Incident Management

Georgia Killcrece

December 2005

ABSTRACT: An incident management capability is the ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. This involves defining a process to follow with supporting policies and procedures in place, assigning roles and responsibilities, having appropriate equipment, infrastructure, tools, and supporting materials ready, and having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way.

BACKGROUND

In 1988, the first large-scale Internet incident (the release of a self-replicating program) occurred and came to be known as the "Internet Worm" or the "Morris Worm." In the aftermath of that incident, the Defense Advanced Research Projects Agency (DARPA) charged Carnegie Mellon University's Software Engineering Institute with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. This center, located at the SEI, was named the CERT Coordination Center (CERT/CC).[1]

The CERT/CC (a type of computer security incident response team, or CSIRT[2]) was formed to provide response to computer security incidents on the Internet and to serve as a prototype for establishing similar operations in other communities. Today, there are a number of different types of organizations and resources available to help handle and respond to computer security incidents [CERT 08, FIRST 08, Killcrece 03b, US-CERT 08, for example].

Over the last twenty years, the CERT Program has seen an evolution from organizations that performed incident response in a purely reactive, ad hoc approach to

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

[1] Carnegie Mellon, CERT Coordination Center, and CERT are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

[2] For more information on CSIRTs, see the corresponding BSI article Defining CSIRTs [Ruefle 08].

those implementing a more formal, comprehensive approach. Having such an organized, strategic plan to handle computer security events and incidents from their detection through their resolution is known as an incident management capability. Having this capability implies the end-to-end management for controlling or directing how security events and incidents will be monitored and detected, responded to, or recovered from, to ensure the organization can continue to meet its operational mission. To do this, the capability must be designed and managed to provide

- policies and procedures that define and assign the appropriate roles and responsibilities for personnel involved in incident management activities
- equipment, infrastructure, tools, and supporting materials to protect systems, detect suspicious events and incidents, assist in recovery, and support the resumption of operations
- qualified staff who are trained to perform consistent, reliable, high-quality incident management functions

OVERVIEW

One of the challenges to be faced in building an effective incident management capability is understanding the broader scope of incident management work. It is no longer enough to just "handle" events and incidents in a technical security context. Twenty years ago, many organizations relegated this responsibility to their IT or Security department—it was a "technical" issue to be solved, and these teams typically handled incidents in isolation. Back then there was limited sharing of knowledge about incidents or communication about the results to stakeholders across the enterprise to identify broader risk to the mission, reputation, brand, etc. But those days are gone, and today enterprises must be able to incorporate security into every aspect of their operations. (See the Governance & Management content area.)

Since incidents can have far-reaching consequences and implications affecting the internal protection (confidentiality, availability, integrity) of critical data and assets, privacy information, supply chain contacts, and beyond, incident management actions can involve many groups within the enterprise—board room and C-level managers[3] who handle governance, budget, and strategic issues; IT,

[3] C-level managers include chief information officers (CIOs), chief security officers (CSOs), chief risk officers (CROs), and other similar executives.

CSIRT, and security staff who coordinate and implement incident response actions; groups such as human resources, privacy officers, risk, audit, legal, and public relations staff who might be brought in to handle aspects of an incident related to their areas of expertise; and others. External groups may also be involved, including regulatory bodies, law enforcement, and possibly other computer response security organizations.

For computer security incident response to occur in an effective and successful way, all the tasks and processes being performed must be viewed from an enterprise perspective. This means identifying the interactions and communications that need to occur, how tasks are done and how the processes relate, how information is exchanged, and how actions are coordinated—no matter who is performing the work.

Focusing only on the response part of the process, for example, misses key actions that if not done in a timely, consistent, and quality-driven manner will impact the overall response, possibly delaying actions due to the confusion of roles and responsibilities, ownership of data and systems, and authority. Response can also be delayed or ineffective if communications are not clear, if appropriate contacts are not known, or if the quality of information provided is inadequate, incomplete, or inaccurate. Any impact on the response timeliness and quality can cause further damage to critical assets and data during an incident.

