Committee for National Security Systems (CNSS)

CNSS-048-07

National Information Assurance (IA) Approach to Incident Management (IM)

May 2007

Prepared By
Investment in Detection, Response, and Recovery Technology Working Group
Committee on National Security Systems

Chair

Foreword

As a result of increasing computer security incidents and decreasing warning time for those incidents, the traditional step-by-step, linear incident response model has become outdated and does not nurture the highly efficient capability that is needed to handle incidents in today's threat environment.

As the traditional linear process has become less effective over time, a new model of Incident Management (IM) has emerged that emphasizes integration of incident-related services into a single, comprehensive program that focuses on incident preparedness, regardless of the nature of the incident.

The evolved IM approach focuses on networking incident-related services to minimize disruption to an organization. IM takes a proactive stance through continuous program activities, rather than a reactive stance of handling individual incidents.

In assisting organizations to transition towards a more evolved model of IM, the National Information Assurance (IA) Approach to IM paper's intent is to provide a set of identifiable actions and recommended future actions for the Committee on National Security Systems (CNSS). The paper promotes a more cohesive approach to capitalize on existing and new strategic partnerships throughout the government and both public and private sectors. The goal is to enhance, expand, and diversify the Committee's role and focus on IM within the national security systems (NSS) community.

/s/
JOHN G. GRIMES

The Need for Incident Management (IM)

As organizations have become increasingly reliant on information technology resources, the number of threats against those resources has sharply increased, as has the potential harm each poses to public and private organizations. Although many organizations have implemented strong defenses against such threats in the form of traditional incident response measures, this approach to detecting, responding to, and recovering from incidents has become less effective over time. To be more effective, the response to these evolving threats and risks posed by computer security incidents requires an incident handling capability that better prepares for and manages incident events. This shift from response to management marks a key development in incident handling. A program management approach to handling incidents broadens response to emphasize prevention, better component integration, and real-time improvements to the process— all weak elements in the traditional incident response model. As a result of these improved measures, organizations' incident handling capabilities are increasingly dynamic and evolving for effectively managing incidents, rather than simply responding to them.

In addition to countering the growing complexity of incidents, an IM approach recognizes that incident handling solutions may be different for incidents within different domains. IM requires a programmatic approach that places emphasis on pre-incident activities: planning and policy, awareness, and detecting and identifying risks. Furthermore, IM is characterized by greater integration of technical capabilities and personnel roles, as well as the concurrent operation of all incident handling components, rather than the linear and sequential process of a more traditional incident response approach.

Standards and Sound Practices

Often, organizations structure their incident response capability to implement a model similar to the classic six-step incident response model shown in Figure 1, in which preparation leads to detection followed by containment, which in turn permits eradication and recovery, and feedback into the next preparation stage.

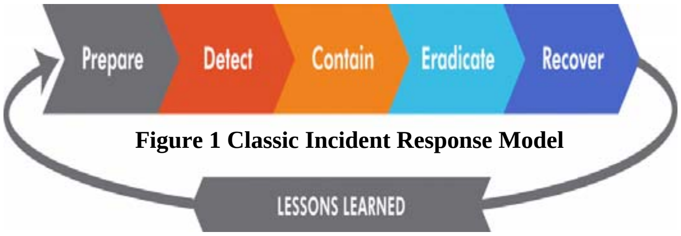

Figure 1 Classic Incident Response Model

When implemented, performed, and supported properly, the traditional six-step incident response approach can provide some strong benefits. The structured approach facilitates consistent and sound incident handling practices that reduce the business impact of incidents. The preparation and lessons learned steps promote a more effective incident response team and capability. Unfortunately, many organizations that implement the six-step model do not follow it effectively. If one phase in the linear process is not completed, the cycle may stop midstream. Furthermore, important steps, particularly lessons learned, are often skipped because the incident response program is too focused on containment, eradication, and recovery. The incident response team and the organization do not learn all they can from incidents and, subsequently, the incident response capability and security measures do not benefit from the lessons learned.

