CYBER INCIDENT RESPONSE (CIR)

WHEN THE INEVITABLE CYBER -ATTACK OCCURS

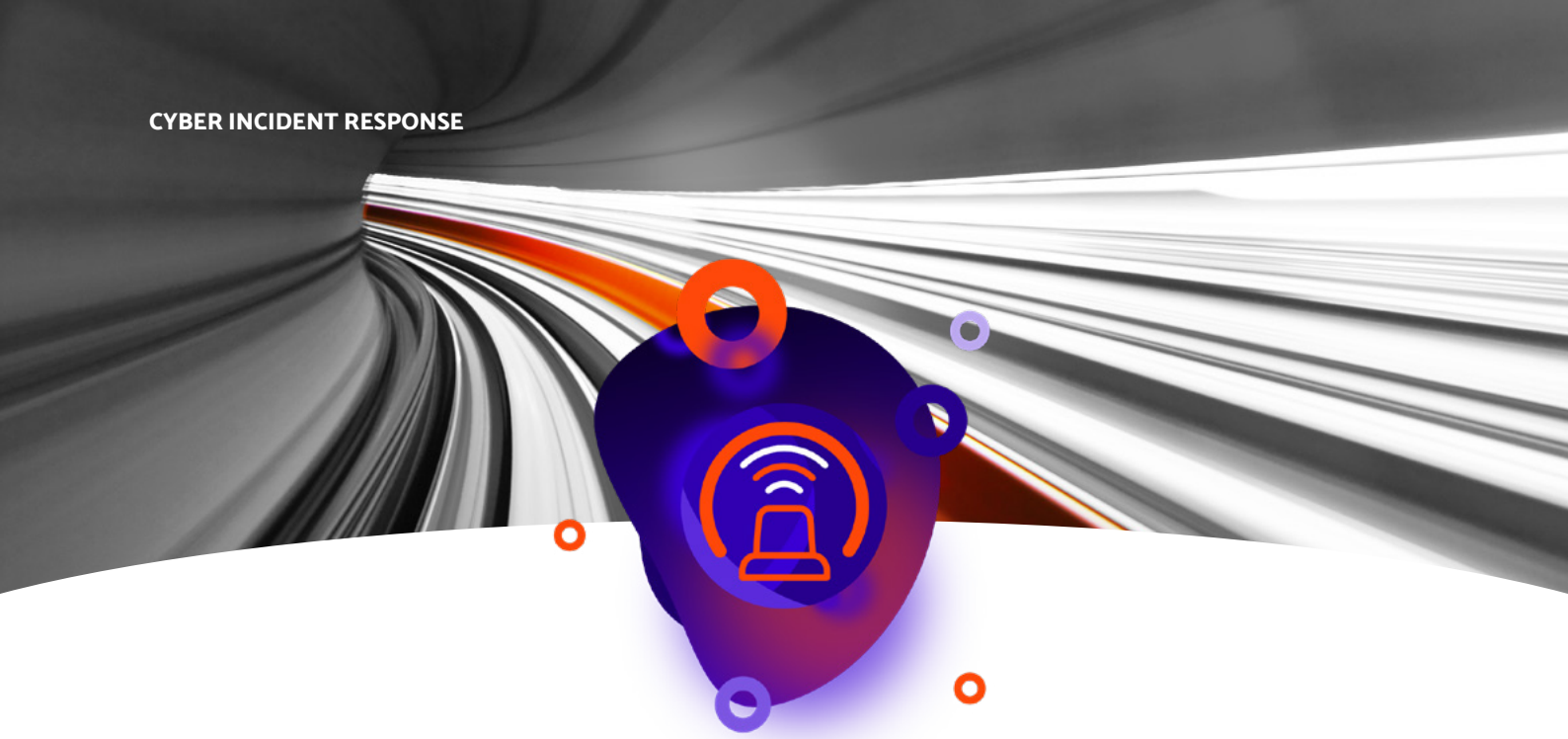
METCLOUD

GET CONNECTED • CYBER SAFE

Official UK Government statistics report that cyber security breaches are a serious threat to all types of businesses and charities.

Among those identifying breaches or attacks, their frequency is undiminished, and phishing remains the most common threat vector. Four in ten businesses **(39%)** and a quarter of charities **(26%)** report having cyber security breaches or attacks in the last 12 months.

Like previous years, this is higher among medium businesses **(65%)**, large businesses **(64%)** and high-income charities **(51%)**.



