An Introduction to Information Security Incident Management Based on ISO/IEC TR 18044:2004

Information is an asset that, like other important business assets, is essential to an organization’s business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Information security is the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

But, no typical information security policies or safeguards will guarantee total protection of information, information systems, services or networks. After safeguards have been implemented, residual weaknesses that may make information security ineffective, and, thus, information security incidents possible, are likely to remain, potentially with both direct and indirect adverse impacts on an organization’s business operations. Furthermore, new, previously unidentified threats will inevitably occur. Insufficient preparation by an organization to deal with such incidents will make any actual response less effective and may increase the degree of potential adverse business impact. Therefore, it is essential for any organization that is serious about information security to have a structured and planned approach to:

- Detect, report and assess information security incidents
- Respond to information security incidents, including by the activation of appropriate safeguards for the prevention and reduction of, and recovery from, impacts (e.g., in the support and business continuity planning areas)
- Learn from information security incidents, institute preventive safeguards and, over time, make improvements to the overall approach to information security incident management

ISO/IEC TR 18044:2004 Information technology—Security techniques—Information security incident management provides advice and guidance on information security incident management for information security managers and information systems managers. The main objective of this article is to provide an overview of information security incident management based on ISO/IEC TR 18044:2004.

IMPORTANCE OF INCIDENT MANAGEMENT

Business environments are inter-networked with public and private networks, providing additional opportunity for unauthorized access. Barriers, alarms and alerts, network layering, and system and perimeter security provide a level of security; however, internal and external security breaches continue to occur because of new threats and vulnerabilities. The response to these incidents is a critical component of business continuity, risk management, the maintenance and management of the security infrastructure, and, in some cases, compliance with rules and regulations.

There is no guarantee that even the best possible controls will prevent disruptive and sometimes even catastrophic incidents from occurring. Adverse events such as security breaches, power outages, fires and natural disasters can bring IT and business operations to a halt. Incident management enables a business to respond effectively when a potential or real incident occurs, to continue operations in the event of disruption, and to survive interruptions or security breaches in information systems.
As organizations increasingly rely on information processes and systems, and significant disruptions to those activities result in unacceptably severe impacts, the criticality of effective incident management has grown. Some of the factors that compound the necessity include:

• The trend of both increased occurrences of and escalating losses from information security incidents that have resulted in serious consequences
• The increase of vulnerabilities in software or systems can affect large parts of an organization’s infrastructure and impact operations
• Failure of security controls to prevent incidents
• Legal and regulatory groups requiring the development of an incident management capability
• The growing sophistications and capabilities of profit-oriented attackers

THE INCIDENT MANAGEMENT DEFINITION
ISO/IEC TR 18044:2004 distinguishes between an information security event and an incident:

• An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
• An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Incident management includes incident response. Incident management encompasses a variety of activities including proactive efforts to limit or prevent incidents, whereas incident response is the reactive element in the event of an incident.

The goals of incident management and response activities can be summarized as:

• Detect incidents quickly.
• Diagnose incidents accurately.
• Manage incidents properly.
• Contain and minimize damage.
• Restore affected services.
• Determine root causes.
• Implement improvements to prevent recurrence.

PLANNING CONSIDERATION
As with other aspects of risk management, risk assessments and business impact assessments (BIAs) form the basis for determining the priority of resource protection and response activities.

Planning consideration must include all business functions that are critical, vital and sensitive, as well as those that are nonsensitive and noncritical but necessary support functions. Defining requirements and expectations is primarily the responsibility of business owners and senior management, since they are responsible for operations and safeguarding the assets and the public image of an organization. The plan should address all functions and assets required for an organization to remain viable as a business entity. This includes continuity procedures necessary to survive and minimize the consequence of any potential business interruption.

To provide effective response, a response and recovery plan should be clearly documented and readily accessible when needed, to minimize the effect of disruption. This plan should be based on the long-range IT plan and should be consistent with the overall business continuity and security strategies.
SENIOR MANAGEMENT COMMITMENT
As is the case with other aspects of information security, senior management commitment is critical to the success of incident management and response. It is a component of risk management, and the same rationale and justification will serve.

A business case can be made, in an effort to educate management, showing that effective incident management and response are less costly options than attempting to implement preventive controls for all possible conditions. The notion is that incident management and response are parts of a trade-off that can reduce the cost of risk management efforts by allowing higher levels of acceptable risk. This is possible because impacts can still be managed via effective incident management and response to address the higher risks.13

In other words, if it is more cost-effective to manage and recover from the occasional incident than it is to put in the controls to prevent it, the former may be a prudent resource management decision.14 This is similar to the common approach to protecting against fire with a combination of reasonable prevention means, coupled with a fire department response, if prevention fails, and finally insurance in the rare event that incident management and response fail. While a totally fireproof structure could be built, optimal cost-effectiveness utilizes a combination of risk management approaches.

