Tailor Made
TECHNOLOGIES
IT & Communications

Incident Response

Designed by industry-leading cybersecurity experts, Tailor Made's incident response offers organisations rapid reactions against a cyber-attack. Our award-winning team will help your organisation design and set up a thorough incident response plan, to minimise the disruption and damage to the business as a result of a cyber incident.

INCIDENT RESPONSE

Incident response delivers the highest impact on an organisation when deployed alongside a comprehensive cyber threat risk, or impact, assessment.

TMT helps with post-incident investigation by triaging an incident to ascertain what happened, by who, and from where.

Understanding the experience in more detail helps to identify the full extent of the incident: what data was impacted, how much information was accessed or lost, and how many users were affected?

TMT will also help your organisation report any breaches of personal identifiable information ("PII") to the necessary authorities, including the ICO.

Cybercrime is unpredictable by nature, with many complex and varying methods of gaining access to data and systems. Your organisation could be taken by surprise; it is a key requirement of GDPR to have a clear incident response plan in place. TMT helps organisations by investigating all forms of cybersecurity incidents.

Incident response covers compromised user accounts or phishing emails, right through to a full system and network investigation with an advanced persistent threat (APT), via system pivoting.

Organisations are judged by the authorities on how they respond to data breaches and whether they had a plan in place, not by the actual attack that has occurred.

Proactive measures are critical to the organisation's survival. You must demonstrate competency in identifying and remediating incidents when they occur. To minimise the impact of an attack on your organisation, the time between the attack occurring and detection must be as short as possible. The response must be both rapid and thorough, but above all, it is critical to have a prepared and thought-out plan in place, which is communicated and widely understood throughout the organisation.

BENEFITS

GDPR Incident Reporting Timelines - GDPR requires organisations to report potential breaches of PII data in 72 hours or risk significant financial penalties.
Business Risk Mitigation - By having a clear plan, which can be rapidly enacted, you substantially reduce the risk of liability from customers, suppliers, and the authorities.
Compliance Requirements - The NIS Cyber Security and ISO27001 frameworks mandate an incident management process adequate to handle the likely threats faced by your organisation.
Incident Cost Reduction - Not having made provisions for either appropriate cyber expertise, or an appropriate incident response plan, can significantly increase the cost of a cyber-incident which can rapidly escalate to substantial levels.
Minimise Management Time and Panic - Without having a pre-prepared incident response plan very often senior-level management can become consumed by the technical aspects of a breach and overwhelmed by the pressure of customers, suppliers, and other senior stakeholders hampering the response.