Helping you piece IT together

Incident Response Best Practise Guide

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 The information in this document may be updated from time to time and may at times be out of date.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

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 advise 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

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. Processes and procedures

The Incident Response Team must ensure that clear and comprehensive processes and procedures are in place to enable a coherent and structured response to incidents as they arise. These processes and procedures should be regularly reviewed to ensure that they are still valid. A communications program should be initiated to make all staff members aware of their responsibilities and how to report suspected incidents.

After each incident the processes and procedures implemented should be reviewed to identify any potential gaps and how best to address those gaps.

6.1 Incident remediation

Part of the Incident Response should include incident remediation and how best to restore systems and data to their status before the incident occurred.

7. 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

8. 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**