Overview of IM

Better prevention and more effective handling of incidents can be achieved by integrating an IM program approach into the daily business functions of the organization and establishing strong linkages among those functions. The linear process depicted in the traditional six-step model is insufficient for supporting the IM approach because that model depends on phases and events triggering activity in subsequent phases.

A newly evolving IM methodology focuses on integrating incident-related services into a single, comprehensive program management approach to minimize disruption to an organization. IM takes a proactive stance through continuous monitoring and program improvement activities, rather than a reactive posture focused on responding to individual incidents. As incident handling evolves from responding to managing, it merges into concepts like vulnerability management and the enterprise approach to patch management. IM also eliminates the use of "scripted" incident response policies and procedures that are not practical and do not support an organization's business needs, because it ensures that the appropriate parties are involved in policy and procedure creation, validation, and maintenance via the continuous lessons learned and improvement process.

The IM approach functions as a holistic program whereby a change in one program component is supported by other program components. The central preparation and prevention component, as seen in Figure 2, offers program management and is integral to ensuring each part of the program interacts appropriately with all other parts of the IM capability. The ultimate goal is to make IM a more holistic, networked, and self-improving process.

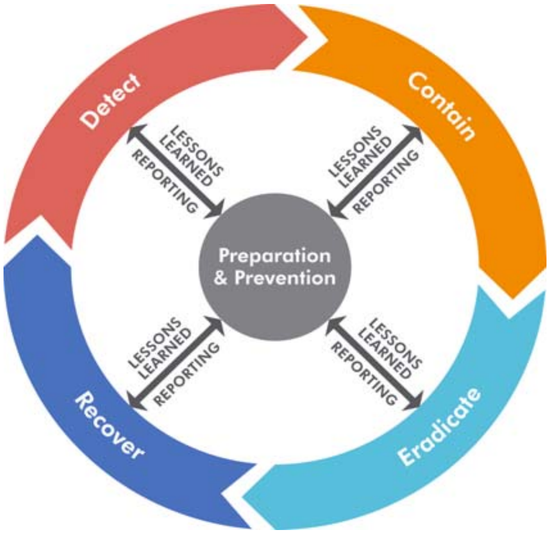

Figure 2—Incident Management Model

Program Approach Versus Response Approach

The program approach to managing incidents integrates the traditional incident response components that are depicted in Figure 1, ensuring that the technical and management capabilities of each component work together to more effectively support incident handling.

Underlying all of the components and capabilities of incident response are fundamental principles of IM—planning, communication, and evaluation.

Planning includes developing strategies and goals, obtaining senior management support, establishing an organizational approach to incident handling, and ensuring IM is effectively incorporated into the rest of the organization's security program.

Communication involving internal and external audiences is critical for facilitating effective response efforts, because so many individuals and groups need to be prepared to communicate quickly when incidents occur; an example of a common issue is managing the release of sensitive information while meeting incident reporting requirements.

Evaluation, which is critical to a successful IM program, includes collecting feedback, performing lessons learned activities, and establishing and gathering metrics on the incident response capability to determine how processes can be improved.

Organization Needs

Organizations have different needs for IM depending on their structure, size, business functions, and other factors. Many organizations already have made major investments in IM-related technology and processes; therefore, guidelines for an organization’s IM approach need to be flexible, scalable, and technology-independent so they can work for any organization. In addition, an organization should progress toward an advanced IM capability by gradually building and enhancing its existing incident handling program. The same methodology is also used to assist organizations in improving individual IM capabilities, such as computer forensics or incident reporting, that have presented challenges in supporting the organization’s mission.

