bsi.

...making excellence a habit.™

Preparing for a breach

Steps to creating an effective incident response plan

Whitepaper

Executive summary

This whitepaper explores the best practice around preparing, responding and reviewing before and after a cyber incident, which can help limit the duration, impact and associated costs that a cyber-attack can have on an organization. .

According to the UK Government nearly half of UK firms were hit by a cyber breach or attack in the last year, as such it is vital that all organizations have a suitable incident response procedure in place.

This whitepaper describes what incident response is, why it is important for businesses and how it can affect your organization. It also details the phases that encompass the whole incident response stream.

Incident response

Incident response is defined as the "capability to effectively manage unexpected disruptive events with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits." A well-defined procedure should ensure that there are suitable resources and personnel to deal with any event. This procedure will allow the business or organization to continue to operate with minimal disruption.

The process will vary depending on the size and the resources available within an organization. A small company without an internal IT department would gain from a fully outsourced incident response capability, with contracts in place with a third party to ensure that incidents are dealt with in a timely manner. Larger organizations should have at minimum the following items in place:

- Perform a threat assessment of the organization to identify key threats and asset targets
- Incident response plan defined and regularly reassessed
- Appropriate security infrastructure
- Detailed and centralized logging
- Play/run books providing the key steps for dealing with the most probable incident types

Cyber incidents vary due to the source of the incident e.g. from a single criminal element through to an advanced, state sponsored attack, rather than the type of attack e.g. hacking, phishing attack.

The CREST Incident Response guidelines defines incident response management as three phases:

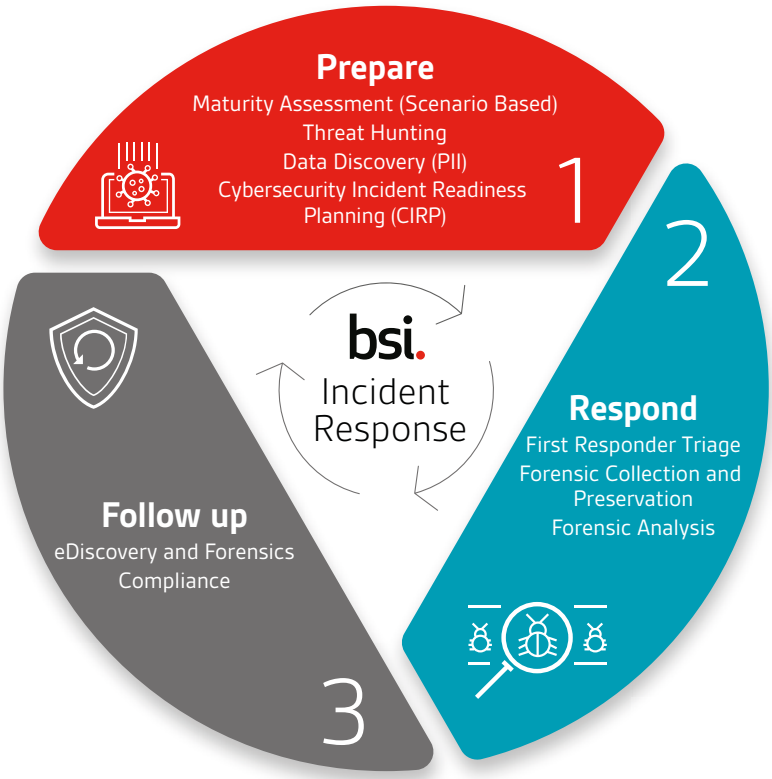
- **Prepare**
- **Respond**
- **Follow up**

In the following sections, we will outline the key activities in each of these phases and detail the implications to an organization.

Why is incident response important?

Cyber attacks are becoming more frequent, with the compromise of personal and business data typically targeted, it is vital that the capability to respond quickly and effectively is available. By having a defined incident response capability, it allows an organization to respond systematically, using a consistent methodology to ensure that all of the appropriate tasks and actions are performed.

Having a policy and process helps to minimize loss or theft of information and disruption of services caused by incidents. With the appropriate incident logging and documenting, a defined process gives the ability to use the information gained during incident handling to better prepare for future events.



Prepare

The prepare phase is typically seen as the most important as it defines the process to deal with an incident, but more importantly it should aid the prevention of incidents by identifying weaknesses in an organizations systems, networks and applications.

Key sub-activities that occur in the prepare stage, using internal teams and/or external support include:

- **Maturity assessment:** assessment of the status of an organization's cybersecurity incident response capability
- **Threat hunting:** performing proactive "hunts" through networks for indications of malicious activity and software
- **Data discovery:** identifying and prioritizing key data flows and assets
- **Cybersecurity Incident Readiness Planning (CIRP):** review existing operating procedures and environment to ensure that in the event of an incident there is sufficient information and processes in place to contain the incident in a timely manner, minimizing impact

The prepare phase should ensure that key assets are identified and what the likely attacks against the assets are. A threat analysis assessment should be preformed to identify the primary attack vectors that could be used against each critical asset.

