CYBER SECURITY INCIDENT RESPONSE SERVICES

CYBER SECURITY INCIDENT RESPONSE SERVICES

Cyber incident response or cyber security incident response services may be called on when an organisation has suffered a data breach, when they suspect they are being actively attacked or have had their IT infrastructure and IT environment critically impinged through a cyber attack.

A common misconception, especially from the board level and the senior management team down, is that cyber attack are just an IT problem and that “We just need IT to deal with it.” But imagine you’ve got an insider who is disgruntled and has taken a copy of your data and is maybe going to take that to a competitor? Or that you have suffered a ransomware attack and your confidential data is at threat of being leaked online?

IT’S NOT JUST AN IT PROBLEM ANYMORE

Human Resources may need to be involved. Your legal team need to be involved. If it’s a data breach, then you’ve got responsibilities within the UK at least, and certainly within the EU under GDPR to inform the ICO the Information Commissioner’s Office of the event.

With cyber incidents, we often see that companies don’t communicate well, either internally or externally. Good comms is critical to deal with any incident, but it’s especially important with cyber incidents. Organisations should use a structured process to identify and deal with cyber security incidents. Over the years, we have observed and assisted many organisations dealing with extraordinary events, many of which had the capacity to abruptly end the company through catastrophic reputational harm, loss of market confidence, crippling regulatory penalties or ensuing litigation.

In almost all cases, those organisations which had taken the time beforehand to calmly consider how they would respond to various incidents and had the courage under fire to stick to their plans and ‘see it through’ were able to survive. In all cases, communication and collaboration were key – communication with external stakeholders, like clients whose data had been compromised and collaboration with regulators who had the power to revoke operating licences, meant that internal and external stakeholders were not left wondering what was happening or what actions were being taken.

IT HAS OFTEN BEEN SAID THAT AN ORGANISATION THAT HANDLES A BAD SITUATION WELL CAN END UP WITH HIGHER LEVELS OF TRUST THAN HAD THE SITUATION NOT OCCURRED AT ALL.

IN THIS DOCUMENT:

- What is a Cyber Security Incident
- Examples of Cyber Incidents
- Why you Need a Cyber Incident Response Plan
- Regulatory Responsibilities for a Cyber Incident
- Consequences of a Cyber Security Incident
- What is a Cyber Incident Response Plan?
- Key Roles in an Incident Response Team
- How Cyber Security Incident Response Services can Help

WHAT IS A CYBER SECURITY INCIDENT

The UK’s National Cyber Security Centre (NCSC) defines a ‘cyber incident’ as:

- A breach of a system’s security policy in order to affect its integrity or availability
- The unauthorised access or attempted access to a system

Part of creating an incident response plan or framework is making decisions around when the process should be invoked, as every organisation is different, there is no one-size-fits-all, and to begin with, it may involve an element of trial and error. To assist, the Core IR Team should apply an assessment criterion to determine the incident severity, and then respond accordingly. The assessment criteria will no doubt change over time.

EXAMPLES OF CYBER INCIDENTS (DEFINED BY THE UK NATIONAL CYBER SECURITY CENTRE):

- **Malicious code:** Malware infection on the network, including ransomware
- **Denial of Service:** Typically a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems.
- **Phishing:** Emails attempting to convince someone to trust a link/attachment.
- **Unauthorised Access:** Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone’s emails or account.
- **Insider:** Malicious or accidental action by an employee causing a security incident.
- **Data breach:** Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).
- **Targeted attack:** An attack specifically targeted at the business – usually by a sophisticated attacker (often encompassing several of the above categories).

WHY YOU NEED AN CYBER INCIDENT RESPONSE PLAN

Cyber attacks are becoming more common and data breaches are inevitable, organisations of all sizes are at risk, with the National Cyber Security Centre reporting that **38% of surveyed SMEs experienced a breach or attack in 2021**.

With the shift to remote working and more services now being used in the cloud, cyber attackers have an increased attack surface to target and unfortunately, only need to be lucky once.

Often attackers will want to leverage the stability that they get of access to systems over a long weekend, for example, like a bank holiday where they'll attack the network on Friday evening. And then they've got all day Saturday, Sunday and Monday, potentially to completely compromise the network and reduce your ability to recover and remediate.

The core to managing an incident is to think calmly and carefully before an incident occurs about the various scenarios that you may encounter, that you may need to think about and prepare some plans in order to respond.

Having a simple, concise plan will allow you to respond quickly and effectively.

