Incident management

How to effectively detect, respond to and resolve cyber incidents

As security measures evolve, so do the capabilities of our adversaries. As a result, no security can ever be perfect. Incidents can and will happen, so it's important to be prepared for them.

This guidance collection will help you plan, build, develop and maintain an effective cyber incident response capability.

Good preparation is essential

Over recent years there have been numerous incidents reported by the media, and many that have not. These have included widespread and damaging ransomware attacks and the theft of sensitive personal or company data. Meanwhile, fraud and cyber crime continue to cost many millions of pounds each year.

Incidents can be opportunistic or targeted, and threats can originate from outside and inside your organisation. But, whatever the nature of the threat, ***only one thing can help you deal well with a cyber incident - good preparation.***

Develop a response plan

When the inevitable cyber incident or attack occurs, your incident response plan and capabilities should kick in.

A well planned and executed response will help to minimise the damage caused by a cyber attack. This could mean anything from cutting the amount of data lost, to minimising public and media fall out.

Part of a bigger picture

Incident response is a critical part of the cyber security life cycle, but in order to respond appropriately, the other elements of the cycle must be considered. As identified by the National Institute of Standards & Technology (NIST), the life cycle is: Identify, Protect, Detect, Respond, Recover. Our *NIS Directive guidance follows a broadly similar process*.

Your incident response plan should also be linked to disaster recovery, business continuity and crisis management plans, and supported with the relevant capabilities. These come into play when an incident is serious enough to cause major disruption and/or damage to your business.

Structure of this guidance

In the real world, great technology and technical capabilities may still not make for a great response if the right people, with appropriate skills are not in place.

Similarly, skilled people may struggle without an incident response plan, or relevant data analysis tools.

In real responses, the processes, people, and technical capabilities all overlap with each other. Here, we have divided them neatly, for ease of reading and explanation.

Collection structure

1. **Overview of Incident response**
   A high level introduction to the incident response process, including the important issues of detection and notification.

2 **Processes for Cyber Incident Response**
This section outlines the ingredients of a basic response plan, breaking down how an incident should be managed in practice and examining the various stages of a response. This will enable you to develop your own tailor-made plan.

3 **Incident Response Team**
Advice on forming an incident response team, including the skillsets and roles required. This ranges from the critical skills every business should have, to those that only larger businesses may have. We also look at how to develop those skillsets.

4 **Technical Capabilities**
This section explores the technology that will be needed in the event of a cyber security incident. It also considers logs and other types of evidence, along with the technical actions and analyses that can contribute to the successful resolution of a cyber security incident.

5 **Building and Maintaining capability**
What to consider when designing, building and maintaining your Incident Response (IR) capability.

6 **Appendix: Incident timelines**
Breakdowns of the actions which should be taken to stem various types of incident, with commentary.

PUBLISHED

19 September 2019

REVIEWED

19 September 2019

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Large organisations