



Helping you piece IT together

Incident Response Best Practise Guide



Copyright Notice

© 2005 BH Consulting IT Ltd. trading as BH Consulting, All rights reserved. This whitepaper is protected by copyright. Any reproduction of material of this whitepaper must be requested and authorised in writing from BH Consulting. Authorised reproduction of material must include all copyright and proprietary notices in the same form and manner as the original, and must not be modified in any way. Acknowledgement of the source of the material must also be included in all references. BH Consulting reserves the right to revoke such authorisation at any time, and any such use must be discontinued immediately upon notice from BH Consulting.

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 The information in this document may be updated from time to time and may at times be out of date.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.

Table of Contents

1.	Incident handling and Management.....	4
2.	Incident Notification/identification	5
3.	Incident Classification	6
4.	Incident Response	7
5.	Incident Response Team.....	8
6.	The Incident Response Process.....	10
6.1	Incident Recording	10
6.2	Incident Notification.....	10
6.3	Incident Classification	10
6.3.1	Classifications;	11
6.3.2	Incident Tracking.....	11
6.3.3	Response.....	12
6.3.4	Communications	13
6.4	Integration with Other Processes.....	14
6.5	Post Information Security Incident Review	15
6.6	Reporting.....	15
7.	Information Security Incident Response Workflow	16
8.	Further Reading	17
9.	Contact Us	18

1. Incident handling and Management

Security is only as effective as the response it generates. A structured response ensures that an Incident is recognised early and dealt with in the most appropriate manner. An incident that is not responded to in a timely manner can expose an organisation to many issues including, but not necessarily limited to:

- 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.
- The organisation may face potential legal and/or compliance issues depending on the regulatory and legal requirements.
- Exposure to legal cases from third party organisations impacted as result of 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 demonstrates that it is taking 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:

- The rapid and accurate assessment of security incidents and the most appropriate response.
- Shortened recovery times to incidents and minimised business disruption.
- The 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.
- Ensures that the company complies with local legal, regulatory and industry requirements.
- A potential reduction in incidents as the organisation is not considered a "soft target".
- Provides accurate reporting and statistics to continuously improve the security of the organisation

2. Incident Notification/identification

The notification or identification that an incident is occurring can happen in many different ways. Notification of an incident can happen:

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

A process should be in place to notify the relevant personnel that the incident has occurred and a response is required. This process should ensure that the following information is passed onto the response team:

- 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.

Prior awareness to the possibility that an increase in the occurrence of certain incidents may happen can be improved as a result of known intelligence. Alerts from computer virus companies of a new computer virus will increase the awareness that an incident as a result of that virus could occur, alternatively hacking attempts are known to increase at the start of each autumn as students start University and try their new skills online.

3. Incident Classification

In order to ensure that incidents are responded to in a structured manner it is essential that incidents are classified into different levels so that high priority incidents can be responded to quicker than incidents of a lower nature. For example excessive traffic on port 80 on a firewall may indicate the start of a Denial of Service attack and would require a quick response to ensure minimal disruption to the network and therefore would be classified higher than, say a rejected access attempt to the personal directory of an employee.

The severity of the incident does not alone impact the classification. The potential target also impacts the classification. A rejected access attempt to the organisation's sensitive information will have a higher event classification than a rejected access attempt to unclassified information.

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.

4. Incident Response

In order to implement an appropriate incident response, the proper people and processes need to be involved and the most appropriate response subsequently developed. 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 responses to an incident and also that the incident response has the necessary levels of authorisation and autonomy. There is no point having senior management involved in a response 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 all policies and procedures should be properly tested and reviewed on a regular basis to ensure their effectiveness and applicability. A review process should also be put in place to ensure that lessons are learnt 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 be dependant on the incident classification. The response team will also need to confirm that the incident has occurred and if so what the most appropriate response to the incident is. Once an incident has been confirmed and has initiated the appropriate incident response process, all care must be taken to preserve and record all information and potential evidence in the incident a legal or civil case ensues.

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

As a large majority of incidents may happen outside office hours or when key personnel are not immediately available, all staff must be given clear guidelines in how they report and respond to incidents.

Many incidents may simply require an automated response. For example a known computer virus detected in a file could be automatically deleted by the Anti-Virus software and not require a 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 to the firewall or allow the attack to continue so further evidence may be gathered in the incident a legal case may be required.

An Incident Response Log should be kept where all actions and results of those actions are recorded accurately. Details as to who completed the actions, the time of the action and the outcome need to be maintained. This is to ensure that an accurate 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.

