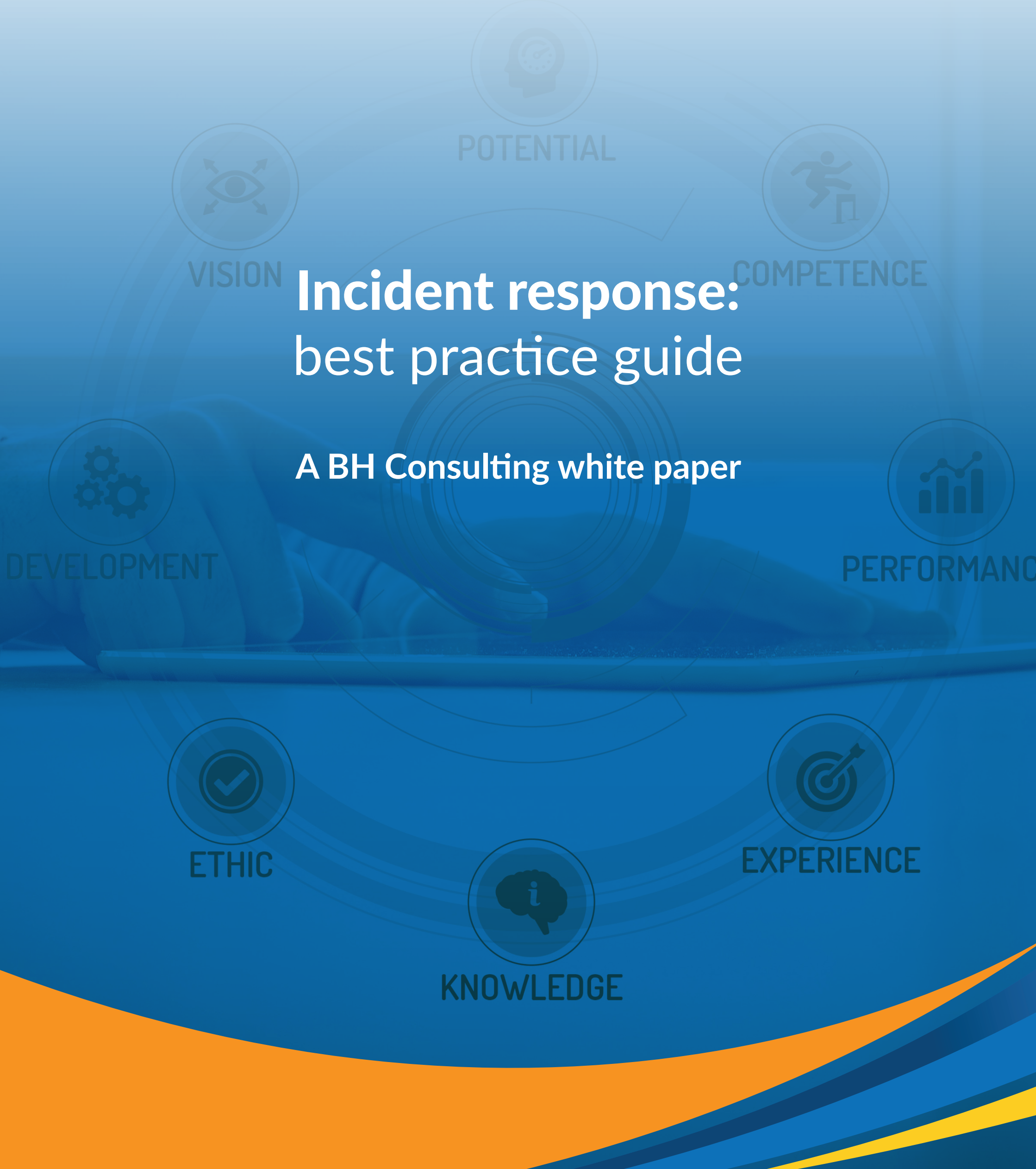
BHConsulting
Your Trusted Cybersecurity Partner



