

MANAGEMENT OF INFORMATION SECURITY INCIDENTS

PhD. Eng **Daniel COSTIN**
Polytechnic University of Bucharest

ABSTRACT

Reporting information security events. Reporting information security weaknesses. Responsible for handling incidents should be a Central Security Incidents Response Team (CSIRT). The incident response process has several phases, from initial preparation through post-incident analysis. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can act to mitigate the impact of the incident by containing it and ultimately recovering from it. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

KEYWORDS: *Security Event; Security Incident; Containment; Recovery; Investigation*

Security incident management is an administrative function of managing and protecting computer assets, networks and information systems. These systems continue to become more critical to the personal and economic welfare of our society. Organizations (public and private sector groups, associations and enterprises) must understand their responsibilities to the public good and to the welfare of their memberships and stakeholders. This responsibility extends to having a management program for “what to do, when things go wrong.” Incident management is a program which defines and implements a process that an organization may adopt to promote its own welfare and the security of the public.

Many incidents start small and progressively escalate into more serious enterprise crises. The most interesting aspect of any such incident is how the nature of the response needed changes, as it progresses from a local, operational incident to a full-blown crisis.

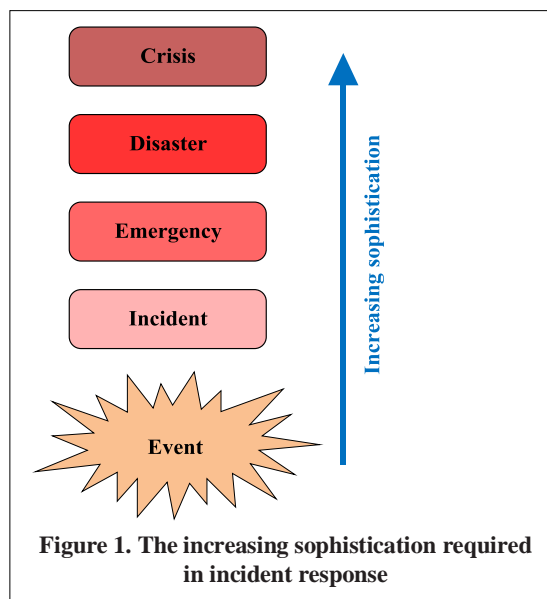


Figure 1. The increasing sophistication required in incident response

Figure 1 shows how the nature of the response becomes increasingly sophisticated according to the severity of the impact. For the lowest level of incident, activities tend to be local, operational and scripted, with a short-term focus on physical assets, such as buildings, people and equipment.

As the business impact of the incident increases, the scope of the response activities grows, involving a broader set of managers across the enterprise and invoking a more complex, and more flexible, set of business continuity plans, with a more medium-term focus on business processes, services and customers.

At its most severe level, a crisis might begin to spiral out of control, overwhelming the organization on a broad front, and demanding a unique response from top management, with a relentless, long-term focus on the enterprise's intellectual assets, such as brand value, operational impacts, corporate reputation, media perception, market capitalization, legal liability, regulatory response, political standing and citizen concerns.

Incident Management Stages

Typically, in management and response terms, the crisis event will include a series of stages.

Figure 2. illustrates some simple stages of a crisis, taking a managing group from the initial period of confusion where few facts may be known and effective decision making is problematic, through to a point where control is exerted, management can consolidate and stabilize the situation, and business recovery measures can be implemented.

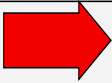
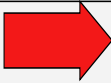
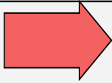
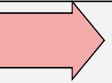
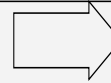
|  |  |  |  |  |
|---|---|---|--|---|
| Confusion | Control | Consolidation | Stabilization | Recovery |
| Limited Information | Understanding Gained | Information Shared | Information Flows | Communications Focused |
| Lack of Expertise | Expertise Mobilized | Expertise Arrives | Expertise in Charge | Expertise Transition |
| Poor Coordination | Coordination Begins | Coordination Matured | Processes Established | Processes Matured |
| Resources Not Mobilized | Resources Mobilized | Resources Arrive | Resources in Play | Resources Demobilized |

Figure 2. Management Stages of a Crisis

An organization should develop a group of individuals that are responsible for handling incidents, a Central Security Incidents Response Team (CSIRT).