5. 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 be made up of 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 a formulated process should be in place to ensure that 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 senior management during a critical incident.

Typically an Incident Response team will be made up of representatives of the following:

- **IT Security**
The core team members will be those from the IT Security team as they are the most knowledgeable with regards to managing and dealing with computer security incidents.
- **IT Operations**
As the operations team is very often the first line of defence/detection of incidents either via monitoring tools or from reports to the support desk, it is essential that representation from this team is on the Incident Response Team.
- **Physical Security**
While IT Security is arguably still in its infancy, the world of physical security has been around for a much longer time. A lot of experience and knowledge gained in the physical world can be applied to the virtual world. In addition, it may be necessary to involve the physical security team in the response to an incident where there has been physical access to compromised systems.
- **Human Resources**
It is essential that a representative from the Human Resource team is involved in the Incident Response Team to ensure that processes and procedures comply with good Human Resource practice and do not impinge on industrial relations. The result of an incident response may be to discipline a staff member for breach of the organisation's acceptable usage policy and this will require the Human Resource team's input to ensure due process.
- **Legal Department**
As with the Human Resource department, it is imperative that legal advice is taken both during the development of the processes and procedures and in the response to serious incidents.
- **Public Relations**
How information is communicated to the public, customers, partners, shareholders and press is a unique skill and one that is necessary to ensure the correct amount of information is disclosed at the right time to the right people.
- **External Expertise**
There will be times due to the nature of the information security incident external expertise will be required. 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 Incident Response Team 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 are 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.
- Relationships with the Incident Response Teams within key partners and key suppliers, such as the company's ISP, need also be established.

6. The Incident Response Process

When an incident is reported the steps below should be followed;

6.1 Incident Recording

Details of the incident should be recorded accurately. The information gathered should include;

- 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.

6.2 Incident Notification

In order to ensure an effective and appropriate response to a potential information security incident the Information Security Manager should be contacted immediately and given the details of the incident.

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

The Information Security Manager should then escalate and notify the appropriate members of the team according to the classification of the incident.

6.3 Incident Classification

In order to ensure that incidents are responded to in a structured manner it is essential the Information Security Manager classifies incidents into the appropriate levels so that high priority incidents can be responded to quicker than incidents of a lower nature. It should be noted that based on additional information gathered during the response to an information security incident the classification of an incident can be changed appropriately.

The severity of the incident does not alone impact the classification. The potential target also impacts the classification. A rejected access attempt to sensitive data will have a higher event classification than a rejected access attempt to non-sensitive systems, for example unauthorised access to a staff member's home directory may be classified with a lower priority than unauthorised access to the payroll system.

Classifying information security incidents will depend on a number of 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 the organisation from a legal and/or public relations point of view.
- Legal and regulatory requirements.

6.3.1 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.	<ul style="list-style-type: none"> • Network wide Virus/Worm 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Failure to download anti-virus signatures. • Request to review security logs. • Minor breaches of the organisation's Acceptable Usage Policy

6.3.2 Incident Tracking

Throughout the lifetime of the information security incident it is important that accurate records are taken of each action taken and the consequences of each action. This is important from a number of points of view;

- 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 the method of tracking the issue needs to be carefully considered. If the network has been compromised it is likely that the attacker may have access to all systems within the organisation and therefore could be alerted that a response is underway and take evasive, elusive and/or destructive action. Therefore thought should be given as to whether or not information security incidents classified as "High" should be recorded within the normal helpdesk system or be tracked using alternative methods such as manual recording or using a standalone system not connected to the network.

During the information security incident all actions should be documented, time recorded and signed. 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.

6.3.3 Response

The type of information security incident will determine the way that the information security response team will handle the incident. Standard operating procedures should be developed and tested by the Incident Response Team. These standard operating procedures should cover incidents such as,

- Malware/Computer 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 organisations 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.

The above procedures should be constantly reviewed and tested for their efficiency and new standard operating procedures implemented when and where required. It should be noted that from time to time information security incidents may occur that fall outside the scope of the above standard operating procedures and as a result they will need to be managed in an adhoc fashion.

Regardless as to 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;

6.3.3.1 Containment.

Containment involves limiting the scope and impact of the information security incident. This is particularly applicable when responding to information security 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 the incident response team should decide on how best to contain an incident. This decision will need to be taken with the objectives of

preventing further systems 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 putting critical services and applications offline.

6.3.3.2 Eradication.

Eradicating an incident entails identifying and removing the root cause of the information security incident. 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.