Incident response: best practice guide

A BH Consulting white paper

About this guide

Security incidents, malicious attacks, hacks, system compromises, and data breaches are, unfortunately, regular occurrences; a risk of doing business. This is not hype or fearmongering. Every year, data theft and cyberattacks rank among the top 10 most likely risks in the World Economic Forum's annual Global Risks Report. Ireland's National Cyber Security Centre's guide for businesses puts the issue even more starkly: "It's no longer a question of if your company will be breached, or even when, it's likely to have happened already. The real question is whether you will know and are you prepared?"

Which brings us to the purpose of this white paper. By starting from the premise that incidents will happen, then it follows that our response becomes critical. In today's connected world, disruption to normal operations has a financial cost, a human resource cost and a business opportunity cost. Good incident response planning can help to minimise the impact of a security incident and ensure continued operations, even in a limited capacity.

Timely incident response has also become necessary in light of the General Data Protection Regulation, which requires all organisations to report certain types of personal data breach to the relevant supervisory authority – and where feasible, to do so within 72 hours of becoming aware of the breach.

In the past, business continuity planning and disaster recovery used to fall onto the shoulders of the IT or security professional. But cyber risk is a business issue and needs management ownership, along with buy-in from all departments. Whether for compliance or operational reasons, incident response now belongs at the table of an organisation's senior leadership or board.

The culture of security has evolved; victim blaming is mostly a thing of the past, and few people point fingers at those who had the misfortune to suffer a security incident. Sympathy is in far shorter supply, however, for any organisation that knew the risks and failed to prepare for them. Accept the fact that you may be attacked and plan for that eventuality. Know how you will respond in advance, identify key stakeholders, and test multiple scenarios. The worst time to check if a response plan is robust is in the middle of an incident.

This white paper contains advice to help to guide organisations of all sizes to build strong incident response capacity for whatever risks may occur.

Why is incident handling and management necessary?

Security is only as effective as the response it generates. Having a structured response process ensures any incident is recognised early and dealt with swiftly and appropriately. Failure to respond to an incident in a timely manner can expose an organisation to many issues including:

- Disclosure of confidential information
- Prolonged recovery times due to more extensive damage as a result of the ongoing incident
- The inability to proceed with a criminal or civil case due to lack of evidence or inadequate evidence gathered
- Negative impact to the organisation's image in the eyes of shareholders, customers and/or partner organisations
- Potential legal and/or compliance issues depending on the regulatory and legal requirements
- Exposure to legal cases from third party organisations impacted by the incident
- Exposure to legal/libel cases from employees/individuals who may have been dealt with unfairly by an inappropriate and/or cumbersome response

An organisation that has a structured and formalised response in place to internal and external IT security incidents shows that it takes its corporate and legal responsibilities seriously and has a positive security posture. This security posture ensures that the organisation can deal with security incidents quickly, efficiently and effectively.

This will result in:

- Rapid and accurate assessment of security incidents and the most appropriate response
- Shortened recovery times to incidents and minimised business disruption
- Confidence to proceed with a disciplinary, legal or civil case as a result of using proper procedures and processes to gather evidence in response to an incident
- Compliance with local legal, regulatory and industry requirements
- Potential reduction in incidents as the organisation is not considered a "soft target"
- Accurate reporting and statistics to keep improving the organisation's security

People and processes

Involving the proper people and processes is key to developing and implementing an appropriate incident response. Some incidents will simply require no response; others will require only an automated response, e.g. drop a connection to a blocked port on a firewall; whereas others will require a more complicated response involving personnel from various parts of the organisation and different levels of management.

It is important to establish the appropriate levels of response to an incident and also that the incident response has the necessary levels of authorisation and autonomy. There is no point involving senior management in responding to an incident that has minimal business impact.