The Central Security Incidents Management Team should be composed of:

- Executive management;
- Staff support department representatives;
- Department heads whose departments have been directly affected by the incident;

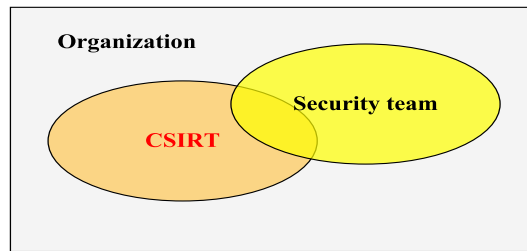


Figure 3. CSIRT within an organization

CSIRT Members should be responsible for the following areas:

- development and preservation of the program and the document,
- defining and classifying incidents,
- determining the tools and technology utilized in intrusion detection,
- determining if incident should be investigated and the scope of such an investigation (law enforcement agencies, forensic work),
- securing the network,
- conducting follow-up reviews,
- and promoting awareness throughout the organization.

Moreover, the CSIRT members must ensure the program reflects the business strategy of the organization as well as the information security group and ultimately have the support of executive management. An Incident Response Plan (IRP) should be developed in accordance with an organization’s Information Security Policies and Procedures.

The incident response process has several phases, from initial preparation through post-incident analysis. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can act to mitigate the impact of the incident by containing it and ultimately recovering from it. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents. Figure 4 illustrates the incident response life cycle.

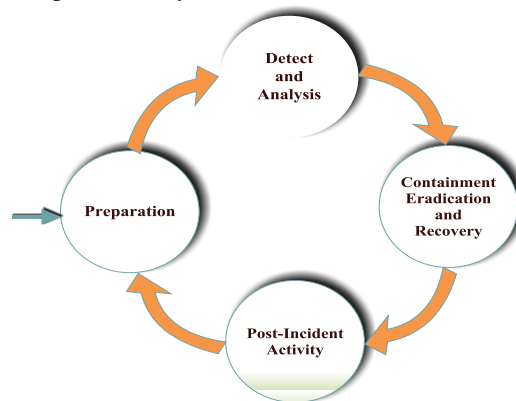


Figure 4. Incident Response Life Cycle

I. Preparation

The first step in handling any incident is to be well prepared. When an incident does occur, it is frequently mired in panic and fear – so it is best to know exactly what to do before it happens. Traditionally, this step includes many policy elements as well as monthly reports, incident team selection, emergency action plans, communication plans and packages of software that can all be used in the event of an incident.

Reporting information security events: Information security events should be reported through appropriate management channels as quickly as possible. Control includes:

- establishment of formal event reporting processes and procedures, setting out actions to be taken and points of contact;
- awareness on the part of all employees, contractors and third-party users of the event-reporting processes, including the requirement to report security events and weaknesses;
- awareness of the requirement to report as quickly as possible, with sufficient detail to allow a timely response;
- awareness of the prohibition on adverse action for reports made in good faith;
- suitable feedback processes to ensure that those reporting events are appropriately notified of results.

Reporting security weaknesses: All employees, contractors and third party users should be required to note and report any observed or suspected security weaknesses in systems or services as soon as possible. Controls include:

- easy, accessible channels for reporting, the availability of which is clearly communicated to employees, contractors and third parties;
- reasonable awareness on the part of employees, contractors and third parties of common signs and symptoms of security events;
- reporting requirement extends to malfunctions or other anomalous events that might indicate a security weakness;
- awareness on the part of employees, contractors and third parties that they should report, but not attempt to test, a suspected security vulnerability unless they have appropriate technical skills and an immediate response is required, since this might be interpreted as a potential misuse.

Some of the main recommended practices for securing networks, systems, and applications for preventing incidents are:

- Patch Management;
- Host Security;
- Network Security;
- Malicious Code Prevention;
- User Awareness and Training.

II. Detect and Analysis

The second step in incident management is the identification phase. In this phase, the organization gathers data, analyzes it, and then determines whether an incident has occurred. The incident handler must calmly assess the situation, be ready to communicate, and be ready to handle all evidence such that it can later be used in legal action (either civil or criminal) if necessary.

Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents. Control includes:

- processes to ensure routine use of data from the ongoing monitoring of systems to detect events and incidents;
- procedures specifically designed to respond to different types and severities of incident, including appropriate analysis and identification of causes, containment, communication with those actually or potentially affected by the incident, reporting of the incident to appropriate authorities, planning and implementation of corrective action to prevent reoccurrence as appropriate;
- collection and use of audit trails and similar evidence as part of the incident **management and investigation process**, and appropriate management of this evidence for use in subsequent legal or disciplinary proceedings;
- formal controls for recovery and remediation, including appropriate documentation of actions taken.