INCIDENT MANAGEMENT PROCEDURES
There is no single, fixed, one-size-fits-all set of incident management procedures for every organization. However, there are a number of good practices that most organizations adopt and customize to meet their needs. One commonly adopted approach is ISO/IEC Technical Report (TR) 18044:2004, available from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The approach described in ISO/IEC TR 18044:2004 consists of four distinct processes:
- Plan and prepare
- Use
- Review
- Improve

Plan and Prepare
Effective information security incident management requires appropriate planning and preparation. For responses to information security incidents to be effective, the following actions are necessary:
- Develop and document an information security incident management policy, and gain visible commitment to that policy from all key stakeholders, particularly senior management.
- Develop and comprehensively document an information security incident management scheme to support the information security incident management policy. Forms, procedures and support tools for the detection, reporting, assessment and response to information security incidents, and details of the incident severity scale, should be encompassed within scheme documentation. (It should be noted that in some organizations, the scheme may be referred to as an information security incident response plan.)
- Update information security and risk management policies at all levels, i.e., organizationwide, and for each system, service and network, with references to the information security incident management scheme.
- Establish an appropriate information security incident management organizational structure, e.g., the information security incident response team (ISIRT), with defined roles and responsibilities allocated to personnel who are available to enable an adequate response to all known types of information security incidents. Within most organizations, the ISIRT will be a virtual team, with a senior manager leading the team supported by groups of individuals specialized in particular topics, e.g., in the handling of malicious code attacks, who will be called upon depending on the type of incident.
- Make all organizational personnel aware, through briefings and/or other mechanisms, of the existence of the information security incident management scheme, its benefits and how to report an information security event. Appropriate training should be provided to those personnel responsible for managing the information security incident management scheme, decision makers involved in determining whether information security events are incidents, and those individuals involved in the investigation of incidents.
- Thoroughly test the information security incident management scheme.
Use
The following processes are necessary to make use of an information security incident management scheme:
• Detecting and reporting the occurrence of information security events (by human or automatic means)
• Collecting information associated with information security events, and assessing that information to determine what events are to be categorized as information security incidents
• Making responses to information security incidents immediately, in real time or near real time
• Where information security incidents are under control, conducting activities that may be required in slower time (e.g., in facilitating full recovery from a disaster)
• If information security incidents are not under control, instigating crisis activities (e.g., calling the fire brigade/department or activating a business continuity plan)
• Communicating the existence of information security incidents and any relevant details thereof to internal and external people and/or organizations (This could include escalating for further assessments and/or decisions as required.)
• Conducting forensic analysis
• Properly logging all activities and decisions for further analysis
• Closing incidents on resolution

Review
After information security incidents have been resolved/closed, the following review activities are necessary:
• Conduct further forensic analysis, as required.
• Identify the lessons learned from information security incidents.
• Identify improvements to information security safeguard implementation, as a result of lessons learned, whether from one information security incident or from many.
• Identify improvements to the information security incident management scheme as a whole, as a result of lessons learned from quality assurance reviews of the approach (e.g., from review of the effectiveness of the processes, procedures, the reporting forms and/or the organizational structure).

Improve
The information security incident management processes are iterative, with regular improvements made to a number of information security elements over time. These improvements are proposed on the basis of reviews of the data on information security incidents and the responses to them, as well as trends over time. This includes:
• Revising the organization’s existing information security risk analysis and having management review results
• Making improvements to the information security incident management scheme and its documentation
• Initiating improvements to security that may encompass the implementation of new and/or updated information security safeguards

INFORMATION SECURITY INCIDENT MANAGEMENT IN OPERATION
Information security events could be detected directly by a person or persons noticing something that gives cause for concern, whether technical, physical or procedural. Detection could, for example, be from fire/smoke detectors or intruder (burglar) alarms, with the alerts made to previously designated locations for human action. Technical information security events could be detected by automatic means, e.g., alerts made by audit-trail-analysis facilities, firewalls, intrusion detection systems and antivirus tools, in each case stimulated by preset parameters. Thus, it is essential that all personnel are well aware of, and have access to, the guidelines for reporting the different types of possible information security events.

How an information security event is handled is dependent upon what it is, and the implications and repercussions that may flow from it. For many people, this will be a decision beyond their competence; thus, the person who has detected an information security event should contact the designated operations support group.

It should be noted that while, in most cases, an information security event will have to be reported onward for action by the operations support group, there may be occasions in which an information security event can be handled locally, possibly with the help of local management. An information security event may be quickly determined as a false alarm, or it may be resolved to a satisfactory conclusion.

The receiving person in the operations support group should acknowledge receipt of the information security event report, enter it into the information security event/incident database and review it. This individual should seek any clarification from the person reporting the information security event, and collect any further information required and known to be available, whether from the reporting person or from elsewhere. Then, a member of the operations support group...
group should conduct an assessment to determine whether the information security event should be categorized as an information security incident or as a false alarm.