All personnel involved in responding to an incident must be properly trained and versed in their responsibilities. If the skills are not available in-house then they should be sourced elsewhere. In addition, you should test all policies and procedures regularly to ensure their effectiveness and applicability. Carry out table-top exercises and scenario planning to find out in advance how well your team works when an incident occurs.

There should also be a review process in place to capture lessons from any incidents that require a response. Failure to take these steps could adversely impact business operations leading to loss of revenue or mission effectiveness, legal ramifications, or a loss of public trust.

The incident response methodology will depend on the incident classification. The response team will also need to confirm that the incident has occurred and, if so, decide the most appropriate response to it. Once an incident has been confirmed and the appropriate incident response process begins, you must take all care to preserve and record all information and potential evidence in the event of a legal or civil case.

The type of response required to an incident will depend on a mixture of business and technical drivers, as it can impact on the employee, customer, and public relations and may even have legal ramifications. Therefore it is essential that clear, concise and accurate processes and procedures that have been approved by senior management are in place for all personnel to follow.

Many incidents may happen outside office hours or when key personnel are not immediately available, so all staff must have clear guidelines in how they report and respond to incidents.

Many incidents may simply require an automated response. For example, if the organisation’s security software detects known malicious software in a file, it could automatically delete it without needing any further response. However, an attack on the firewall will require a more measured response and may require the involvement of senior management to decide whether to shut the firewall down to minimise the damage – or allow the attack to continue in order to gather further evidence for a possible legal case.

You should keep an Incident Response Log which accurately records all actions and results of those actions. This should include details as to who completed the actions, the time of the action, and the outcome. This ensures an exact record of all action is taken in the event that the incident leads to a civil or criminal court case, or indeed these logs can be used to determine the effectiveness of the incident response procedures.

Assembling an incident response team

The incident response team is responsible for managing the organisation's response to an incident and how the organisation interacts with third parties such as law enforcement agencies, regulatory bodies, customers, employees and the media.

The team should comprise a number of people with knowledge and skills in different areas. It may be necessary to source certain skills externally to the organisation. For example, forensic gathering skills are not commonplace and are often better sourced from vendors who specialise in this area. If this is the case, then there should be a formulated process in place to ensure that the resource is available when required.

The incident response team should also have the full backing and support of senior management. This should include giving the incident response team the autonomy and authority to make decisions and carry out actions in the absence of senior management during a critical incident.

Typically an incident response team will include representatives of the following areas of a business:

IT security

The core team members will be those from the IT security team as they are the most knowledgeable about managing and dealing with computer security incidents.

IT operations

The IT operations team are very often the first line of defence/detection of incidents either via monitoring tools or from reports to the support desk, so it is essential that a representative from this team is on the incident response team. Their knowledge of the organisation's data storage systems and network may be critically important.

Facilities management

It may be necessary to involve the physical security or facilities management team in responding to an incident where there has been physical access to compromised systems, and the organisation may need to recover breach evidence from CCTV or swipe card systems.

Human resources

It is essential that a representative from the human resources team is involved in the incident response team because a data breach could involve staff data, or because a member of staff may have caused the breach inadvertently or deliberately. The result of an incident response may involve disciplining a staff member for breach of the organisation's acceptable usage policy; if so, this will require the HR team's input to ensure due process. HR representation also ensures that the response team's processes and procedures comply with good HR practice and do not impinge on industrial relations.

Legal department

As with the HR department, it is imperative to take legal advice both during the development of the processes and procedures and in responding to serious incidents. Legal input may also be needed if there is an obligation to report the incident to a regulator.

Public relations

Communicating information to the public, customers, partners, shareholders and press is a unique skill and one that is necessary to ensure the right amount of information is disclosed at the right time to the right people.

External expertise

Depending on the nature of the incident, you may need to call on external expertise. For example you may need external expertise in computer forensics or criminal investigations if those skills are not available in-house.