REGULATORY RESPONSIBILITIES FOR A CYBER INCIDENT

You may need to report incidents to stakeholders, such as regulators, insurers, or customers. Under the UK GDPR, personal data breaches likely to result in a risk to the rights and freedoms individuals must be reported – within 72 hours of becoming aware of the breach – to the Information Commissioner’s Office (ICO). The ICO takes a particularly dim view of organisations that try to cover that up and not be transparent and disclose what’s going on.

So obviously, you’ve now discovered this data breach event. Data has left the company and the clock is ticking. You’ve got 72 hours to do something.

What happens if you get a phone call from mainstream media or from a computer news website and they say:

"Hey, we heard that you guys have had a data breach event. We found some of your data on the dark web."

Is your organisation prepared with a communication strategy, a PR statement or something that you can put out into the media to say:

"Yes, we're aware we've seen it's happened. We've engaged with a company that's helping us remediate and understand, and we're dealing with the appropriate regulatory authorities."

Most small companies, certainly in the UK, are completely out of their depth in dealing with these kinds of incidents.

CONSEQUENCES OF A CYBER INCIDENT

Costs Incurred for Detection & Response to Malicious Activity

- Digital forensics and investigative activities
  - Specialist external 3rd party investigations for root cause analysis, assessment, and audit
- Crisis management and specialist incident response teams

Lost Business Opportunities

- Lost revenue from downtime of core servers, services, and systems
- Business disruption due to telephony and email systems being disabled
- Lost customers due to poor reputation

Communication & Notification

- Obligations and duties under data protection
  - Emails, letters, outbound calls to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement with outside specialists

Post-breach Responsibilities

- Customer service desk and inbound communications from customers (due to high volume of data protection requests or complaints)
- Provision of credit monitoring and identity protection services to impacted customers
- Legal expenditures & regulatory fines

CONSEQUENCES OF A CYBER INCIDENT

Cyber incidents can have far-ranging effects on an organisation, and there can be numerous, often unexpected consequences. Damages incurred could be financial, operational, or reputational.

This excludes cost of the ransom, loss of intellectual property, or any monies loss due to irrecoverable fraudulent payments.

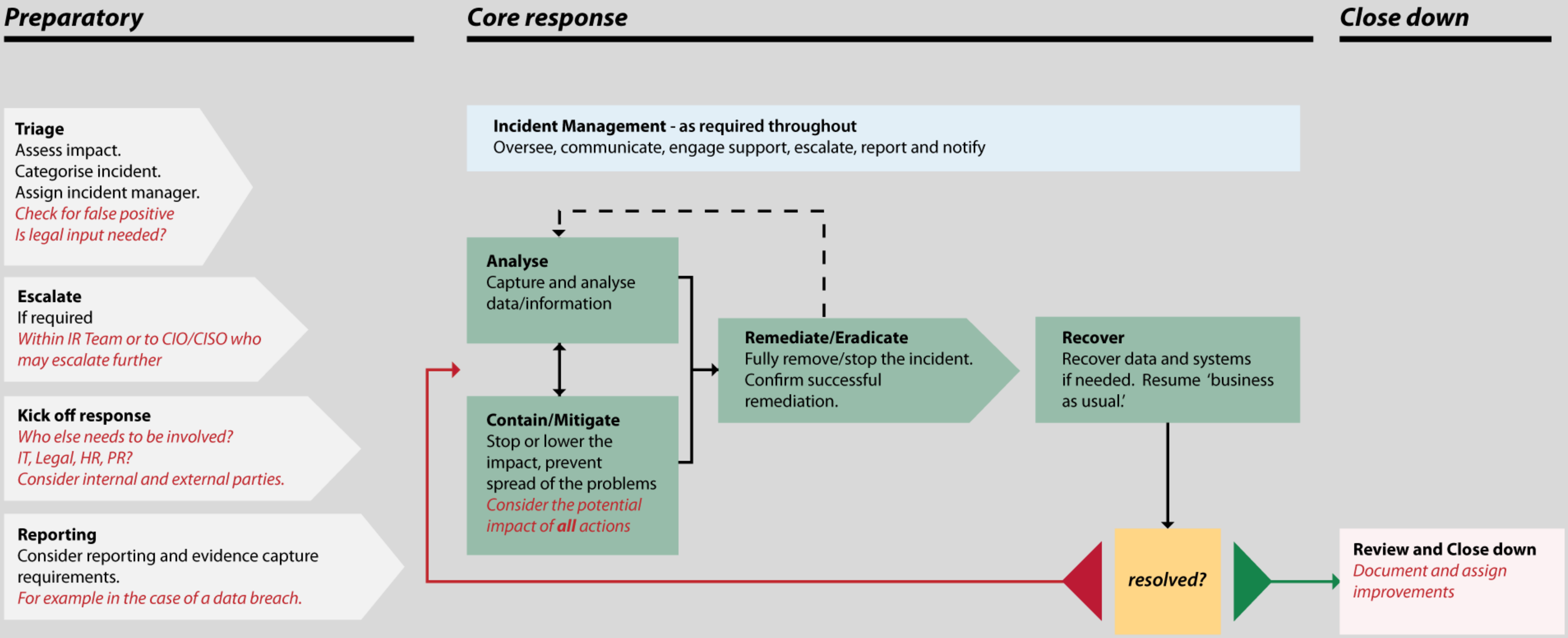
A significant portion of the total cost could come from lost business opportunities, which can be caused by web facing applications, services or payment systems being taken offline, server downtime, telephony or email systems being disabled, through to staff having to remediate the effects of the breach, rather than working on their usual daily activities.