An organization should have the appropriate level of skilled personnel, software and hardware to deal with the various types of cyber incident.

Logs are essential to most investigations and as part of the preparation regular reviews should be performed to ensure that the level of logging, sources of log data and the log retention levels are sufficient to provide the level of detail required.

The final element of preparation is to ensure that an organization has a well-defined, regularly reviewed, and practised methodology for dealing with the various types of cyber-attacks. The methodology on a simple level could just ensure that evidence preservation is performed, and that a contracted third party is engaged, with the named contact details easily available for incident escalation. Larger organizations may wish to develop full run-books and processes for different types of incidents.

Remember that data breaches are not always big events – sending an attachment to the wrong person may be a data breach. Does your organization have a response plan in place if a sensitive document is sent to the wrong person?

BSI's Cybersecurity and Information Resilience team frequently deal with incidents involving Microsoft Exchange. By default most organizations do not have Mailbox Auditing enabled for mailboxes. This often leaves the Incident Response team with only limited information to base their analysis on, minimizing their ability to fully understand what actions an attacker took. Enabling enhanced logging such as this, especially for high value systems and users, greatly improves the ability to respond effectively to an incident.

Respond

An organization's ability to respond efficiently and effectively will be greatly improved by having completed adequate preparation in advance. Following a practised and well known response plan will aid the responders in successfully identifying and responding to any incident rapidly.

Key sub-activities that occur in the respond stage, using internal teams and/or external support include:

- **First responder triage:** determining scope and whether any specialist resources – including third parties will be required
- **Forensic collection and preservation:** correctly capturing and preserving relevant evidence in a forensically sound manner
- **Forensic analysis:** conducting forensic analysis activities to uncover the true cause of an incident, its scale, and its impact

The first step to responding to an incident is to clearly identify it. Organizations will need to determine the type of incident, the extent of it, the magnitude of the problem and the systems and data at risk.

Correctly identifying the scope and scale of an incident is key to ensuring it is contained. Technological solutions are often vital in identifying incidents. Solutions related to log analysis and monitoring; data loss prevention systems, anti-virus systems, firewalls, and others can be utilized to identify the scope of an incident. Companies are often better at collecting and storing logs than analysing their content. To bridge this gap, cloud-based security-as-a-service (SaaS) solutions offer an effective way to ensure log file content and security alerts are correctly identified and classified on a 24x7 basis, which may not be possible for a company to manage internally.

Adequate training for IT help desk staff is often crucial to identifying incidents. They need to be aware of suspicious indicators, fraud and impersonation attempts, and red flags to suspicious activities, for example accounts being locked out.

When an incident is suspected, the key responders as defined in the incident response plan should be assembled. This team will need to define the objectives and investigate the incident. They will need to quantify the who, what, when, where and why of the attack.

It can be helpful to break down the investigation into parts. Firstly, the incident should be classified to determine whether it is critical, significant, or negligible impact. It should be prioritized then as a high, medium or low priority, and on the back of this the investigation should be assigned to the appropriate personnel based on the impact and priority determined.

First responders will then seek to collate relevant data sources, such as log files, documents, computers, laptops, servers, and other relevant material from systems believed to be in scope. They should have the necessary skills and knowledge to perform a quick analysis of each collected data source to find evidence of the incident, the data at risk, and the actions of the attacker.

Once the analysis has identified likely steps taken by the attacker, remedial actions should be taken to lock out the attacker. This could be achieved by steps such as locking out affected user accounts, changing user and system passwords, blocking IP addresses or websites, or in certain circumstances shutting systems or services down.

Once an attacker has been locked out it may be necessary to recover affected systems. In the case of data loss, this may mean restoring systems from backup to a clean state before the incident. For compromised user accounts, this may entail changing passwords and permissions. In the case of an exploit of a vulnerable system, patching or updates may recover the system from the incident.

Follow up

A thorough and complete post-mortem of any incident is considered best practice.

Typical sub-activities that occur in the follow up stage, using internal teams and/or external support include:

- **eDiscovery and forensics:** leverage technology and procedures to fully support organizations in facilitating an efficient review of electronic evidence
- **Compliance:** ensure all relevant mandatory obligations are maintained, for example any reporting under regulations such as the EU GDPR or NIS or similar mandates

First responders will typically attempt to triage the most important records and logs only to identify the scope of an incident while it is still a live threat. Once it is determined that the attacker has been successfully locked out and the recovery process has been completed then time will usually permit a more in-depth analysis.