How a computer security incident management capability is instituted or structured within an organization can differ greatly. Because so many groups can be involved, depending on the nature of the incident and the required response, having defined interfaces and assigned roles and responsibilities is a key requirement. Often, even though others throughout the organization may be involved, a core group is established to help coordinate the overall incident management function. This core group may take the form of a defined group of people or a designated unit such as a CSIRT. This can be seen in organizations such as

- local, state, and provincial governments
- educational institutions and research networks
- national initiatives

The group can also be part of other security, IT, risk management, or business continuity functions. This is common in commercial industry, where this function may be served by

- crisis management teams
- resiliency teams

- security response teams

Some organizations may choose to outsource this capacity to a managed security service provider.

In whatever way the incident management capability is structured, any group responsible for performing incident management actions must recognize that they don't operate in isolation and that communication and interaction with all appropriate entities is key—whether internal to the organization or with other external contacts. An overall security strategy must be implemented to ensure that all operational units understand their role in the incident management process.

In this article we describe five high-level processes[4] that compose a model for the various functions that are undertaken as part of an incident management capability:

- Prepare/Sustain/Improve (Prepare) – establish, sustain, and improve the CSIRT
- Protect Infrastructure (Protect) – make changes in the infrastructure to protect systems or mitigate an ongoing computer security event
- Detect Events (Detect) – recognize and report events when they occur and look for indicators that might identify future events/incidents
- Triage Events (Triage) – categorize, correlate, and prioritize events and assign them to someone for further investigation and possible response
- Respond – plan, coordinate, and carry out effective response to incidents

This incident management model can be used by an organization to identify what processes it is already performing, benchmark against what others are doing (including third parties), identify where gaps exist, and highlight what interfaces need to exist between all the processes and all the participants. It can be used to help build a consistent, reliable, and repeatable set of processes to identify, detect, analyze, and respond to computer security incidents.[5] This model can also be used to help an organization

---

4 These are explained in more detail in [Alberts 04] (see Section 2 of that document).

5 Or (as might be the case) used as an inward focus for tracking down events/incidents within the organization that may be launching attacks against other organizations.

- identify the components of such a capability and the processes that should be in place to perform effective incident management
- develop workflows and tasks that can be followed to implement or improve the incident management capability

INCIDENT MANAGEMENT AS PART OF THE CERT® RESILIENCY ENGINEERING FRAMEWORK

Very often in organizations and institutions, there is a question of where incident management fits—is it in IT operations? Is it part of security management? Is it in risk management? Is it in disaster recovery? Over the past few years, members of the SEI's CERT Program have been working with the Financial Services Technology Consortium (FSTC) to identify mature practices in banking and financial services industries. Research and development in this area has produced a framework that shows how all these areas fit together and complement each other. This framework is called the CERT® Resiliency Engineering Framework (REF).[6]

Operational resiliency is the organization's ability to sustain the mission in the face of operational risks such as those resulting from

- failed internal processes
- inadvertent or deliberate actions of people
- problems with systems and technology
- external events

Operational resiliency depends on effective management of core operational risk management activities such as security management (SM), business continuity and disaster recovery (BC/DR), and IT operations.

The REF model states that SM, BC/DR, and IT are three separate areas, but they work together to support and sustain operational resiliency. These three areas (SM, BC/DR, IT)

- are dependent on each other to complete their missions

---

[6] See the CERT® Resiliency Engineering Framework, v0.95R [REF 08]. The framework is the foundation for a process improvement approach to security and business continuity.

- share the same goals, objectives, requirements—driven by organizational needs
- focus on the protection and productivity of the same objects
- rely on shared, common practices

Risk management focuses on keeping critical objects or assets productive by limiting risk and managing the impact of realized risk.

Operational resiliency is the concept of managing operational risk to ensure mission viability by being able to adapt to new risks as they emerge and acting before reacting. Because resiliency is a function of risk management and security is a risk management activity, security contributes to operational resiliency through the risk management link. Incident management is one part of security management and therefore also a risk management activity.

The REF model also describes a foundation for a process improvement approach to security and business continuity. It does this by describing a collection of 21 capability areas. One of those capability areas is "Incident Management and Control (IMC)."