THE CHALLENGE

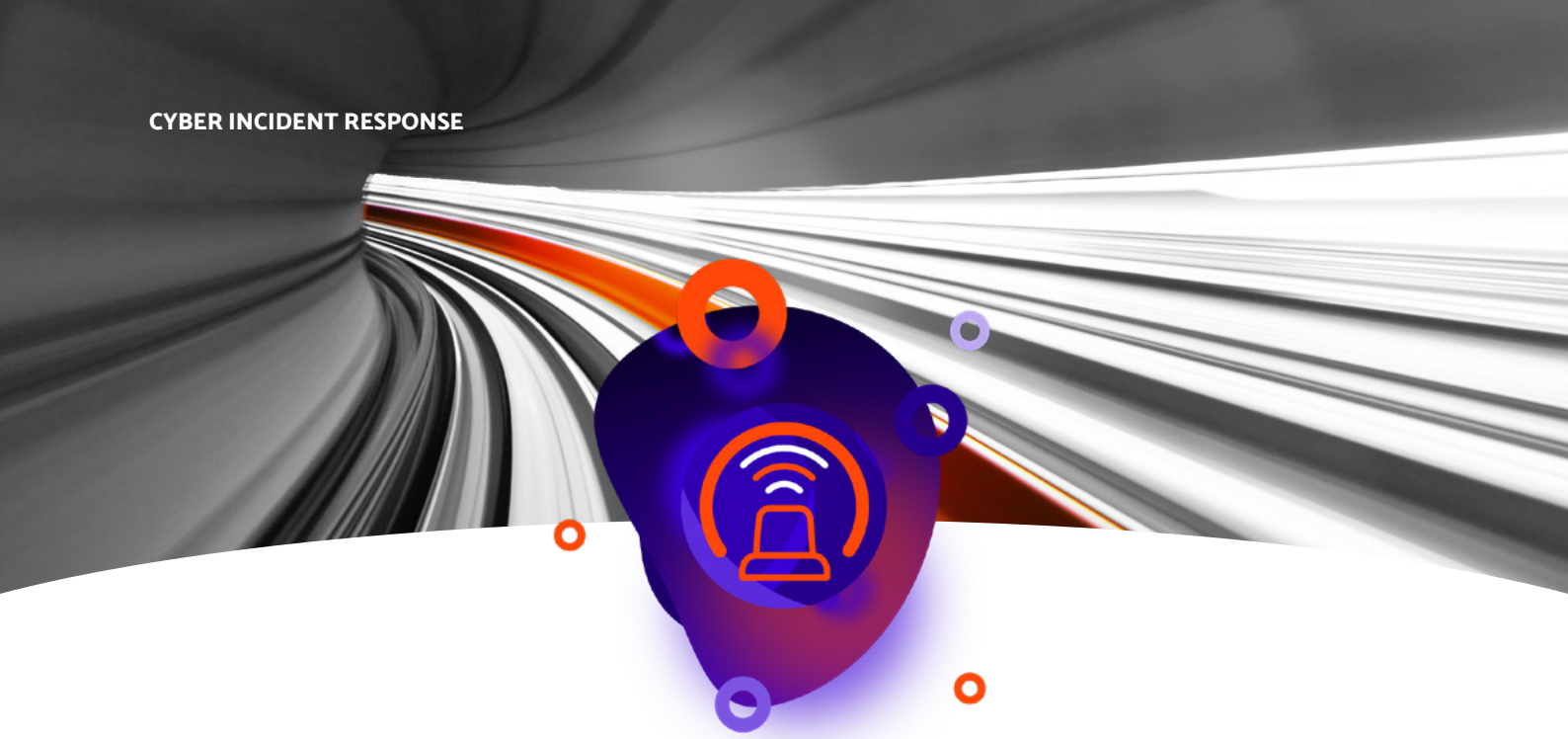
Given the significant rise of cybercrime it has become even more important that organisations have a robust response to cyber-attacks.

The biggest challenge for organisations is the inability to implement efficient cyber security controls, often due to lack of awareness and experience. Furthermore, most organisations do not plan sufficiently and therefore lack an appropriate response capability.

WHY CIR IS VITAL FOR ORGANISATIONS

The absence of a well-tested and rehearsed plan can be detrimental during an actual cyber-attack and therefore a swift response is essential when an attack is identified. It will be essential to fully understand the type of attack, how to mitigate and triage. In parallel the organisation will need to communicate to all key stakeholders depending on the severity and impact of the attack.