Note: depending on the seriousness and impact of an information security incident, it may be necessary to mobilise all or only part of the information security incident response team.

Once the team is in place, it should:

- Develop/review the processes and procedures that must be followed in response to an incident
- Develop/review guidelines for incident classification. This should not be solely the responsibility of the Incident Response Team but must involve the business owners responsible for the systems and data being protected
- Manage the response to an incident and ensure that all procedures are followed correctly
- Review incidents to determine what lessons can be learnt and what process improvements may be required
- Review changes in legal and regulatory requirements to ensure that all processes and procedures remain valid
- Review intelligence data such as information from log files, results from automated incident responses, third-party websites and industry seminars to determine trends and changes in the IT security landscape and where future incidents could originate
- Review and recommend technologies to manage and counteract incidents
- Establish relationships with the local law enforcement agency and the appropriate government agencies
- Form relationships with the incident response teams within key partners and suppliers, such as the company's ISP

The incident response process

When an incident is reported, follow these steps:

Recording

In order to ensure an effective and appropriate response to a potential information security incident, all members of staff should know the relevant personnel to contact (e.g. an Information Security Manager or designated person in charge of risk) on discovering the incident has occurred. It is important to capture the following information, in as much detail as possible:

- The date and time the incident occurred
- The date and time the incident was detected
- Who/what reported the incident
- Details of the incident including:
  - A description of the incident
  - Details of the systems involved
  - Corroborating information such as error messages, log files, etc.

The Information Security Manager should then evaluate the incident and determine whether to treat it as a security incident or whether to refer it to the support desk to be handled as a normal service incident.

Notification

The notification or identification that an incident is occurring can happen in many different ways, including:

- Automatically from specific security devices such as an alert from a firewall
- Automatically from non-security devices such as a network monitoring system that observes unusual network activity
- Manually from a review of system and security log files on network and/or security devices
- Staff noticing unusual or suspicious activity on the computer system
- Staff noticing content in breach of the company's security policy on a colleague's computer
- Customers or the public who may have noticed corruption to their data, receiving a phishing email or noticed defacement on the company's website

Known intelligence can improve prior awareness to the possibility of an increase in the occurrence of certain types of incidents. Some examples of reliable intelligence include:

- Alerts from computer security companies about new malware variations and attack trends (e.g. https://blog.trendmicro.com/, https://www.mcafee.com/blogs, https://www.welivesecurity.com/, https://blog.malwarebytes.com/)
- Updates from national computer emergency response teams about certain attack types (e.g. https://iriss.ie/, https://www.ncsc.gov.ie/, https://www.ncsc.gov.ie/, https://www.us-cert.gov/)
- Notices from national and international law enforcement about types of cybercrime and fraud (e.g. https://www.europol.europa.eu/, https://www.enisa.europa.eu/, https://www.garda.ie/en/, https://www.fbi.gov/investigate/cyber)
- Reliable news or specialist media can be a source of information about cybersecurity trends (e.g. https://www.infosecurity-magazine.com/, https://www.scmagazine.com/, https://portswigger.net/daily-swig, https://www.vice.com/en_us/section/tech, https://www.sans.org/newsletters/, https://www.databreachtoday.com/, https://www.darkreading.com/)

Similarly, major global news events are often a trigger for online criminal gangs to launch phishing campaigns and online scams that exploit people's curiosity.

Alternatively, hacking attempts are known to increase at the start of each autumn as students start University and try their new skills online.

Classification

Not every security incident is of equal importance. Classifying incidents into different levels of importance ensures a structured approach that enables a faster response to high priority incidents than to incidents of lower importance.

For example, excessive traffic on port 80 on a firewall could indicate the start of a Denial of Service attack and would require a quick response to ensure minimal disruption to the network; therefore it would be classified higher than, say, a rejected access attempt to an employee's personal directory.