The IMC capability within REF, just like the IM Process Model, promotes the establishment of processes for detecting, analyzing, responding to, and learning from incidents to

- prevent the impact of unanticipated risks
- manage their impact when realized
- provide a source of knowledge to improve protection strategies and continuity and sustainability plans and practices

Having an incident management capability in place contributes to the operational resiliency of the organization. Once again, however, since incident management is a risk management activity, it must be recognized that technology solutions are not the only important part of the response. Achievement of the business and operational mission must be balanced in light of any response strategies, and organizational process and human actions must be taken into account. Technology alone does not achieve success.

The definition of an incident within the REF context is very broad; it can relate to anything that disrupts achieving the mission. The focus of computer security incident management is on a smaller subset of events: those that are malicious or unauthorized.

The REF model also highlights other capability areas that relate to or are influenced by activities from the incident management and control capability, such as vulnerability management, compliance management, service continuity, monitoring, root cause analysis, training and awareness, and communication. To be successful at incident management, an organization must also look at being successful in these areas and defining the interfaces between them and the incident management process.

As new products, services, or technologies are deployed, computing infrastructures or business partners change, or business strategies are realigned, organizations need to understand the importance of aligning their incident management activities with broader enterprise activities.

Approaching security in this managed and strategic way, sharing the vision, balancing enterprise-wide drivers and costs with business risks, etc., can enable the security effort to ultimately be more successful [REF 08].

INCIDENT MANAGEMENT PROCESS MODEL

Incident management, then, can be seen as an abstract, enterprise-wide capability, potentially involving every business unit within the organization. It can be viewed as a subset of the organization's broader security, risk, and IT management activities and functions. It can often cross into general security and IT management tasks and practices. Because of the large amount of staff inside and outside an organization who might be involved, it is important that a plan exists for how these pieces interact with each other so that incidents are handled in a smooth and timely manner.

To be successful, this plan should

- integrate into existing processes and organizational structures so that it enables rather than hinders critical business functions
- strengthen and improve the capability of the constituency, where required, to effectively manage security events and thereby keep intact the availability, integrity, and confidentiality of an organization's systems and critical assets
- support, complement, and link to any existing business continuity or disaster recovery plans where and when appropriate
- support, complement, and provide input into existing business and IT policies that impact the security of an organization's infrastructure
- implement a command and control structure, clearly defining roles and responsibilities, as well as accountability for decisions and actions

- be part of an overall strategy to protect and secure critical business functions and assets
- include the establishment of processes for•detection and triage
  - categorization and prioritization
  - notification and communication
  - analysis and response
  - collaboration and coordination
  - maintenance and tracking of records

Figure 1 provides a graphical representation of the CERT incident management process model.

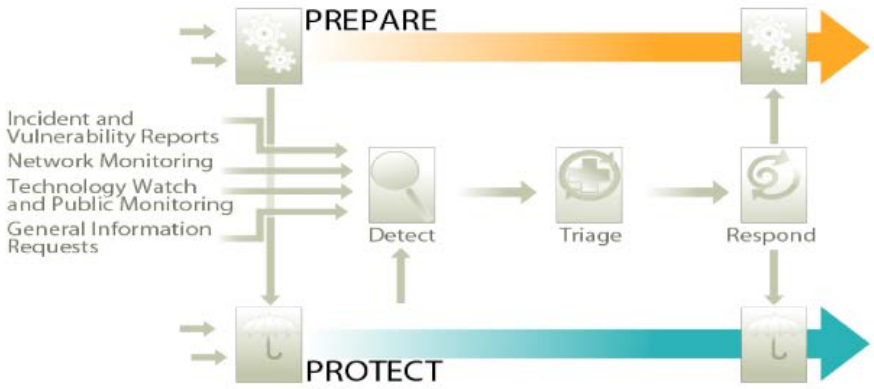

Figure 1. Incident management best practice model

The figure can be explained as follows:

- The Prepare and Protect processes are shown as continuous, ongoing processes above and below the Detect, Triage, and Respond processes. This is signified by the arrows going across the diagram and by having the icons for each at the beginning and end of the arrows. These processes involve putting into place all the necessary staff, technology, infrastructure, policies, and procedures needed for incident management activities to occur in a timely, coordinated, and effective manner. The use of the arrows surrounding the Detect, Triage, and Respond processes show that Prepare and Protect support and enable the other processes.
- The small arrows coming into the Prepare and Protect process indicate requirements, policies, or rules that will govern the structure and function of these processes. These arrows also indicate incoming process improvement recommendations.
- The line from the Prepare to the Protect process signifies a handoff between these two processes. In this case, the information passed is process improvement recommendations for changes in the computing infrastructure

that result from a postmortem review done in the Prepare process. These changes in the infrastructure, for example, will help harden and secure the infrastructure to help prevent similar events or incidents from happening or the same activities from re-occurring.