Doing all of this in the `eye of the storm' is very stressful and poor decisions will inevitably be made. Cyber incident management and response is a key tool to have in a firm's armoury



KEY STEPS TO MINIMISE THE IMPACT OF A CYBER-ATTACK

STEP 1. PREPARE

Preparation is key: performing a criticality assessment, carrying out threat analysis and addressing issues related to people. Process, technology, and information will get the fundamentals in place. This stage will highlight gaps and vulnerabilities in your current implementation.

STEP 2. PLAN

With the information gathered in step 1 can now be implemented a robust Cyber Incident Response Plan. The plan and associated documentation that should be readily accessible in the event of an incident for instance, a document outlining a firm's response procedure or a list of all relevant internal and external contacts and their details. Appointed individuals will have access to the relevant documents and decide on who these can be sent to, where they are stored and in what format. There can be varying degrees of severity in a disruptive cyber incident and as such it is important to respond in a proportionate manner. Establishing severity criteria or metrics can help inform how quickly an incident needs to be managed, allow the proportionate assignment of resources, as well as the most appropriate escalation path.

Continued...

2.

Roles and responsibilities

It is important to have a governance framework in place and reporting lines in respect of managing incidents are widely understood. Having clearly defined roles and responsibilities, as well as a coordinated approach involving a range of internal stakeholders ensures that in the event of an incident, you can proceed swiftly and effectively.

Board and senior management

Having board-level direction and senior manager accountability for the implementation of cyber incident policies, procedures and response testing can help drive a cyber resilience culture and ensure appropriate oversight.

Incident coordinator

It is useful to identify an individual or a team to be the single point of coordination for response actions and communications during a cyber incident to reduce the risk of conflicting instructions or information from different stakeholders. The coordinator should be an individual available at the time of the incident who is the most knowledgeable, skilled, and experienced according to the type of incident that has arisen.

Subject matter experts

Those staff with specialist knowledge play an important role in offering their expertise in the event of a major incident. Cyber security experts should be consulted during a cyber incident particularly as they should have in-depth knowledge of the firm's information security control environment.

Continued...

2.

Press and PR

These teams are important in managing the incident communication strategy to external stakeholders. Timely, accurate and transparent information provision may be key in protecting the firm's reputation.

Legal

Involving the legal team during the management of an incident can help to ensure all legal requirements and considerations are covered.

Risk and compliance

Can help advise on the risks and help liaise with regulators where necessary.

Business continuity/operational resilience

It is worth consulting relevant business continuity and operational resilience teams in the event of a cyber incident.

HR

To ensure the welfare of staff is protected during an incident (for instance enabling support for any staff affected by an attack or relocating staff to another site).

Finance

Involving members of the finance team can help ensure that the firm has access to emergency funds and be able to allocate resources, such as to independent experts or to rebuild software. Likewise, involving members of these teams can help ensure the continuity of financial management information.

Continued...

2.

Record

Having a nominated individual to document the decisions, timeline and incident response measures taken is also important. Ensuring there is a clear audit trail is of significant benefit when conducting post incident reviews, particularly if firms wish to claim on their insurance. In the event of an incident, timely escalation to the relevant stakeholders and ensuring decision makers authorise and approve putting the response plan into action is essential to mitigate any potential harm to the organisation and your clients. More information can be found on the NCSC's dedicated guidance on building an incident response team.

Build: A cyber security incident response team (CSIRT) - NCSC.GOV.UK

3.

STEP 3. TEST & REHEARSE

It is imperative that you test and rehearse your cyber incident response plan. This will help you iron out any issues. This will also provide significant reassurance to all stakeholders and provide essential evidence to auditors and Insurance providers. The test & rehearsal can be performed as a tabletop exercise bringing together all key stakeholders to run through several likely scenarios and levels of criticality.

Why METCLOUD?

Award winning company for cybersecurity, innovation, and excellence. Our vision is to be the global brand of choice for next generation cybersecure cloud services. Our services have been architected with security by design. Ransomware, Cloud vulnerabilities, Phishing attacks Social engineering and vulnerability management are the five top global security threats. METCLOUD's portfolio of cyber security and cloud services will ensure that you protect, defend, and mitigate any potential cyber attack irrespective of how it was carried out.

Let’s get connected.

Call 0121 227 0730
and speak to one
of our experts.

Email the team.
hello@metcloud.com

Visit our website for
more information.
metcloud.com

METCLOUD

GET CONNECTED • CYBER SAFE

02/2022