WHAT IS AN INCIDENT RESPONSE PLAN?

An incident response plan is a process that allows organisation to effectively respond and recover from cyberattacks. The plan should be documented, understood, and regularly rehearsed.

There is no one team or department that can manage all aspects of an incident in a modern company. The interconnected nature of everything we do revolves around communication and information flow, and the IR process is no exception.

Steps and processes will vary depending on whether an industry standard incident response framework has been adopted but will usually include; detection and analysis, capture of relevant data/information, containment/mitigation to prevent the spread of the problem, remediation and eradication to stop the problem, recovery of data and systems, review findings and take action to ensure it won’t reoccur.



Preparatory
Core response
Close down
Triage
Assess impact.
Categorise incident.
Assign incident manager.
Check for false positive
Is legal input needed?
Escalate
If required
Within IR Team or to CIO/CISO who may escalate further
Kick off response
Who else needs to be involved?
IT, Legal, HR, PR?
Consider internal and external parties.
Reporting
Consider reporting and evidence capture requirements.
For example in the case of a data breach.
Incident Management - as required throughout
Oversee, communicate, engage support, escalate, report and notify
Analyse
Capture and analyse data/information
Contain/Mitigate
Stop or lower the impact, prevent spread of the problems
Consider the potential impact of all actions
Remediate/Eradicate
Fully remove/stop the incident. Confirm successful remediation.
Recover
Recover data and systems if needed. Resume 'business as usual.'
resolved?
Review and Close down
Document and assign improvements

Example of an Incident Response Workflow (source: UK, National Cyber Security Centre)

KEY ROLES IN AN INCIDENT RESPONSE TEAM

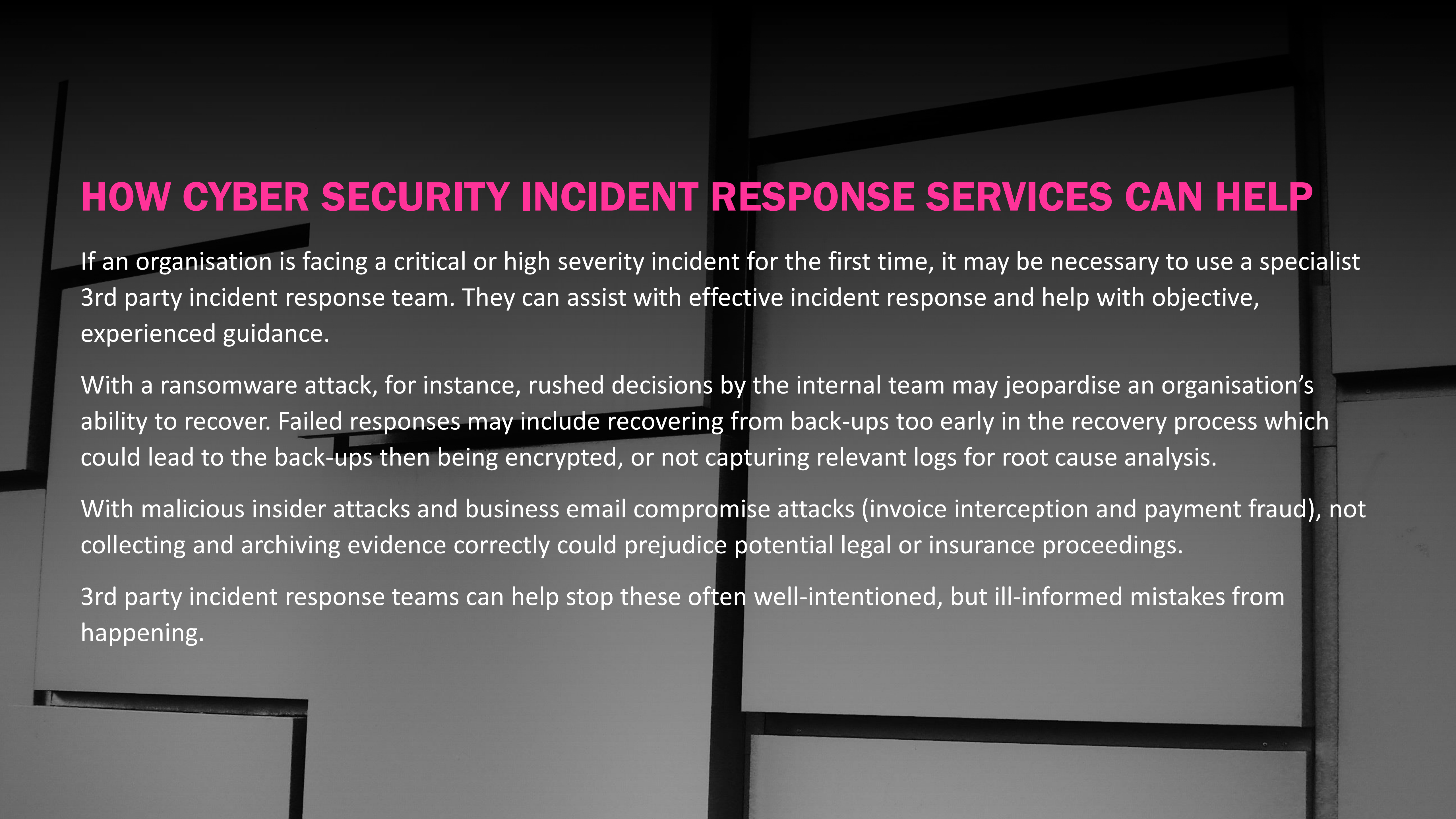
When any incident happens, there’s a core group of people that need to be involved, and that’s what we refer to as the core incident response team. That typically involves a member of the board or at least the senior management team. And typically, they’ll come in as an observer. We don’t necessarily want that person to run or manage the incident. Will want someone from legal because they’ll need to take a view on the company’s legal position in response to the incident.

