+44 345 094 0945
www.waterstons.com
Article

Exercise your cyber security

Oct 2022

Exercise your cyber security

Cyberattacks have continued to rise on three fronts; the number of attacks orchestrated, the level of sophistication demonstrated, and the impact inflicted.

Categories Cyber Resilience, Cyber Security Strategy

Oct 2022

-
-
-
-

Sean-Francis Brown

Senior Information Security Consultant

Email

sean.brown@waterstons.com

According to SonicWall, ransomware attacks increased by 105% in 2021, and the explosive growth of strategies such as double and even triple extortion ensured that these attacks were more successful.

This increased complexity has brought about a real-time shift in mindset from cybersecurity to cyber resilience; not only defending against cyberattacks but preparing for swift and timely response and recovery when an attack does occur.

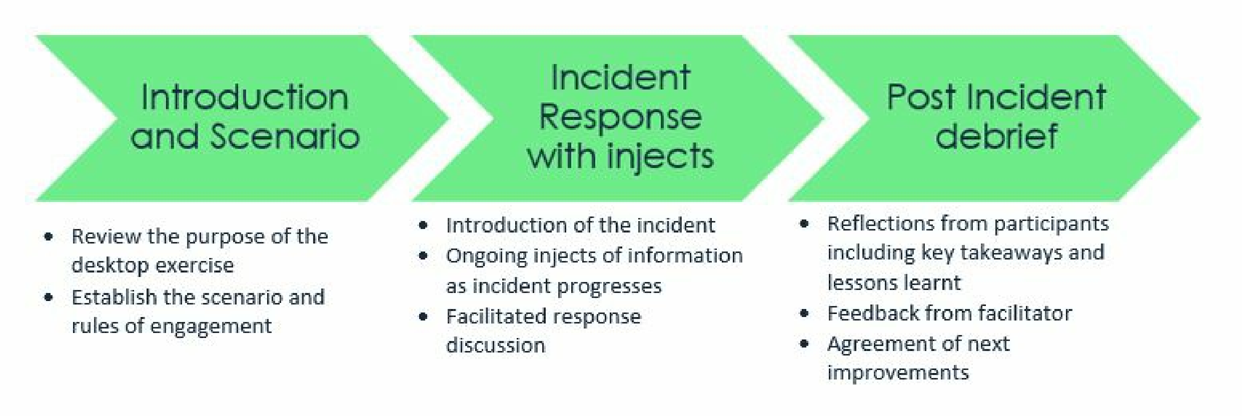
Defending against sophisticated ransomware, attacks on the digital supply chain, and exploitation of deep-rooted vulnerabilities are just some of today’s security challenges that require organisations to move beyond defending against cyberattacks, into establishing a readiness to respond to and recover from a cyber incident should one occur.

Placing cyber resilience at the core of every organisation's cyber security strategy is key, and one way to do this is by creating a regular schedule of cyber desktop exercises. These aim to examine your cyber incident processes, responses to and recovery from incidents, resuming operations with minimal disruption.

Objectives of the desktop exercises

- Increase team awareness of cybersecurity including risk management, planning and the threat landscape related to prevention, protection, response and recovery of critical system assets
- To evaluate incident response processes for suitability and effectiveness
- To evaluate leadership process knowledge and capability to timely implement the technical steps
- To Identify areas of further improvement in the incident response processes

What happens during a desktop exercise?



Introduction and Scenario

- Review the purpose of the desktop exercise
- Establish the scenario and rules of engagement

Incident Response with injects

- Introduction of the incident
- Ongoing injects of information as incident progresses
- Facilitated response discussion

Post Incident debrief

- Reflections from participants including key takeaways and lessons learnt
- Feedback from facilitator
- Agreement of next improvements

Why use these exercises?

Cyber exercising is a key method of testing both the technical infrastructure and user training of an organisation to ensure it is up to scratch in the event of a cyberattack. These exercises can be used as a tool to identify gaps and begins an open discussion for future improvement.

Cyberattacks are a case of 'when', not 'if', and you are unsure of your organisation's cyber resilience structure, contactthe team today to find out how we can help.

View our cyber security services.