Sharing Information

In the networked world, most incidents will affect multiple organizations and, as a result, organizations must be able to communicate effectively to reduce the risk to the overall community. The lack of a consistent language for describing computer security incidents seriously hampers the ability to share information and reduces the utility of those sharing arrangements that do exist. Standards such as the Common Vulnerabilities and Exposures (CVE) list and the Open Vulnerability and Assessment Language (OVAL) are fairly mature, but many organizations have not adopted them and implementation in commercial software is not consistent. CVE and OVAL make an important contribution to standardizing the language but are not intended to be the full taxonomy required to describe computer security incidents.

Although there are limited requirements for organizations to report incidents, for IM to be effective on an enterprise level across multiple organizations, information sharing must occur at the program level of the individual organizations. An understandable roadblock to sharing information in this manner is the reluctance of organizations to expose vulnerabilities by disclosing their incident history. Even if the vulnerability has been mitigated by the organization, public awareness of the event may result in a loss of credibility and confidence, damaging the reputation of the organization.

In the absence of specific information sharing requirements related to incidents, some solutions have been offered to bridge the need to share information with the reluctance to do so. Some secure mediums and independent organizations have been set up to allow international private and public sectors to exchange incident information through a trusted and confidential exchange.

Addressing national security systems (NSS) presents additional obstacles to information sharing because of the classified nature of the information on those systems. Even when the NSS itself is unclassified, the existence of a specific vulnerability is probably classified. Information sharing is an area that will require additional attention to determine workable solutions.

Conclusion

An increase in computer security incidents and the unpredictability of these incidents makes the traditional step-by-step, linear incident response model outdated. This type of traditional model is too highly focused on responding to individual incidents and does not adequately emphasize preventing incidents and improving incident handling. Lessons learned, which are often skipped in the traditional model, must be incorporated throughout the incident handling process.

As the traditional linear process has become less effective over time, a new model of IM has emerged that emphasizes integration of incident-related services into a single, comprehensive program focused on incident preparation and prevention. This IM approach incorporates the program management that is integral to ensuring that each part of the program interacts appropriately with all other parts of the organization’s incident handling capabilities and that no single part operates independently of the whole program.

In addition, an IM program can help organizations to overcome some of the incident handling obstacles they face where incident response measures fail. This includes tailoring capabilities to address specific organizational needs, not just meeting legislative incident response requirements. This strategic IM approach strives to achieve a self-improving incident handling process that is implemented across the enterprise. Finally, the strategic IM approach is proactively structured to reduce the impact of incidents, minimize damage, and contain problems.

Actions and Recommended Future Actions

The Committee on National Security Systems (CNSS) has provided a set of identifiable actions and recommended future actions in order to form a more cohesive approach and capitalize on existing or new strategic partnerships throughout the government and both public and private sectors with the goal of enhancing, expanding, and diversifying the Committee's role and focus on IM within the NSS community and those communities that interface with NSS.

Actions:

1. The CNSS Secretariat shall be responsible for updating CNSS issuances, as applicable and appropriate, on IM as relevant to NSS.
2. The Investment on Detection, Response, and Recovery Technologies (IDRRT) Working Group shall develop a national policy, as relevant to NSS/NSI, on IM.
3. The CNSS shall identify and appoint a Committee/Subcommittee Member to champion, support, and oversee the collaborative efforts in developing strategic partnerships on IM and report status to the Committee/Subcommittees.
4. The CNSS shall assign the Education, Training, and Awareness Working Group to conduct an evaluation for identifying, developing, and establishing training and certification standards with regard to IM.
5. The CNSS shall assign the Architecture and Information Sharing Working Group and IDRRT WG to work together to consider information sharing requirements for IM.

Recommended Future Actions:

1. The IDDRT WG shall create a roadmap for IM partnership with established Incident Response Centers, Coordination Groups, and Response Teams.
2. The Committee shall request that a CNSS Representative be included, as an observer at meetings, conferences, or other activities of existing organizational structures (e.g., National Cyber Response Coordination Group, Information Technology – Information Security Analysis Center…) order to maintain currency on IM matters.
3. The IDRRT WG shall research the feasibility of identifying, developing, and establishing training and certification standards, via or in conjunction with academia, for IM or leverage existing education, training, and awareness resources/assets.