6.3.3.3 Recovery

Recovery means restoring a system(s) back to their normal operational status. This may require restoring system(s) 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.

6.3.4 Communications

Throughout the information security incident it is essential that appropriate communications are maintained. This includes communicating to the appropriate IT and business management levels on the impact and progress of the incident.

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

In addition, the nature of the incident may require confidentiality is maintained as it may involve a criminal case, the disciplining of a staff member or be publicly embarrassing to the organisation.

Where possible, information on information security incidents should be shared 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.

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 how they should be handled;

6.3.4.1 Press enquiries

All press and media enquiries should be strictly handled by the organisation's PR department. No other member of staff should comment to media or press enquiries regarding any information security incident.

6.3.4.2 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.

6.3.4.3 Third Party Partners

Depending on the nature of the information security incident it may be necessary to contact third party partners and suppliers to alert them of the incident. This may be as a result of the investigations into the incident identifying the source of the incident being from one of those companies or requiring assistance from those companies to investigate or eradicate the incident.

For example an attack on the organisation's Internet connections may require the assistance of the providing ISP in dealing with the attack. In the main, these types of communications should be at an operational level and ideally relationships should be established previous to any incidents to ensure an effective response.

6.3.4.4 Public

Similar to press enquires all public enquiries regarding an information security incident should be dealt with by the Press Officer.

Depending on where the organisation conducts business, legal and/or regulatory requirements may require that affected customers are notified of the breach. The decision to contact customers should be made by the Senior Management in consultation with the legal department.

6.3.4.5 Staff

It is important that appropriate levels of communication are maintained 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 that the suspected staff member's privacy and rights are maintained 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.

6.3.4.6 Management

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

6.3.4.7 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.

6.4 Integration with Other Processes

Due to its nature, the Information Security Incident Response Process should be tightly integrated with other existing processes such as;

- Change Management Process
- Service Incident Management Process

- Disaster Recovery Management Process

6.5 Post Information Security Incident Review

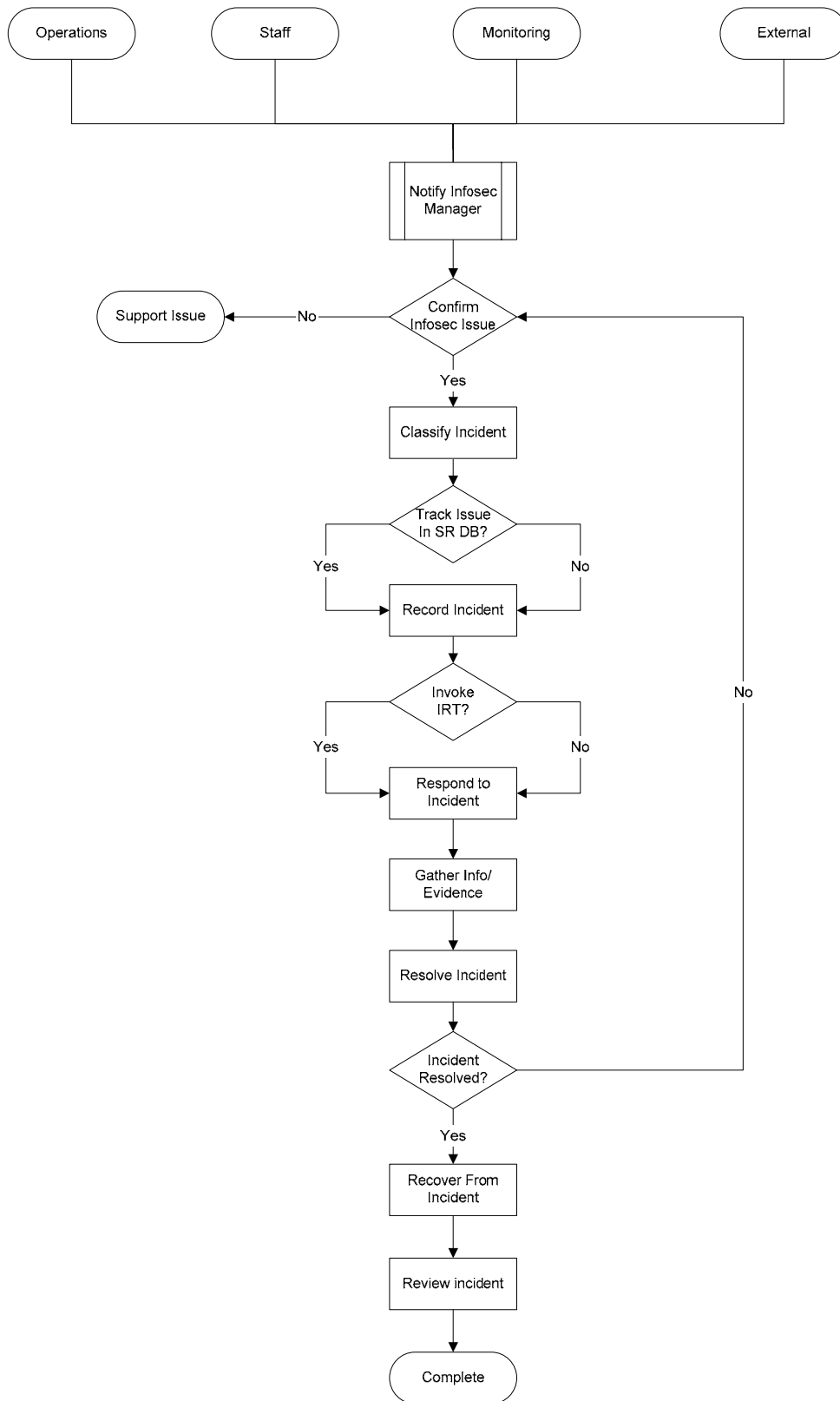
Subsequent to any information security incident a thorough review of the incident should occur. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify any areas that may need to be improved. Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible.