- The Detect, Triage, and Respond processes are shown in sequence as information coming into the Detect process is evaluated to determine whether it is actionable and needs to be passed on to the Triage process for further analysis and assessment. If in the Triage process the received information (an incident report, a vulnerability report, a general information request, or a suspicious event) requires a response, it is passed on to the Respond process.
- The arrow going from Protect to Detect indicates the passage of any incident or vulnerability reports that may result from infrastructure evaluations. It is possible that during an evaluation or assessment, a vulnerability, ongoing incident, or remnant of a past incident may be discovered. This information would need to be passed to the Detect process for further evaluation.
- The arrows going from the Respond process to the Prepare (or Protect) process signify the handoff of process improvements and corresponding incident data or response actions and decisions where appropriate. The handoff from Respond to Prepare passes this information to the postmortem review subprocess within the Prepare process (and similarly as it relates to the Protect process).

Over the last several years a number of books and articles have been written about incident management and incident response activities [Fraser 97, ISS 01, Kruse 02, Mandia 01, SANS 03, Schultz 02, Sokol 00, van Wyk 01]. Although many use slightly different terminology, a similar set of tasks is discussed. Most of the tasks include detecting and reporting events and incidents, containing and resolving incidents, and recovery of systems. Other steps that relate to these functions include identification, containment, eradication, investigation, and notification.

In this context, incident management is not just the application of technology to resolve computer security events. It is also the development of a plan of action, a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency.

Building an Incident Management Capability

In developing an incident management capability, an organization must determine who is currently performing incident management and related tasks and identify who will be part of the incident management team. Identifying people across the enterprise who must work together to analyze and resolve incidents and then assigning them specific roles and responsibilities is one of the most critical tasks that can be done in building and improving a capability.

Getting management buy-in and consensus within the organization is always the first recommendation for implementing a formalized process. This establishes a foundation that is needed for success. If possible, have executive management establish a policy and corresponding procedures that define the incident management process and key participants. This policy and set of procedures must then be announced, taught, and enforced.

The purpose of each group within the capability and their roles and responsibilities should be defined and documented. Corresponding workflows that illustrate how an incident flows through the incident management process, including detection, reporting, triage, analysis, response, and closure, should be completed.

Incident reporting forms, guidelines, and procedures should be created and distributed to all organizational employees, including becoming part of employee orientation programs and annual security training. If employees do not know how and what to report, computer security events and incidents might occur that are not detected in a timely manner.

Postmortems on all key incidents should be done to determine ways to improve infrastructure protection strategies and response policies, procedures, and processes. Mock incident exercises should be conducted at least on an annual basis to test that everyone knows what to do, how to report, and how to respond.

Incident management, just like other key security management functions, must be shown to be important to the organization.

Process Diagrams

Process modeling techniques are useful for illustrating an abstraction of a business process, highlighting key activities and artifacts required to conduct the process. Figure 2 shows a simplified example.

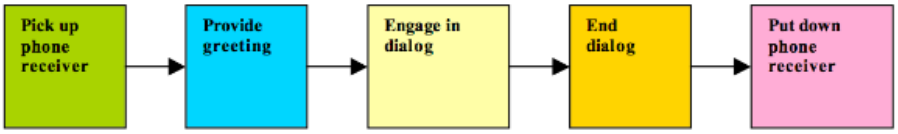

Figure 2. A simple example of a process diagram for answering the telephone

A workflow model is a specific type of process modeling technique, providing a description of how tasks are done, by whom, in what order, and how quickly. It differs from other modeling techniques, such as data flow diagrams and flow charts, because it specifically defines interrelationships and dependencies among tasks and activities. Understanding these interrelationships and dependencies

among tasks and activities is important when analyzing the risk inherent in a business process such as incident management.