Appendix A

Abbreviations and Acronyms

CNSS	Committee on National Security Systems
CVE	Common Vulnerability and Exposures
FISMA	Federal Information Security Management Act
IM	Incident Management
IT	Information Technology
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security Systems
OMB	Office of Management and Budget
OVAL	Open Vulnerability and Assessment Language

Appendix B

References and Resources

1. Committee on National Security Systems (CNSS) Investment in Detection, Response, and Recovery Technology (IDRRT), *Frequently Asked Questions (FAQ) on Incidents and Spills*.
2. NIST Special Publication 800-61: *Computer Security Incident Handling Guide*
3. Common Vulnerabilities and Exposures (CVE)
4. Open Vulnerability and Assessment Language (OVAL)
5. Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002.
6. Office of Management and Budget (OMB) Circular A-130.
7. The National Strategy to Secure Cyberspace, February 2003.
8. The National Security Strategy of the United States of America, March 2006.
9. National Security Directive (NSD), 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, 5 July 1990.

Appendix C

Glossary[1]

Classified information spillage. Security incident that occurs whenever classified data is spilled either onto an unclassified or information system (IS) with a lower level of classification.

Clearance. Formal security determination by an authorized adjudicative office that an individual is authorized access, on a need-to-know basis, to a specific level of collateral classified information (Top Secret, Secret, Confidential).

Computer security. Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated.

Computer security incident. See incident.

Denial of service. Any action or series of actions that prevents any part of an IS from functioning.

Firewall. System designed to defend against unauthorized access to or from a private network.

Incident. Assessed occurrence having actual or potentially adverse effects on an information system.

Incident handling[2]. All activities and procedures involving security incident detection, containment, eradication, reporting and recovery.

Incident management (IM)[3]. A program management approach to incident handling emphasizing prevention, networked component integration, and real-time improvements to incident handling procedures.

Incident response[4]. A reactive approach to handling computer security incidents, often following a traditional linear model consisting of five phases: prepare, detect, contain, eradicate, and recover.

Information assurance (IA). Measures that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information security policy. Aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

Information system (IS). Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

[1] All terms and subsequent definitions are from CNSS Instruction No. 4009: *National Information Assurance (IA) Glossary*, unless otherwise noted.

[2] This term's definition was created for the purpose of this white paper in accordance with CNSS guidance on related terms and subject matter.

[3] Ibid.

[4] Ibid.

Intrusion. Unauthorized act of bypassing the security mechanisms of a system.

Malicious code. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an IS. (See Trojan horse.)

National security information (NSI). Information that has been determined, pursuant to (NSI) Executive Order 12958 (as amended) (Ref b.) or any predecessor order, to require protection against unauthorized disclosure.

National security system (NSS). The basis for the identification of national security systems is the definition provided in law (44 U.S.C. 3542(b)(2), which was established by FISMA, Title III, Public Law 107- 347, December 17, 2002):

"(2)(A) The term *national security system* means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

(i) the function, operation, or use of which—
(I) involves intelligence activities;
(II) involves cryptologic activities related to national security;
(III) involves command and control of military forces;
(IV) involves equipment that is an integral part of a weapon or weapons system; or
(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified1 in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications)."

Systems not meeting any of these criteria are not national security systems. (Further guidance on making NSS determinations is available in NIST Special Publication 800-59 Guideline for Identifying an Information System as a National Security System, Appendix A.)

Network. IS implemented with a collection of interconnected nodes.

Risk. Possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability.

Risk assessment. Process of analyzing threats to and vulnerabilities of an IS, and the potential impact resulting from the loss of information or capabilities of a system. This analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

Risk management. Process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an IS. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations. (NIST Special Publication 800-53)

Spillage. See classified information spillage.

User. Individual or process authorized to access an IS.