The severity of the incident does not determine the classification alone. The potential target is also a key factor: a failed access attempt to the organisation's sensitive information like the payroll system will have a higher classification than a rejected access attempt to unclassified information. It is worth noting that the classification can change based on additional information that emerges during the response or investigation.

Classifying incidents will depend on many factors such as:

- The nature of the incident
- The criticality of the systems being impacted
- The number of systems impacted by the incident
- The impact the incident can have on organisation from a legal and/or public relations point of view
- Legal and regulatory requirements for disclosure

Classifications:

Classification	Explanation	Example
High	An incident poses an immediate threat to all systems, the exposure of critical or sensitive systems, may result in criminal charges, regulatory fines or may result in undue bad publicity for the organisation.	• Network-wide malware or ransomware outbreak • Active external/internal unauthorised access to systems • Compromise of information resulting in serious data disclosure • Serious breaches of the organisation's Acceptable Usage Policy
Medium	An incident poses a threat to a limited number of systems, may compromise non-critical or non-sensitive systems or involved time critical investigation into a staff member's activities.	• In-active External/Internal unauthorised access to systems. • Localised Virus/Worm outbreak • Breach of the organisation's Acceptable Usage Policy
Low	An incident poses no immediate threat to systems.	• Failure to download anti-virus signatures • Request to review security logs. • Minor breaches of the organisation's Acceptable Usage Policy

The Information Security Manager or designated staff member should then escalate and notify the appropriate members of the incident response team according to the classification of the incident.

Tracking

Throughout the lifetime of the security incident, it is important to make accurate records of each action that individuals or the team takes, and the consequences of that action. This is essential for several reasons:

- To aid in the ongoing troubleshooting and diagnosis of the issue
- In the event the incident results in a criminal or civil case, the accurate recording of events may be submitted as evidence regarding the investigation
- In the event the incident results in a staff disciplinary case, the accurate recording of events may be submitted as evidence regarding the investigation.
- For post-mortem diagnosis of the incident to determine potential areas of improvement within the processes and procedures relating to information security incident response

Once the information security incident has been classified, there needs to be careful consideration of how to track the issue. If the network has been compromised, it is likely that the attacker may have access to all systems within the organisation. If so, they could become aware that a response is underway and take evasive, elusive and/or destructive action. Therefore it is worth thinking about whether or not to record certain high priority information security incidents within the normal helpdesk system or instead to track using alternative methods such as manual recording or using a standalone system not connected to the network.

During the incident, document, time-record and sign all actions. If not already notified, notify the support desk with details of the information security incident.

Depending on the scale, impact and duration of the information security incident consideration should be given as to whether additional resources may be required on the organisation's support desk to deal with client queries. For example, a prolonged incident may result in the loss of business-critical services which may result in a higher volume of calls to the support desk.

Response

The type of information security incident will determine the way the information security response team handles the incident. The incident response team should develop and test standard operating procedures to cover incidents such as:

- Malware/virus infection
- External unauthorised access to systems
- Internal unauthorised access to systems
- Theft of computer equipment and related data
- Discovery of illegal content on the organisation's information processing systems
- Serious breach of the organisation's Acceptable Usage Policy
- Minor breach of the organisations Acceptable Usage Policy
- Defacement of the organisation's website
- Denial of Service Attack on the organisation's information processing systems, e.g. Internet connection
- Email Flood Attack on the organisation's information processing systems
- Compromise of information processing services belonging to third-party partners, e.g. ISP, supplier, hosting provider
- Disclosure of confidential information

Constantly review and test these procedures for their efficiency and adopt new standard operating procedures when and where required. It is worth noting that from time to time, security incidents may occur that fall outside the scope of the standard operating procedures. You will need to manage them in an ad hoc fashion.

Regardless of whether an information security incident falls within the scope of existing standard operating procedures or not, the following are the main steps within the process:

Containment

Containment involves limiting the scope and impact of the incident. This is particularly applicable when responding to incidents as a result of malware, such as a virus, due to the ability of such software to spread rapidly.