Benefits to be gained by mapping the incident management processes include

- enabling a comprehensive understanding of the current (as-is) state
- identifying risks to successful completion of the mission of the incident management capability
- supporting decisions about improvements to incident management operations (to-be state)

Said another way, mapping the incident management processes can help an organization understand all the activities, roles and responsibilities, technology, interfaces, and dependencies that are occurring during the incident response activities and how they relate to and depend on one another. It also can highlight missing activities or those with inherent weaknesses that can be then targeted for improvement. Risks that affect the successful response to incidents can be recognized and mitigated. By understanding the whole set of processes, improvements can be made in to avoid the waste of isolated fixes.

So, for each high-level process, the categories and descriptions that are used in describing the incident management workflow are listed in Table 1. These provide details about multiple aspects of a process and its associated activities (the goals and objectives for doing a piece of the process, what triggers it, what rules or regulations ”drive” the need to do it, how you know it has been completed, inputs and outputs, subprocesses, etc.). Substituting explicit (real) names, labels, and associations in place of these generic terms provides an organization with a range of information that can be used to pinpoint where processes are well defined and where they may not be. Handoffs (or interfaces) are the exchanges between actors (e.g., from one person to another, a technology to a person, a person to a technology, or even technology to technology) and occur between the major processes, from Detect to Triage, Triage to Respond, etc.

Table 1. Incident management workflow description information categories

Information Category	Description
Mission/objectives	The goals for this process. Defines what should be accomplished by the successful completion of the process activities.
Triggers	Activities that initiate the process. Could be an event or an input.
Completion criteria	Conditions that must be met for the process to be successfully completed.

Policies and rules	Any policies, laws, regulations, rules, etc. that govern this process or its outputs.
General requirements	Any type of supporting information, procedures, or technology that may be needed to successfully perform activities associated with this process.
Inputs	The required inputs for this process.
Input name	The name of the input.
Input description	A short description of the input, including the sending process.
Input form	The form of the input (usually verbal, electronic, and/or physical).
Outputs	The possible outputs of this process.
Output decision	Any relevant decisions that will produce one output versus another.
Output name	The name of the output.
Output description	A short description of the output, including its destination.
Output form	The form of the output (usually verbal, electronic, and/or physical).
Subprocess	All of the subprocesses or activities for this process.
Subprocess name and diagram	The abbreviation (e.g., D1 for the first subprocess of Detect), the name (e.g., Notice Events), and a simple diagram indicating the relevant box on the process flow as a visual reference for the reader.
Subprocess require-ments	The requirements for this subprocess, namely, what must occur for this subprocess to be successful. Also included are any inputs and outputs related to these subprocess requirements.
Written procedures	Any procedures that must be followed by those conducting this subpro-cess.
Key people	The roles of key people who may conduct this subprocess or who need to be involved in any discussions or decisions.
Technology	The types of supporting technology that may be needed to successfully perform this subprocess.

Other/miscellaneous	Any other relevant items for this subprocess.

One of the main objectives for undertaking this incident management process work is to show that it is an enterprise-wide, distributed capability. Over the years a number of problems resulting in ineffective implementations of incident management capabilities and processes have been seen, such as those

- that do not support the organizational mission, goals, or business drivers
- with no corresponding policies or procedures to govern their actions
- with no defined processes, accountability, or roles and responsibilities in place
- that provide unwanted/unneeded, redundant, or duplicate services
- that were established without being integrated into existing processes, resulting in a lack of communication, coordination, and data sharing where needed

For example, if we focus only on the ”response” part of a process, other key actions can be missed (e.g., analysis, coordination, involvement of management, notification to other external parties) that might impact the overall response—possibly delaying actions, causing ineffective communications, or the provision of poor quality information about an event or incident. Any impact on the response timeliness and quality can cause further damage to critical assets and data during an incident.[7] Identifying and defining these interfaces and the roles and responsibilities of the various participants across the organization is a key part of setting up any effective incident management capability.

