be prevented, and attacks deliberately responded to and recovered from.

This cyber resilience is achieved through adopting an holistic cyber security strategy, with a deliberate focus on governance, risk and compliance, and the selection of proportionate technical controls.

Cyber assessment framework

The National Cyber Security Centre's cyber assessment framework (CAF) is an outcome-based information security management system promoting cyber capability and resilience across four strategic objectives:

1. Managing security risk
2. Protecting against cyberattacks
3. Detecting cyber security events
4. Minimising the impact of cyber security incidents.

Our approach to cyber resilience for clients

Starting out as a gap analysis assessment to establish the current cyber resilience maturity baseline, we immerse ourselves in understanding our clients' people, processes and technological security controls, assessing and agreeing the maturity target profile to be achieved, protecting against under- and over-specifying of security controls.

The outcome of the assessment informs the development of the cyber resilience security strategy, prioritising four key strategic activities aligned to each of the CAF objectives:

1. **Managing security risk**

Information security risk management is the reason we invest in security controls and further underpins the decisions we make over the future direction of the cyber security strategy.

Effective risk management should drive everything we do in cyber security; if we cannot attribute a security decision back to the management of risk, it is likely not doing an awful lot.

We guide our clients through the identification and assessment of the sources of risks, rather than assessing all of their information assets inventory, which is designed to afford pragmatism, while preserving comprehension.

2. **Protecting against cyber-attacks**

Developments in the cyber security tool stack (e.g. malware defences, firewalls and web filtering) continue to evolve at pace, partly driven by merging and acquisition of specialised security companies by larger solution providers.

Not only could clients be paying for the same capability twice over, adversely the current security stack may not be capable of preventing and detecting the latest cyber security threats. This is certainly true for those organisations reliant on traditional, signature-based malware protection.

We perform a holistic review of our clients' security stack, investigating opportunities for efficiency, better integration and gaps in capability, supported by a review of the network architecture against a secure best practice architecture model, applying the principles of 'secure by design'.

3. **Detecting cyber security events**

Identifying cyber security incidents quickly is integral to providing an effective incident response and minimising the potential for disruption.

This often involves deploying a security information and event management (SIEM) tool that is capable of automatically processing and analysing thousands of log entries generated from security tools, network and system services, and end user devices.

The central activity of the SEIM is to generate alerts warranting investigation, however this requires a skilled workforce which is ready to respond to them as and when they are generated. For some organisations it's far more effective and efficient to outsource this capability to a trusted security operations centre (SOC).

We have an in-house, 24/7 SOC native to the AlienVault SIEM and we guide or clients to make the best decision suited to them including a tailored deployment strategy, prioritising the most valuable logs telling a cyber incident.

4. **Minimising the impact of cyber security incidents**

An organisation can only be effective in their response to an incident if they are suitably prepared with appropriate processes, people and technology capabilities in place; assisting in a deliberate and highly coordinated response.

Without such a capability in place, delayed and ineffective decision-making may occur, resulting in the magnification of impact that could otherwise have been prevented.

Often, the starting point is to conduct an incident response maturity assessment before developing and implementing a cyber incident response plan.

This is a continuous improvement journey, starting with prioritising the basics then, once the plans are in place, we exercise them in a simulated setting against a realistic desktop scenario.

Regardless of size or sector, to remain resilient to future cyber security threats, the direction of your security strategy should be moving towards one of resilience. Our team of experts are well placed to understand your needs to create an effective resilience plan.

To find out more, check out the team and their expertise here.