wavenet cyberguard

FACT SHEET

CyberGuard

Incident Response:

Expert support at the ready in the event of a major security event

The devastating impact of a cyber security breach on IT systems and organisational reputation cannot be underestimated. When faced with such incidents, a rapid and composed response, backed by expert management guidance, becomes absolutely crucial.

At Wavenet, we have observed that organisations grappling with incidents often experience confusion and panic.

We understand that each incident is unique. With more than 20 years of experience under our belt, Wavenet has encountered a multitude of attack scenarios and keeps up to date with the latest attack trends. By leveraging our comprehensive knowledge and expertise, we are well-equipped to guide organisations through any cyber security crisis they may face.

Our solutions are designed to address the challenges you face when it comes to cyber breach preparation and response.

What is classed as a cyber security incident?

- Website attack
- Data compromise
- Business Email Compromise
- Malware infection
- Ransomware
- Insider threat
- Denial of Service (DOS/DDOS)

Wavenet's Incident Response encompasses comprehensive incident management guidance and support, covering all aspects, from preparation, investigation, containment and eradication to recovery and ongoing mitigation strategies.

Incident Response Service

Wavenet's Incident Response service is a recurring subscription that offers up to £20,000 of specialist resource per annum with pre-arranged terms and conditions for addressing cyber related incidents, anytime day or night. It provides you with immediate access to our CyberGuard resources with priority response times, consequently minimising the overall impact of the security event. As part of the onboarding process and to ensure an effective response, we will carry out a Discovery Assessment. The team will collect the relevant technical and network information and make recommendations around your current incident plan.

Of course we'd prefer that no organisation ever has to experience a cyber security incident, so in the event that you don't need to call on us you can use some of that expert resource on a variety of technical or strategic for example;

- Advisory services including IR planning & tabletop exercises.
- Penetration testing

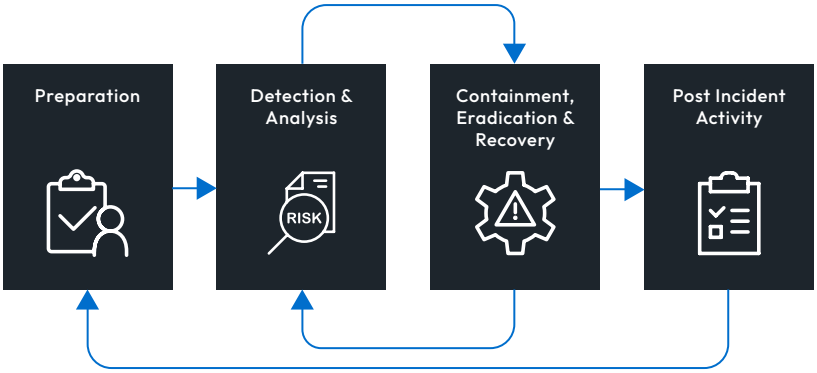
The Incident Response Team will follow our CREST approved methodology.

Preparation: Prepare your organisation by establishing a dedicated incident response team, creating a plan, and identifying critical assets and roles.

Detection and analysis: Continuously monitor for signs of incidents, analyse them to determine their nature, and understand their scope.

Containment, eradication, and recovery: Isolate and control the incident, eliminate its root cause, and restore affected systems to normal operation.

Post-incident activity: Document the incident, review response processes, and update plans while sharing information with relevant parties, lessons learnt.



All Incident Response services include the following stages as detailed below.

Engagement kick-off

- Define the scope of the retainer and identify key stakeholders.
- Establish communication channels and points of contact.

Pre-engagement information gathering

- Collect baseline information about the organization's IT infrastructure, network architecture, critical assets and existing log sources that could be used during an IR engagement.
- Document existing incident response plans, policies, and procedures.

Tailoring the incident response plan (chargeable optional)

- Review and refinement of incident response procedures with key playbooks for common threats
- Full Incident Response Plan creation with detailed scenarios, escalation plans, and a tabletop exercise to test the plan
- Tabletop exercises that simulate a real-world cyberattack scenario, such as ransomware or data breach, testing both the technical and communication aspects of incident response

Why Wavenet CyberGuard?

- Wavenet has more than 20 years' experience supporting organisations of all sizes during cyber breaches.
- 24/7/365 Incident Response access to the experts
- CREST accredited for Cyber Security Incident Response Team (CSIRT) comprising highly experienced cyber security experts who will assist in the event of a cyber security incident with a structured and coordinated approach to managing and mitigating cyber security incidents.
- End-to-end support during the lifecycle of an incident, from discovery and containment through to recovery, lessons learnt. Also Support and advice on some of the non-technical aspects of an IR engagement, e.g. internal & public communications advice, liaising with legal and regulatory authorities

Have you thought about...?

Security Information & Event Management (SIEM)

We can help you better understand your threat landscape and react to threats in real-time, deploying technology that constantly analyses events across your entire infrastructure so that cyber attacks and breaches can be quickly identified, studied and mitigated.

Let's talk

0344 863 3000

enquiries@wavenet.co.uk

wavenet.co.uk

wavenet cyberguard