Business Case

When the Internet Worm incident occurred in 1988, the size of the network was estimated at 60,000 hosts. The January 2008 Internet Domain Survey shows more than 541.6 million hosts advertised in the Domain Name Service [ISC 08]. Clearly, no single incident management capability is able to effectively serve such a vast constituency, and this illustrates the need for more teams and capabilities. The number of teams established to respond to attacks has grown, but not every organization has a defined or formalized incident management capability.

---

[7] Lack of communications and coordination during the handling of events and incidents is often raised at postmortems and after-action reports.

Incident management capabilities that are institutionalized as CSIRTs or security teams often face the hurdles of having to justify the need for their existence, gaining that support and understanding for the problems they are trying to address, and getting key management buy-in. Organizations such as the Government Forum of Incident Response and Security Teams (GFIRST), FIRST [FIRST 08], TF-CSIRT, and APCERT promote the formation of teams by providing a forum for information sharing, training, and best practice guidance to help teams develop their capabilities.

The general public is becoming more aware of security breaches. Reports concerning breaches at financial institutions, universities, and other organizations resulting in the theft of hundreds of thousands of consumer credit card numbers and other personal information have been reported in the media.[8] In some of these reports, equipment containing sensitive information was stolen or systems contained software vulnerabilities that had been exploited to gain unauthorized access to the information.

Many other sources, such as business surveys and web sites, provide information on the cost and extent of attacks. A survey conducted among security executives and law enforcement personnel by CSO magazine in cooperation with the United States Secret Service and the CERT/CC indicated an estimated $666 million in losses due to electronic crime. A set of surveys conducted by the Australian High Tech Crime Centre, the Australian Federal Police, Queensland Police, NSW Police, Victoria Police, Tasmania Police, South Australia Police, Northern Territory Police, Western Australia Police, and AusCERT presents an analysis of computer attacks and misuse trends in Australia over the 12 months prior to February 2005 [AusCERT 05].

---

[8] On August 5, 2008, U.S. attorneys charged eleven perpetrators allegedly involved in stealing more than 40 million credit and debit card numbers. This is believed to be the largest "hacking" and identify theft case ever prosecuted by the Department of Justice [DoJ 08].

From another perspective, a variety of regulations and legislation has been introduced in the United States over the last few years in an attempt to address some of these security issues. For example, the California Security Breach Information Act (California Civil Code 1798.82, also referred to as SB 1386) requires organizations that maintain personal information about individuals to inform those individuals if the security of their information is compromised. Other laws and regulations such as HIPAA,[9] GLBA,[10] and SOX[11] affect how information and data are handled in organizations, including how events and incidents are handled and managed. The Federal Information Security and Management Act (FISMA) requires federal agencies to implement some type of capability for responding to computer security incidents [FISMA 02]. All of these point out the growing need for having comprehensive, enterprise-wide policies and procedures with well-defined processes to facilitate responding to incidents.

Agency Inspector General (IG) reports, as well as Government Accountability Office (GAO) reports, also can be drivers to improving incident management practices. Over the past few years, such reports have pointed out deficiencies in federal government information systems and the nation's critical infrastructures [GAO 04].[12]

Other resources that may be helpful in developing a business case for a CSIRT (as well as in establishing an incident management capability) include the following:

- NIST Security Management and Guidance documents, which focus on risk management, security program management, training and awareness, con-

---

9 The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was signed into law on August 21, 1996. This law includes important new protections for millions of working Americans and their families who have preexisting medical conditions or might suffer discrimination in health coverage based on a factor that relates to an individual's health.

10 The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions.

11 The Sarbanes-Oxley Act of 2002 is legislation enacted to protect shareholders and the general public from accounting errors and fraudulent practices. The act is administered by the Securities and Exchange Commission (SEC).

12 As recently as May 2005, the GAO pointed out weaknesses in the effectiveness of security programs to mitigate and respond to cybersecurity threats [GAO 05]. Agencies have reported that some tools are not robust enough to help them do the work (e.g., effectively detect, prevent, remove, or analyze incidents). The report also stated that the Office of Management and Budget (OMB) will incorporate emerging cybersecurity threats in its annual review and evaluation of agency security programs.

tingency planning, personnel security, administrative measures, etc., are available at http://csrc.nist.gov/publications/PubsTC.html, and the Federal Agency Security Practices (FASP) can be found at http://csrc.nist.gov/fasp/.

