AMR Cyber Security

Incident Response

WHITE PAPER

February 2023

VERSION: 1.0

TABLE OF CONTENTS

YOUR CYBER DEFENCE TOOLBOX

Tom Miller from AMR CyberSecurity describes how organisations can best defend against, detect and respond to cyber-attacks.

Many organisations are concerned about potential and actual cyber security attacks, both on their own organisations and through the supply chain. Dealing with cyber security incidents – particularly sophisticated cyber security attacks – can be a daunting, difficult task, even for the most advanced organisations.

The best way to shield against attack is to develop an appropriate cyber security incident response capability - and adopting a systematic, structured approach to cyber security incident response.

Recent cyber security incidents have seemingly focused on supply chain attacks. The UK's NCSC has recently released guidance on how to assess and gain confidence in your supply chain cyber security.

Measure your cyber incident response maturity

CREST, the international not-for-profit, membership body representing the global cyber security industry has developed a maturity model to assess an organisation's cyber security incident response capability. The model includes a maturity assessment tool - the Cyber Security Incident Response (CSIR) Maturity Assessment - which measures response maturity on a scale of 1 (least effective) to 5 (most effective).

Organisations can use this to benchmark their response capabilities against industry best practice and to support improvement activities.

Develop your cyber incident response processes

Organisations should develop and implement a set of documented incident response policies and procedures. This allows them to respond to security incidents in an appropriate, repeatable, timely and effective manner. Procedures should also be developed to record 'lessons learnt' from an incident and implement incremental improvements as required.

Incident response processes should cover all stages of an investigation:

- Identifying cyber security incidents
- Investigating the situation (including triage)
- Taking appropriate action (e.g., contain incident and eradicate cause), and
- Recovering systems, data and connectivity

Organisations should also ensure the following aspects are considered when developing cyber incident response and management policies:

- Ensure the right people in the organisation are involved in response plan development. This includes IT security, HR, legal, key suppliers, communications and public relations teams, and most importantly, senior management.
- Ensure Incident Response plans are aligned to disaster recovery, business continuity and crisis management plans
- Establish clear roles and responsibilities, including clear incident escalation

pathways for key decision makers

The CREST CSIR Maturity Assessment Model stipulates that incident response processes should take account of:

- Definitions required to support the triage element of the cyber security incident process (e.g., to define what criteria are required to classify and prioritise incidents)
- Advice and guidance provided on government websites, such as the NCSC Top Ten steps to cyber security.
- Publicly available traditional or cyber security specific incident response guides, such as the NIST Computer Security Handling Guide, the Responding to targeted cyber-attacks report from ISACA.

Test your cyber incident response capability

Regular testing of your incident response capabilities provides a means of measuring organisational resilience and the effectiveness of your cyber incident response capability.

The first stage of testing an incident response capability is to identify likely attack use cases that may impact your organisation. Threat scenarios can be based on a variety of sources including specialist external threat intelligence providers and published national threat assessments.

Threat scenarios can be developed internally, based on previous internal incident records and knowledge of the internal security team, or published open-source intelligence information relating to attacks impacting your sector. There is a range of tools organisations can use to develop their attack use cases, such as the MITRE ATT&CK Framework.

Testing cyber incident response capability against identified attack use cases can be via desktop exercise, simulated, targeted attack-based testing or red team testing.

Desktop-based testing is an effective, safe means of testing cyber incident response capability and can be led and delivered by internal security teams.

The NCSC has produced useful guidance for organisations looking to create their own cyber incident response exercises. It's written for IT staff, cyber risk management and business continuity teams in small to medium sized organisations.

More mature organisations can look to supplement desktop-based testing with simulated, targeted attack-based testing or red team testing to directly test their organisation's resilience and effectiveness of their cyber incident response capability.

CREST has developed a Simulated Target Attack and Response (STAR) scheme, which provides a framework and an assured set of service providers which are capable of carrying out Intelligence-Led Penetration Testing.

CREST STAR intelligence-led penetration tests use threat intelligence to deliver attack simulations, delivering assurance that organisations have appropriate countermeasures and responses to detect and prevent cyber-attack.

Tests are carried out by experienced penetration testing providers on all types of organisations, and are considered the most realistic form of assurance service in the sector.

Results are then combined with a review of the company's ability to recognise and react to cyber security-related attacks.

Another option available to organisations looking to test their incident response policies and processes is the NCSC's Exercise in a Box.

Exercise in a Box is a free-to-use online tool that provides exercises based around the main cyber threats faced by organisations. It includes everything you need for setting up, planning, delivery, and post-exercise activity, all in one place.

There are a great many resources available out there – many of them free. Organisation, preparation and ensuring the right people and processes are in place are the best methods to ensure your organisation remains as safe from attack as can be.