Typically the goals of a follow up analysis will be to:

- Identify the root cause of the incident
- Verify that all compromised systems were correctly identified and recovered
- Quantify and analyse the affected data
- Assess affected data to determine if there are any legal obligations arising from the incident

A thorough analysis of the root cause should identify a number of improvements to minimize the chance of a reoccurrence or another incident occurring. Lessons learned should be quantified; an action list of improvements created and assigned to stakeholders, and the details should form part of the next iteration of the "prepare" phase of incident response planning.

Particular attention should be focused on legal obligations in the event of a data breach. The new GDPR rules have a requirement to report a data breach to the data protection authority within 72 hours of becoming aware of any breach. The follow up process therefore has only limited time to quantify if such a notification is required. It should be noted that not all of the answers in relation to how an incident occurred or a full clarification on what data was breached is necessary within the 72 hour window. If it is suspected that some Personally Identifiable Information (PII) was breached then a company should notify the data protection authority in their jurisdiction within the 72 hour window. A follow up report detailing the full details of the incident can follow once this has been completed. Working closely with the data protection authority and opening a channel of communication with full disclosure throughout the investigation as early as possible will minimize the chances of punitive fines being imposed.

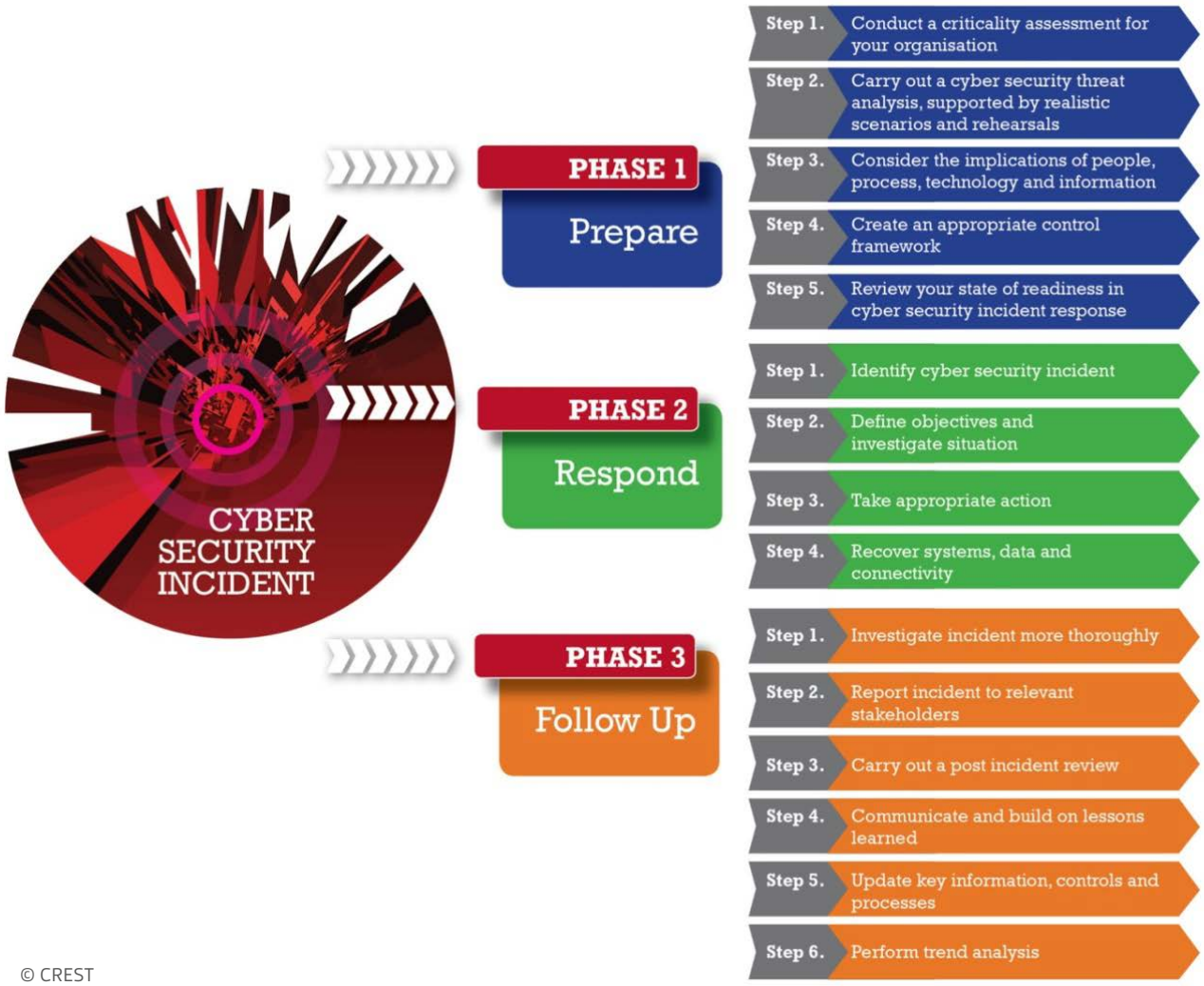
Quantifying breached data and analysing it to identify PII can be a difficult task. Breached data can be large in size and can come from mixed or unstructured data sources. In order to analyse and review this data in an effective and efficient manner specialist tools may be required. eDiscovery and Digital Forensic tools can be useful in this regard.