- In addition to the above, several Homeland Security Presidential Directives have established the importance of developing incident management plans for protecting national critical infrastructures and developing a National Response Plan. These address the need for developing comprehensive plans for incident management preparedness, prevention, response, recovery, and mitigation activities.

While some of these references are clearly government-focused, the information can be useful to other organizations (commercial entities, academic institutions, or national, state, and local agencies) in developing their strategy for a CSIRT or to help support the business cases for developing an incident management capability.

Relevant Metrics

In terms of metrics, a number of different approaches have emerged. For example, guidelines, checklists, and best practice documents (such as the NIST 800 series) are available, such as

"Security Self-Assessment Guide for Information Technology Systems," SP800-26

"Recommended Security Controls for Federal Information Systems," SP800-53

"Performance Measurement Guide for Information Security," SP800-55

"Computer Security Incident Handling Guide," SP800-61

These documents provide benchmark processes and practices that organizations can use to measure their compliance with the guidance or can also use to help build their own processes or implement best practice standards.

The Department of Homeland Security, through US-CERT, has developed a set of federalized metrics adapted from those currently in use by the Department of Defense to evaluate its Computer Network Defense (CND) Service Providers. The U.S. Department of Defense established a directive and instruction (DoD 8530) whereby all DoD components are required to establish and provide for

computer network defense services.[13] These services are built around a framework of functional capabilities that are often provided by an incident management capability and are defined as Protect, Detect, Respond, and Sustain. The CND metrics are used by the DoD to certify and accredit teams. A secondary goal is to ensure a higher quality of protection through increased maturity and understanding of the services provided by the CNDSP. The DoD's evaluation process is used as a measurement of mission effectiveness, operational performance, and functional maturity through a number of critical success factors. Building off these efforts, the CERT Program published the Incident Management Capability Metrics and Incident Management Mission Diagnostic method, to provide a baseline or benchmark of incident management practices and a risk-based approach for determining the potential for success of an organization's incident management capability, respectively.

GLOSSARY

CSIRT	An acronym for a computer security incident response team
event	Any anomalous occurrence or behavior in a system that is relevant to the security of the system.
federalized metrics	A set of metrics that federal agencies can use to evaluate their incident management processes in the areas of Protect, Detect, Respond, and Sustain/Improve.
hacker	A slang term for an individual who gains unauthorized access to computer systems for the purpose of stealing or corrupting data.
honeynet	A collection of high-interaction systems (honeypots) that are probed, attacked, or compromised. Honeynet activity is primarily evaluated to gather information about threats that are being used, how the threats are evolving, and how to identify successful countermeasures against those threats.
honeypot	A system resource whose value lies in unauthorized or illicit use of that resource solely for the purpose of observing the interactions of that system with other external actors.

[13] As outlined in DoD Directive O-8530.1, "Computer Network Defense," and DoD Instruction O-8530.2, "Support to Computer Network Defense."

incident	US-CERT defines an incident as the act of violating an explicit or implicit security policy. This can include any real or suspected adverse event in relation to the security of computer systems or computer networks. Any real or suspected adverse event in relation to the security of computer systems or computer networks.
incident management	The performance of reactive and proactive services to help prevent and handle computer security incidents.
incident response	Actions taken to resolve or mitigate an incident, coordinate and disseminate information, and implement follow-up strategies to stop the incident from happening again.
phishing	The act of sending email falsely claiming to be a legitimate entity in an attempt to fool the recipient into surrendering private information.

BIBLIOGRAPHY

[Alberts 04]

Alberts, Christopher; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.

[Allen 01]

Allen, Julia H. *The CERT Guide to System and Network Security Practices*. Reading, MA: Addison-Wesley, 2001.

[AusCERT 05]

AusCERT. *Australian Computer Crime and Security Survey*, 2005.

[Brezinski 02]

Brezinski, D. & Killalea, T. *Guidelines for Evidence Collection and Archiving* (RFC 3227), 2002.

[CAIF 05]

RUS-CERT. Common Announcement Interchange Format (CAIF), 2005.

[CERT 08]

CERT/CC. *CSIRT Development*, 2008.

[CSIRT 08]

CSIRT Development Team, CERT/CC. *Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)*, 2008.

