CYBER INCIDENT RESPONSE TESTING

CYBER SCALE

When a security incident occurs, you need to lean on your plans and teams to lead you to a successful outcome, but how often do you exercise your plans to test their effectiveness?

Cyber Security is a business problem, not just an IT problem and the involvement of leadership teams in both response and proactive learning is critical to minimise the impact of cyber related incidents.

Are your teams able to identify a potential threat? Do they know when they need to call for additional help? Do your business leaders know their role within an Incident Response process?

Scenario exercises are a practical way for organisations to test their Incident Response Plans in a safe environment and educate staff on cyber security in the event of a security incident and/or data beach.

With our Incident Response Exercises, we stress test your cyber response with safe theoretical tabletop exercises with a focus on utilising your plans to bring your business operations back to business-as-usual.

Incident response exercises allow you to rehearse difficult situations and identify improvements, enabling your teams to react as efficiently as possible should a real-life incident occur. This testing helps to eliminate panic and confusion and allows teams to make decisions in a more calm, confident and structured way

OUR EXERCISES ARE DESIGNED TO EVALUATE YOUR RESPONSES TO THE FOLLOWING TYPES OF ATTACKS/EVENTS

PHISHING | DATA BREACH | MALWARE | DDOS

RANSOMWARE | DOUBLE EXTORTION RANSOMWARE | 3RD PARTY DATA BREACH

BENEFITS OF INCIDENT RESPONSE TESTING

- Test the cohesiveness of your Security teams and your Leadership Team.
- Testing processes and plans helps build confidence in real life situations.
- Test your internal communications and points of escalation.
- Identify any operational gaps.
- Identify any gaps in your plans and documentation.
- Greater clarity across the business.
- Identify and discuss key business decisions that will need to be made (for example, potential payment of ransoms).

HOW IT WORKS

- Discovery workshop to understand your business and the areas most relevant to test.
- You choose from a selection of pre-built scenarios (or we can choose for you); these are then tailored to your business and your incident response process.
- The planned exercise is scheduled at a mutually convenient date.
- Each exercise is delivered by our qualified and experienced consultants, either onsite or remotely. Each exercise workshop takes typically 2-4 hours.
- Following the exercise, you will receive a report giving a full overview of the exercise including observations and recommendations, presented by our team and explained in non-technical language.

Call Us: 01603 339550
E-Mail: contact@cyberscale.co.uk
Web: www.cyberscale.co.uk
Book a Discovery Call to Discuss Your Security Needs