The Information Security Manager and/or incident response team should decide on how best to contain an incident, with the aim of preventing further system compromise, allowing adequate time and resources for investigating the incident, while at the same time restoring the systems to operational status as soon as possible.

The team should also have full authority to conduct whatever actions they deem necessary to contain the incident – up to and including taking critical services and applications offline.

Eradication

Eradicating an incident entails identifying and removing the root cause. Simply restoring a system to operational status without identifying the root cause of the compromise may result in the information security incident re-occurring again at a later stage.

It is important to gather whatever evidence available in a forensically sound manner. This means ensuring all steps and actions are clearly documented with original media and log files digitally signed and stored securely to prevent tampering. All investigations should be conducted on verified copies of the original media and log files. It may be necessary to engage with external expertise to conduct the forensic investigation.

Recovery

Recovery means restoring a system or systems back to their normal operational status. This may require restoring from backups or reinstalling from known and certified original media. Part of the recovery process should ensure that the integrity of the backup being used for the restore operation has been thoroughly verified and that the restore operation was successful.

Communications

Maintaining proactive communication can be an important part of any incident response plan, where appropriate. This includes communicating to the appropriate IT and business management levels on the impact and progress of the incident as it happens.

During an information security incident it is essential to maintain confidentiality throughout the incident's lifecycle. In the event of a high priority incident, no communication should occur over existing information systems like email, because they may be compromised and could alert the attacker to the investigation.

In addition, the nature of the incident may require confidentiality if it involves a criminal case, the disciplining of a staff member, or if there is a risk of reputational damage to the organisation.

Where possible, share information on security incidents on a strict need to know basis only. Ideally, all updates from the incident response team to those outside the team should come only from the information security officer or equivalent role.

From time to time, it may be necessary to communicate with external parties during or as a result of an information security incident. The following are the main contact points and some advice on how to handle them:

Media enquiries

Handling media enquiries should be strictly by the organisation's PR department. No other member of staff should comment to the press about any information security incident. When preparing post-incident statements for the media:

- Deal only in verified facts
- Avoid speculation
- Explain the incident in business terms
- Include details of users or services affected by the breach.

Law enforcement

It may be necessary to instigate criminal proceedings as a result of an information security incident. This could be due to criminal activity conducted by users within the organisation or the requirement to prosecute an external unauthorised attacker. The decision to proceed with a criminal case should be made by the Senior Management in consultation with the legal department.

Third-party partners

Depending on the nature of the incident, you may need to alert third party partners or suppliers. This may be as a result of the investigation identifying the source of the incident as one of those companies or asking for their help to investigate or eradicate the incident.

For example, an attack on the organisation's internet connections may require the assistance of the ISP in dealing with the attack. In the main, these types of communications should be at an operational level. Ideally, relationships with key personnel in the service provider or partner should be in place before any incidents as this ensures a more effective response.

Public

As with media enquiries above, the Press Officer or external PR Advisor should deal with all public enquiries about an information security incident.

Depending on where the organisation conducts business, or what sector it operates in, certain legal and/or regulatory requirements may demand that the organisation notifies affected customers of the breach. Senior management, in consultation with its legal advisors, should make the decision to contact customers.

Staff

It is important to maintain appropriate levels of communication with staff during an incident, notwithstanding the requirements for maintaining confidentiality. This is particularly important when the incident involves the investigation of a staff member. In such a case, it is extremely important to maintain the suspected staff member's privacy and rights at all times. The Human Resource department will play a key role in this regard.

Information security incidents that impact directly on the availability of production systems will need to be managed in such a way to keep impacted staff updated as to when the systems may be likely to be restored while at the same time maintain any necessary confidentiality.

Management

Depending on the severity and the impact of an incident, senior management may need to be made aware and kept updated on the progress of the issue. Where possible, the escalation tree for an information security incident should be the same as that used for all service issues.