[DoJ 08]

U. S. Department of Justice. "Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers," 2008.

[EISPP 03]

European Information Security Promotion Programme (EISPP), 2003.

[FIRST 08]

Forum of Incident Response and Security Teams, 2008.

[FISMA 02]

U.S. Congress. Federal Information Security Management Act of 2002, Title III of the E-Government Act of 2002 (H.R. 2458; P.L. 107-347). Available online through http://www.gpoaccess.gov/plaws/107publ.html.

[Fraser 97]

Fraser, B., ed. *Site Security Handbook* (RFC 2196), 1997.

[GAO 04]

Government Accountability Office. *Cybersecurity for Critical Infrastructure Protection* (GAO-04-321), 2004.

[GAO 05]

Government Accountability Office. *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities* (GAO-05-434), 2005.

[Honeynet 08]

The Honeynet Project, 2008.

[Howard 97]

Howard, John D. "An Analysis of Security Incidents on the Internet 1989–1995." PhD Thesis, Carnegie Mellon University, 1997.

[IDWG 05]

Intrusion Detection Working Group. Intrusion Detection Exchange Format, 2005.

[IETF 06]

Internet Engineering Task Force. *Extended Incident Handling (inch)*, 2006.

[ISC 05]

Internet Systems Consortium. *ISC Internet Domain Survey*. http://www.isc.org/index.pl?/ops/ds/ (2005).

[ISS 01]

Internet Security Systems. *Computer Security Incident Response Planning: Preparing for the Inevitable*, 2001.

[Killcrece 03a]

Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-001, ADA421684). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[Killcrece 03b]

Killcrece, G.; Kossakowski, K.; Ruefle, R.; & Zajicek, M. *State of the Practice of Computer Security Incident Response Teams* (CSIRTs) and references therein (CMU/SEI-2003-TR-001, ADA421664). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[Kruse 02]

Kruse, Warren G. II & Heiser, Jay G. *Computer Forensics: Incident Response Essentials*. Reading, MA: Addison-Wesley, 2002.

[Mandia 01]

Mandia, Kevin & Prosise, Chris. *Incident Response: Investigating Computer Crime*. Berkeley, CA: Osborne/McGraw-Hill, 2001.

[REF 08]

Resiliency Engineering Framework Team, SEM. *CERT Resiliency Engineering Framework Preview Version 0.95R*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[Ruefle 08]

Ruefle, Robin. Defining Computer Security Incident Response Teams (Revised 2008).

[SANS 03]

The SANS Institute. *Computer Security Incident Handling Step-by-Step*. The SANS Institute, October 2003. Information on how to acquire this guide is available at http://store.sans.org/.

[Schiffman 01]

Schiffman, Mike. *Hacker's Challenge: Test Your Incident Response Skills Using 20 Scenarios*. Berkeley, CA: Osborne/McGraw Hill, 2001.

[Schultz 90]

Schultz, E. Eugene, Jr.; Brown, David S.; & Longstaff, Thomas A. "Responding to Computer Security Incidents." Livermore, CA: Lawrence Livermore National Laboratory. ftp://ftp.cert.dfn.de/pub/docs/csir/ihg.txt.gz (1990).

[Schultz 02]

Schultz, Eugene & Shumway, Russell. *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*. Indianapolis, IN: New Riders Publishing, 2002.

[Shirey 00]

Shirey, R. *Internet Security Glossary* (Network Working Group FYI 36, RFC 2828), 2000.

[Sokol 00]

Sokol, Marc S. & Curry, David A. *Security Architecture and Incident Management for E-business*. Atlanta, GA: Internet Security Systems (whitepaper), 2000.

[TERENA 08]

TERENA Task Force. *TF-CSIRT - Collaboration of Security Incident Response Teams*, 2008.

[TI 08]

Trusted Introducer for CSIRTs in Europe, 2008.

[US-CERT 08]

United States Computer Emergency Readiness Team, 2008.

[van Wyk 01]

van Wyk, Kenneth R. & Forno, Richard. *Incident Response*. Sebastopol, CA: O'Reilly & Associates, Inc., 2001.

[West-Brown 03]

West-Brown ,Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001120