And it may be the case that they need to have outside or external communications with the firm’s legal solicitors so that they can get additional advice. If we’re talking about an incident that they’re not necessarily familiar with around the legislation or the regulatory requirements that are relevant. Facilities may need to be involved.

So what’s happening with the building. For example, with a data theft event, it may be the case that the attackers had physical access to your building. In which case you need to be looking at the data around card access systems.

A composition of the Core Incident Response Team, may be as follows:

- Board Representative or CEO/CFO
- Director for Regional Operations
- Technical Services Director
- Head of Legal & Compliance
- Head of Internal Audit
- Head of IT & Cybersecurity
- Head of Human Resources



HOW CYBER SECURITY INCIDENT RESPONSE SERVICES CAN HELP

If an organisation is facing a critical or high severity incident for the first time, it may be necessary to use a specialist 3rd party incident response team. They can assist with effective incident response and help with objective, experienced guidance.

With a ransomware attack, for instance, rushed decisions by the internal team may jeopardise an organisation’s ability to recover. Failed responses may include recovering from back-ups too early in the recovery process which could lead to the back-ups then being encrypted, or not capturing relevant logs for root cause analysis.

With malicious insider attacks and business email compromise attacks (invoice interception and payment fraud), not collecting and archiving evidence correctly could prejudice potential legal or insurance proceedings.

3rd party incident response teams can help stop these often well-intentioned, but ill-informed mistakes from happening.

CYBER SECURITY INCIDENT RESPONSE SERVICES

If you have a cyber security incident, believe you are under attack or have been compromised, then call us immediately for assistance on +44 (0) 207 193 4905 or email us at incident@first-response.co.uk

Pro-active services First Response provide include:

- Cyber Security Incident Response Preparedness
- Managed Endpoint Detection and Response
- Managed Security Operation Centre

ABOUT FIRST RESPONSE

Established in 2013, First Response is a cybersecurity, digital forensics, and incident response company. Working with SMBs, SMEs & MSPs to protect their organisations and accelerate cybersecurity maturity. This is through outcome-focused consultancy and services incl. managed cybersecurity services (endpoint, network, mobile & cloud), and secure infrastructure design.

Our technical specialists comprise respected security and investigative professionals from a diverse set of backgrounds, including police cyber-crime units, the security services & enterprise network specialists.

We are headquartered in London with offices in Manchester and Rome, from where we assist our clients around the world. We also help organisations navigate the complex issues surrounding systems breaches, server compromises and data loss. Working with a wide variety of clients including banks, law firms, energy & manufacturing companies and public sector bodies.

Contact

Email: info@first-response.co.uk
Tel: +44(0) 20 7193 4905
Web: https://first-response.co.uk/

first
response