maintel

Cyber Security Incident Response

There is no perfectly safe cyber security system, so breaches are inevitable. This holds true for organisations of all sizes and types, so much so that cyber security professionals often operate in an ***"assumed state of compromise"***. As a result, there's always a need to react to breaches, limit the damage and strengthen defences. In short, every organisation needs a plan B.

If your organisation has been breached, what really matters is how you respond. Incident response is a comprehensive discipline covering everything from containing and eliminating the threat to understanding the event's impact, gathering forensic data, and communicating to stakeholders and participating in legal proceedings. All of these processes need to be done rapidly, precisely and with careful coordination.

What does incident response involve?

Every breach is unique and the nature of the incident will only become clear after the investigation is initiated.

Incidents are also dynamic, evolving events, so an effective response must have immediate access to experts across several diverse competencies. Experienced, multi-disciplinary cyber security partners, such as Maintel, are ideal for the task.

The following are common elements of incident response:

Triage

The team assesses the damage and quickly takes steps to ***"stop the bleeding,"*** including up against an active adversary. This often involves removing malware and recovering data, but the specifics will vary depending on the type of incident.

Containment

Before taking any further steps, the team needs to identify and eliminate the threat so it cannot do further damage to your organisation's system. Whether it's a smash-and-grab attack or a quieter, more sophisticated one involving multiple hidden re-entry points, our team is equipped to get the attackers out and re-establish security.

Post-breach analysis

Determining the root cause of the breach and the way it played out enables you to demonstrate that appropriate security measures were in place. This provides defence against charges that the breach was caused by negligence, including by regulators and civil litigators.

Communication

Most incidents affect customers, clients, and other stakeholders, so it's important to inform them in a straightforward, honest, and timely way. To do so effectively, we work alongside experienced crisis PR professionals where necessary to protect your reputation.

Forensic investigation

Unless careful precautions are taken, important evidence can be destroyed during the triage and containment phases. Our experts preserve data at every step and have the tools and expertise required to work out what went wrong.

Decision making

A breach or attack may just be the beginning of the story. In cases like ransomware attacks, leaders will need to make important decisions, including whether to pay. Our experts can determine what data was taken and consult on the best action, ensuring that leaders have all the information they need.

Legal and insurance cooperation

When a law firm or insurance provider is involved, our experts can perform investigation work, provide expert witnesses, and aid in the investigation.

Our incident response offerings.

If something has already gone wrong, we offer incident response as a service.

For proactive organisations, we also offer incident response on retainer. This takes the panic out, since we'll be ready to help immediately, it can save a number of hours which can significantly impact the damage to a business from a breach. It can also be valuable in any ICO follow-up as it demonstrates that you were aware of the risk and had proactive looked to address the risk to minimise impact.

We also work with our clients to ensure that they are adequately prepared to carry out an investigation and provide effective support should an incident occur.

Why choose Maintel?

Maintel through our partners are a leader in cyber security, and we help organisations of all sizes respond to real-world incidents every day. In addition to incident response, our experience covers all areas of cyber security, so we have a broad, deep understanding of the tactics that attackers employ and how best to counter to them.

Our threat intelligence capability enables us to identify different types of attacks and respond accordingly, and our organisational experience means we can communicate effectively to senior stakeholders.

We have skilled staff at our Security Operations Centre (SOC) around the clock as part of our Managed Detection and Response (MDR) service. This means that whenever you pick up the phone, you'll be talking to someone who is equipped to help.

We approach each incident holistically to address every angle – from triage and containment, to law and reputation management.