Information and other evidence collected at this stage may need to be used at a future time for disciplinary or legal proceedings. The person or people undertaking the information collection and assessment tasks should be trained in the requirements for collection and preservation of evidence.15

Unless the organization has developed a detailed planned response to typical risk scenarios, much potential evidence will never be collected or will become worthless as a result of contamination. Moreover, during an investigation, the organization will be constantly faced with a dilemma: lose business when essential systems are switched off so that evidence can be properly preserved, or be profoundly handicapped and incur losses because evidence cannot be produced.16
Taking into account that information systems will create and retain electronic records only if specifically designed to do so,\textsuperscript{17} it is recommended that the planning stage include the following steps:\textsuperscript{18}

- Identify the main likely threats faced by the organization.
- Identify what sorts of evidence the organization is likely to need if it has to proceed to civil litigation or criminal proceedings.
- Identify to what extent the organization may already have the evidence.
- Identify what the organization will need to do to secure additional essential evidence.
- Identify potential legal problems such as admissibility, data protection, human rights, limits to surveillance, obligations to staff and others, and disclosure in legal proceedings.
- Identify the management, skills and resource implications for the organization.
- Turn the results into an action plan, which will need regular revision as the organization and its ICT infrastructure develop.

If the information security event is determined as likely to be an information security incident, and if the operations support group person has the appropriate level of competence, further assessment may be conducted. This may result in required remedial actions (e.g., additional emergency safeguards) being identified and referred to the appropriate person for action.

It may be evident that a crisis should be declared and, thus, for example, the business continuity manager should be notified for possible activation of a business continuity plan.

If an incident cannot be resolved by first-line support, more expertise or authority has to be involved. This is known as escalation and can take place at any time at any support level in the resolution process (figure 1).\textsuperscript{19}

**LESSONS LEARNED**

Once an information security incident has been closed, it is important that the lessons learned from the handling of the information security incident be quickly identified and acted upon. The lessons could be, for example, in terms of:\textsuperscript{20}

- New or changed requirements for information security safeguards. These could be technical or nontechnical (including physical) safeguards. Dependent on the lessons learned, these could include the need for rapid material updates for, and delivery of, security awareness briefings (for users as well as other personnel), and rapid revision and issue of security guidelines and/or standards.
- Changes to the information security incident management scheme and its processes, reporting forms and information security event/incident database

**LAW ENFORCEMENT INVOLVEMENT**

If there is reasonable suspicion that a crime was committed, law enforcement agencies should be included early in the process, so that volatile and fragile digital evidence is not compromised.

The results of a study conducted by the US Department of Justice show that many organizations are reluctant to report hacks. The perceived rationales for not reporting an intrusion include:\textsuperscript{21}

- The victim company does not know which law enforcement entity to call.
- If the victim company does report the intrusion to an appropriate agency, law enforcement will not act. Instead, the fact of the intrusion will become public knowledge, irreparably shaking investor confidence and driving current and potential customers to competitors who elect not to report intrusions.
- If law enforcement does act on the report and conducts an investigation, law enforcement will not find the intruder. In the process, however, the company will lose control of the investigation. Law enforcement agents will seize critical data and, perhaps, entire computers; damage equipment and files; compromise private information belonging to customers and vendors; and seriously jeopardize the normal operations of the company. Only competitors will benefit as customers flee and stock value drops.
- If law enforcement finds the intruder, the intruder will likely be a juvenile, reside in a foreign country or both, and the prosecutor will decline or be unable to pursue the case.
- If the intruder is not a minor, the prosecutor will conclude that the amount of damage inflicted by the intruder is too small to justify prosecution.
- If law enforcement successfully prosecutes the intruder, the intruder will receive probation or at most insignificant jail time, only to use his/her hacking experience to find fame and a lucrative job in network security.

Although the network owners have the obligation to secure their systems, and law enforcement has an obligation to investigate and prosecute, when appropriate, neither can function effectively without the other. Network operators need to view law enforcement as a necessary part of system...
protection, and law enforcement agencies need to be able to count on the cooperation of victims to fulfill their responsibilities.

CONCLUSION

Incident management can be considered the emergency operations part of risk management. Activities that take place as a result of unanticipated attacks, losses, thefts, accidents or any other unexpected adverse events occur as a result of a failure or lack of controls.

Poorly managed incidents have the capacity to become unmitigated disasters unless effectively managed.

Incident management is, nominally, a component of risk management and can be considered the operational and reactive element. That is, if managing risk were insufficient to prevent a threat from materializing and causing an impact, incident management and response capabilities should be available to react appropriately to limit damage and restore operations. An additional component is the forensic capability to investigate how the intrusion occurred and what actions can be implemented to minimize future risk.

ENDNOTES

3 Op cit, ISO/IEC 27002:2005
4 Ibid.
6 ISACA, Security Incident Management Audit/Assurance Program, USA, 2009, www.isaca.org/auditprograms
7 ISACA, CISM Review Manual 2011, USA, 2010
8 Ibid.
9 Op cit, ISO/IEC TR 18044:2004
10 Op cit, ISACA 2008
11 Ibid.
12 Ibid.
13 Ibid.
14 Ibid.
15 Op cit, ISO/IEC TR 18044:2004
16 The Information Assurance Advisory Council (IAAC), Directors' and Corporate Advisors' Guide to Digital Investigations and Evidence, 2009
18 Op cit, IAAC 2009
20 Op cit, ISO/IEC TR 18044:2004