INCIDENT RESPONSE PLANNING (IRP)

CYBER SCALE

Businesses are becoming increasingly aware of the organisational risks and potential for financial loss and reputational damage posed by cyber-attacks. Even with the best preventative measures in place risk of compromises and potential data breaches remains and therefore a formalised security Incident Response Plan is a key tool to improve resilience. This is where CyberScale can help your business be prepared.

Cyber-attacks don't only affect a business across IT and systems, they have the potential to impact your business in multiple ways, so any Incident Response Plan should encompass other areas of your business such as HR, Legal and Finance.

Incident Response Planning is an organized approach to preparing for, detecting and containing a security breach or cyberattack, Your IRP is there to minimise damage, protect your data & systems, and to ensure your business recovers from the incident as quickly as possible.

Ensuring that you have an IRP in place means that you will have a tool that enables you to respond proactively and quickly, making clear decisions based on the information needed by your business to do so.

CyberScale will work with your business to create and deliver a specific and actionable plan that will detail where all responsibilities sit, what each person is required to do in the event of a Cyber-attack and also when each part of the plan needs to be engaged.

Alongside the creation of an Incident Response Plan CyberScale are experienced in producing tailored Incident Response Run Books and building Incident Response Exercises.

Incident Response Run Books

The Incident Response Plan needs to be broad enough to cover multiple scenarios; our experience shows that many elements of managing an incident still require decision making depending on the nature of the incident. CyberScale can create supporting runbooks for common scenarios, which can be used to add context to the IRP and further improve your organisations' ability to manage the associated risks of any cyber-attack.

Incident Response Exercises

In order to evaluate the effective implementation of your Incident Response Plan and identify areas for potential improvement, CyberScale highly recommends undertaking regular Incident Response Exercises. Following the initial delivery of the plan and the incorporation of the procedures into business-as-usual operations, we can work with your team to identify likely incident scenarios and design appropriate exercises to test your ability to manage these incidents.

The Incident Response Plan Creation Process

1.

1. IRP workshop:

CyberScale will discuss core components of the Incident Response Plan with appropriate members of your team including Roles, Resources, communication, supporting systems, integration with other plans and training.

2. IRP creation:

Initial draft to be created and reviewed with your team, including high level process flows and supporting process documentation. Following review, this will be revised as necessary to create a final version for delivery.

2.

3.

3. IRP familiarisation:

CyberScale will host a session with relevant members of your team to familiarise them with the plan & process, ready for use in your business.

Book a Discovery Call to Discuss Your Security Needs

E-Mail: contact@cyberscale.co.uk

Call Us: 0800 030 6616

www.cyberscale.co.uk/contact