III. Containment, Eradication and Recovery

When an incident has been detected and analyzed, it is important to contain it before the spread of the incident overwhelms resources or the damage increases. Most incidents require containment, so it is important to consider it early in the course of handling each incident. An essential part of containment is decision-making (e.g., shut down a system, disconnect it from a wired or wireless network, disconnect its modem cable, and disable certain functions). Such decisions are much easier to make if strategies and procedures for containing the incident have been predetermined. Organizations should define acceptable risks in dealing with incidents and develop strategies accordingly. It is highly recommended that organizations create separate containment strategies for each major type of incident. The criteria should be documented clearly to facilitate quick and effective decision-making.

Investigation of incidents: Where disciplinary or legal action may be part of the follow-up to an information security incident, any investigation should be initiated in a manner that follows documented procedures and conforms to accepted practices. This control includes:

- specifying what persons or classes of person may request an investigation, and on what basis;
- specifying what persons or classes of person may initiate an investigation process, including collection of evidence;
- specifying the necessary documentation to initiate an investigation, and the documentation required as the investigation proceeds;
- procedures for securing and maintaining the integrity of investigatory records;
- observing appropriate procedures to assure "chain of custody" for any information collected.

IV. Post-Incident Activity

Lessons Learned: One of the most important parts of incident response is also the most often omitted: learning and improving. Each incident response team should evolve to reflect new threats, improved technology, and lessons learned. Many organizations have found that holding a "lessons learned" meeting with all involved parties after a major

incident, and periodically after lesser incidents, is extremely helpful in improving security measures and the incident handling process itself.

The "Lesson Learned" control includes:

- routine sharing of data on information security incidents among the parties responsible for receiving reports and managing investigations;
- periodic reports summarizing the data derived from this sharing.

Lessons learned meetings provide other benefits. Reports from these meetings are good material for training new team members by showing them how more experienced team members respond to incidents. Updating incident response policies and procedures is another important part of the lessons learned process.

Collection of evidence: Where an investigation has been initiated as part of possible disciplinary or legal action, evidence should be collected, retained and presented in a manner that follows documented procedures and conforms to accepted practices. Control includes:

- specifying who may initiate an investigation, and on what basis;
- specifying the necessary documentation to initiate an investigation, and the documentation required as the investigation proceeds;
- securing and maintaining the integrity of copies of paper records, including "originals" if such exist;
- securing and maintaining the integrity of copies of electronic records or other data on computer media relevant to the incident;
- observing appropriate procedures to assure "chain of custody" for any information collected.

When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the law enforcement early in any contemplated legal action and take advice on the evidence required.

Conclusion

All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities, analyzing the nature, mechanics, and effects of the vulnerabilities, and developing response strategies for detecting and repairing the vulnerabilities.

Before the attack, companies need to organize and train cross-disciplinary central security incident response teams - CSIRT. A CSIRT will receive requests for assistance and reports of threats, attack, scans, misuse of resources, or unauthorized access to data and information assets. They will analyze the report and determine what is happening and to mitigate the situation and resolve the problem.

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

Where evidence is required, it should be collected to ensure compliance with legal requirements.

Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

Organizations should use the lessons learned process to gain value from incidents. There should be mechanisms in place to enable the types, volumes and costs of information security incidents to be quantified and monitored.

References

1. ISO/IEC 27001:2005 Information technology - Security techniques - Information Security Management Systems - Requirements
2. ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management
3. Blyth, Michael: *Business Continuity Management*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2009
4. Gupta, Jatinder: *Handbook of Research on Information Security and Assurance*, Information Science Reference, Hershey, New York, 2009
5. Janczewski, Lech: *Internet and Intranet Security Management: Risks and Solutions*, Idea Group Publishing, 2000,
6. Lacey, David *Managing the Human Factor in Information Security*, John Wiley & Sons Ltd, West Sussex, England 2009
7. Northcutt, Stephen: *Computer Security Incident Handling Step By Step*. The Sans Institute, 1998.
8. Tipton, Harold; Krause, Micki: *Security Management Handbook* 5th ed, Auerbach Publications, 2005
9. Tulloch, Mitch: *Microsoft Encyclopedia of Security*. Microsoft Press, Redmond, WA, 2003