secarma
CYBERSECURITY EXPERTS

A Advise C Certify T Test

Incident Response Exercising

Modern organisations face a range of cybersecurity risks and whilst every effort may be made to prevent a breach, if one does occur an organisation must be prepared to respond to that breach quickly and effectively.

The period of dealing with a security breach is one of tension. If a company is not adequately prepared for the efficient handling of an incident, then a time of tension becomes one of crisis.

Who Is It For?

Our Incident Response Scenario Testing (also know as 'Wargaming') is for organisations who have established an incident response and business continuity plan, that wish to test the effectiveness of that plan in a controlled manner.

How Can We Help?

Secarma have developed a Cybersecurity Incident Wargaming service, which is designed to explore the effectiveness of an incident response plan against realistic scenarios, through a tabletop exercise.

Wargames are usually scheduled for a three-hour session, allowing for the steps of incident response to be deeply explored, yet still allowing for breaks and open discussion in the group.

At the end of the session, the intention is that the response team will more clearly understand the strengths and weaknesses of their incident response planning.

We have found these sessions work best when each aspect of the response team is represented in the room, such as the board, the technical team, and the communications team.

What We Test

We typically develop scenarios that are based on real-world incidents that have previously taken place. However, if your organisation wishes to test against a specific scenario, we can build a bespoke exercise. Example scenarios include:

- **Malicious Software Outbreak**
  This scenario plays through the common stages of a major malware outbreak to test how well an organisation can identify, contain, eradicate, and recover from an attack such as mass ransomware.
- **Denial of Service Attack**
  This scenario walks through a complex denial of service attack that impacts a major, or public, system. It tests how well an organisation identifies and mitigates the attack, whilst managing the potential public relations impact of service outages
- **Website Defacement**
  This scenario walks through how an organisation responds to a very public breach such as a website defacement. It tests how well they can identify the issue that led to the defacement, restore systems to working order, harden them from further attacks, and manage the public response.

3 Archway, Birley Fields, Manchester M15 5QJ
0161 513 0960
secarma.com
actnow@secarma.com

The consultant will begin by proposing a realistic scenario that the organisation may face. The delegates will then work through how the organisation would respond to the situation in broad terms, such as what detection and recovery steps the IT team would take, and any public statements or public notification the organisation would decide (or is required) to make.

The exercise will begin with a simple opening statement, then the representatives will work together through the steps of the incident response plan. 'Injects' will be raised at scheduled times throughout the scenario, which include new information to progress the scenario. Examples of each can be seen below:

How Does It Work?

SCENARIO EXAMPLE

- **Opening Statement**

"A single member of staff has reported that their computer has locked and is displaying a message to the effect: 'this machine has been encrypted, to gain access to the files send 0.5 bitcoins to the following address..."

- **Inject Example #1:**

"The number of reported infections has increased to 15 staff members"

- **Inject Example #2:**

"Word of the incident has spread to social media; an anonymous twitter account has reported that your organisation has been 'hacked'".

The scenario will be designed to be realistic, often following through the steps of a previously observed security incident or attack. The team members are encouraged to discuss the plan amongst themselves, but can ask the consultant for clarification on the scenario or wording of the injects.

Exercise Output

At the end of the session, the intention is that the response team will more clearly understand the strengths and weaknesses of their incident response planning. However, notes will be taken throughout the session, and the consultant will produce a formal report. The report will detail issues discovered during the session and how the organisation can improve their preparedness for an incident in the future.