BSI utilizes many such products, in particular the Nuix Investigator Workstation software can be used to identify patterns of information such as names, addresses, phone numbers, financial data, and others within data. The Veritas eDiscovery Platform contains a detailed information classifier engine to help identify PII within processed data. Many other software products are also available which can accomplish similar results. BSI can assist organizations who wish to utilize software platforms such as these.

Recommended resources

CREST

CREST is a leading international body providing guidance and best practice in the field of information security. BSI follows the CREST methodology for Incident Response, which is summarized in the graphic below:



The CREST website contains an Incident Response Maturity Assessment tool that many organizations may find helpful to assess their internal capability and response to a data incident. This is available at http://www.crest-approved.org/cyber-security-incident-response-maturity-assessment/index.html and is free to download.

Conclusion

Incident response will inevitably grow as an area for companies to deal with. In the past organizations have often only thought of incident response when an incident is uncovered. This can lead to a panicked, incomplete, and inefficient response. In much the same way that disaster recovery planning has become adapted by organizations, so too should incident response planning. Processes, walkthroughs and drills will all help the response. When an incident does occur, following a clear methodology will ensure the quickest and best response is achieved. A thorough follow up will then ensure all regulatory obligations are met, and feed back into a better plan for the next event.

Case Study – Office 365 Incident

Office 365 account login had been compromised and upon investigating the account it was observed that an auto-forward of all incoming email to a third party address had been enabled by the attacker.

We assisted the client to respond to the incident. Log files from Office 365 were extracted and examined. The scope of the incident was determined to be ten user accounts. Analysis of the log files confirmed the start date that the forward was implemented. Additionally examining the emails received during this time identified phishing emails which were the most likely source of the attack. The accounts were secured by a reset of the password.

Our team then focused on the follow up to the analysis. Recommendations were made to enable two-factor authentication for Office 365. Server side rules were also implemented to prevent forwarding of emails to third party domains. The sender of the phishing email and the domains lined to from the email were blocked for all users. A programme of end user awareness training on spotting phishing emails was also implemented for all users.

However, a big challenge for the follow up for this incident was to identify if any PII was in the breached data. We took a copy of the affected mailboxes and processed the data using Nuix Investigator Workstation and the Veritas eDiscovery platform. The volume of data was substantial, with almost 250,000 unique documents identified.

Utilizing these powerful platforms allowed us to perform extensive searches to isolate PII within the dataset. Data such as names, addresses, and phone numbers were identified. Searches were also performed to attempt to identify more abstract issues such as financial, health, sexual orientation, trade union membership, and other information classes that would be considered sensitive. The Veritas eDiscovery platform allowed the client to review the relevant documents directly, further classifying the breached data and extracting redacted versions for reports.

A thorough investigation such as described above is essential to demonstrate to the data protection authority that the incident was not only resolved, but the consequences and data lost was comprehensively reviewed.

BSI Cybersecurity and Information Resilience

BSI Cybersecurity and Information Resilience helps you address your information challenges. We enable organizations to secure information, data and critical infrastructure from the changing threats that affect your people, processes and systems; strengthening your information governance and assuring resilience. Our cyber, information security and data management professionals are experts in:

Cybersecurity

Penetration testing, vulnerability management, incident response and cloud security services

Security awareness

Phishing and user awareness training, online solutions, social engineering and simulation testing

Information management and privacy

Information risk management, privacy, data protection, eDiscovery and forensics

Compliance and testing

PCI DSS services, Cyber Lab testing and product and software assessments (CC, CAS-T/CPA)

Our expertise is accredited by:

CREST

PCI Security Standards Council QUALIFIED SECURITY ASSESSOR

CYBER ESSENTIALS

CREST STAR

CHECK IT Health Check Service

Find out more

UK

Call: +44 345 222 1711
Email: cyber@bsigroup.com
Visit: bsigroup.com

IE/International

+353 1 210 1711
cyber.ie@bsigroup.com
bsigroup.com

bsi.