6.6 Reporting

In order to improve the Information Security Incident Response Process it is essential that accurate records are kept of the change requests and reviewed accordingly. Monthly reports reflecting the following should be produced;

- 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

7. Information Security Incident Response Workflow



8. Further Reading

- RFC-2196: Site Security Handbook Chapter 5 Security Incident Handling
<http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc2196.html#sec-5>
- RFC-2350: Expectations for Computer Security Incident Response
<http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc2350.html>
- Carnegie Mellon Cert Coordination Center. "Creating a Computer Security Incident Response Team: A Process for Getting Started"
<http://www.cert.org/csirts/Creating-A-CSIRT.html>
- Malisow, Ben "Moment's Notice: The Immediate Steps of Incident Handling" 2000
<http://www.securityfocus.com/focus/ih/articles/moments.html>
- Understanding Incident Response
<http://www.fedcirc.gov/docs/understanding.html>
- CERT/CC Incident Reporting Guidelines, Revision Jul 30, 2001
http://www.cert.org/tech_tips/incident_reporting.html
- The SANS Institute – (<http://www.sans.org>)
- United States National Institute of Standards and Technology, SP 800-86 (DRAFT), "Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response" -(<http://csrc.nist.gov/publications/drafts.html>)
- Microsoft, "The Antivirus Defence-in-Depth Guide" - (http://www.microsoft.com/technet/security/topics/serversecurity/avdind_0.msp)
- United States National Institute of Standards and Technology, SP 800-61, "Computer Security Incident Handling Guide" (<http://csrc.nist.gov/publications/nistpubs/index.html>)
- RFC-2196: "Site Security Handbook Chapter 5 Security Incident Handling" (<http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc2196.html#sec-5>)
- RFC-2350: "Expectations for Computer Security Incident Response" – (<http://www.cse.ohio-state.edu/cgi-bin/rfc/rfc2350.html>)
- Carnegie Mellon Cert Coordination Centre. "Creating a Computer Security Incident Response Team: A Process for Getting Started" – (<http://www.cert.org/csirts/Creating-A-CSIRT.html>)
- Malisow, Ben "Moment's Notice: The Immediate Steps of Incident Handling" – (<http://www.securityfocus.com/focus/ih/articles/moments.html>)
- Understanding Incident Response – (<http://www.fedcirc.gov/docs/understanding.html>)
- CERT/CC "Incident Reporting Guidelines" – (http://www.cert.org/tech_tips/incident_reporting.html)
- "Incident Response-Investigating Computer Crime" – Kevin Mandia & Chris Proise – McGraw Hill – ISBN number 0-07-213182-9
- "The Cuckoo's Egg" – Cliff Stoll – Pocket Books – ISBN number 0-7434-1146-3

9. Contact Us



Helping you piece IT together

If you wish to contact us or provide any feedback on this whitepaper you may do so using the following contact details.

Telephone : +353-(0)1- 4404065
Website : <http://www.bhconsulting.ie>
Email : info@bhconsulting.ie