Legal

Depending on the nature of the incident and whether it will involve a criminal prosecution or staff disciplinary proceedings, regular contact should be maintained with the legal expertise within the incident response team to ensure that the most appropriate steps are taken.

Integration with other processes

Due to its nature, the information security incident response process should integrate tightly with existing business processes such as:

- Change management
- Service incident management
- Disaster recovery management.

Post-incident review

After any information security incident, there should be a thorough review. This ensures the steps taken during the incident were appropriate and to identify any areas that may need to be improved. Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible.

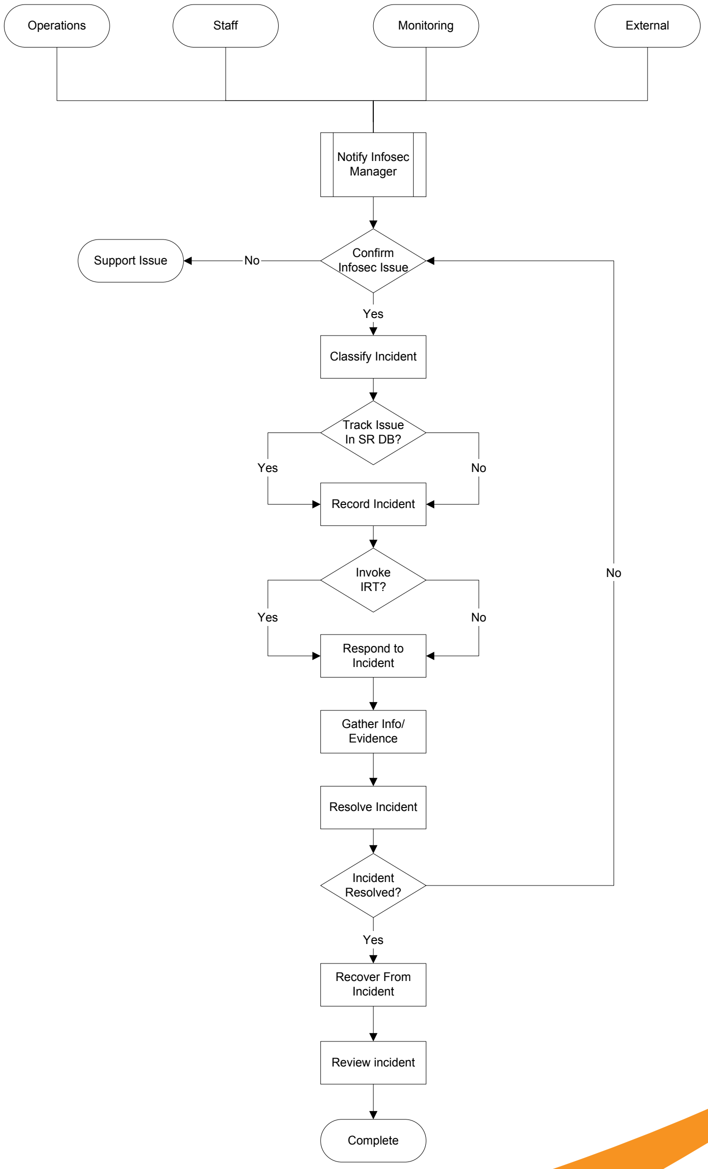
Reporting

In order to improve the incident response process, it is essential to keep accurate records of the change requests and review them accordingly. Aim to produce monthly reports reflecting the following details:

- Number of information security incidents submitted, broken down by priority
- Number of information security incidents submitted, broken down by type
- Number of information security incidents resulting in service requests.

Incident response workflow

This graphic provides a useful visual aid to help guide the workflow of the incident response process.



Copyright Notice

Disclaimer:

BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

For more information please contact us:

+353 (0)1 440 4065

info@bhconsulting.ie

www.bhconsulting.ie