Incident Handling and Reporting

Paul Cichonski, NIST
Tom Millar, US-CERT

Presentation Overview

- Brief Recap of Existing Incident Handling Guidance
- How Existing Guidance is Changing
- Incident Handling Automation Initiatives

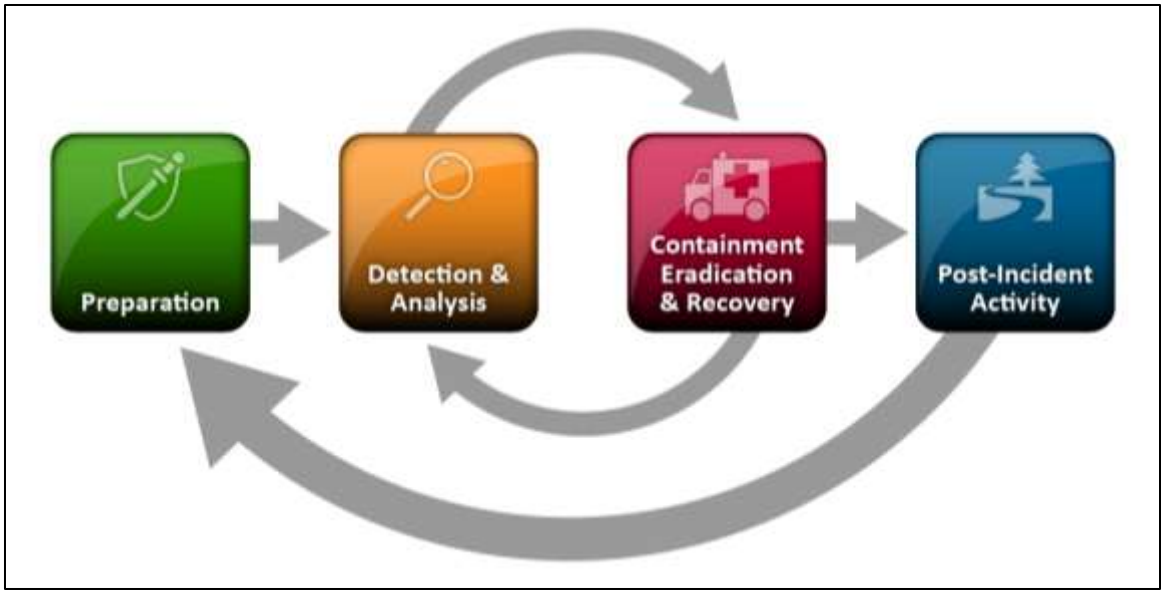
Recap: The Basics

- Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.
- Incident Handling: Mitigating incidents to minimize their business impact.

Recap: Examples of Incidents

- Many think of incidents as “hacking”
  - Attacker crashes a Web server
  - Attacker gets a system’s passwords
- Most incidents are not
  - Malware infects hundreds of computers and exfiltrates data to a command and control server.
  - User distributes pirated software through peer-to-peer file sharing
  - Employee sends a threat by e-mail

Recap: Incident Handling Lifecycle



- All phases are important to performing incident handling efficiently & effectively.
- Feedback loops between phases is essential.
- Originally defined in NIST SP 800-61.

Recap: Interaction with External Organizations

- A CSIRT may have to interact with external organizations for different reasons.
  - Coordinating on response of cross-cutting incident.
  - Communicating with media as to the extent of the incident.
- Organizations should develop policies and procedures detailing:
  - What organizations they will interact with.
  - Methods of interaction.

Updates to Incident Handling Guidance → NIST SP 800-61, rev.2

- Why are updates needed?
  - NIST SP 800-61, rev.1 released in March 2008 (over 4 years ago).
  - Current thinking on incident response has evolved.
- What is being updated?
  - New Incident Categories (now called Attack Vectors).
  - Multi-dimensional approach to prioritization.
  - Focus on Coordination and Info Sharing
  - Lifecycle staying the same.
- When will updates occur?
  - Public comment period on NIST SP 800-61, rev. 2 (Draft) ended in March 2012.
  - Final should be out by the end of July 2012.

Attack Vectors (1 of 2)

- **External/Removable Media:** An attack executed from removable media or a peripheral device—for example, malicious code spreading onto a system from an infected USB flash drive.
- **Attrition:** An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g., a DDoS intended to impair or deny access to a service or application; a brute force attack against an authentication mechanism, such as passwords, captchas, or digital signatures).
- **Web:** An attack executed from a website or web-based application—for example, a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware.
- **Email:** An attack executed via an email message or attachment—for example, exploit code disguised as an attached document or a link to a malicious website in the body of an email message.

Attack Vectors (2 of 2)

- **Impersonation:** An attack involving replacement of something benign with something malicious—for example, spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
- **Improper Usage:** Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories, for example; a user installs file sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
- **Loss or Theft of Equipment:** The loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token.
- **Other:** An attack that does not fit into any of the other categories.

Multi-Dimensional Incident Prioritization →Functional Impact

"Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems. Incident handlers should consider how the incident will impact the existing functionality of the affected systems. Incident handlers should consider not only the current functional impact of the incident, but also the likely future functional impact of the incident if it is not immediately contained."

- NIST SP 800-61, Revision 2 (Draft)

Functional Impact Categories

Category	Definition
None	No effect to the organization's ability to provide all services to all users
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
Medium	Organization has lost the ability to provide a critical service to a subset of system users
High	Organization is no longer able to provide some critical services to any users

Multi-Dimensional Incident Prioritization →Information Impact

"Incidents may affect the confidentiality, integrity, and availability of the organization's information. For example, a malicious agent may exfiltrate sensitive information. Incident handlers should consider how this information exfiltration will impact the organization's overall mission. An incident that results in the exfiltration of sensitive information may also affect other organizations if any of the data pertained to a partner organization."

- NIST SP 800-61, Revision 2 (Draft)

Information Impact Categories

Category	Definition
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
Integrity Loss	Sensitive or proprietary information was changed or deleted

Multi-Dimensional Incident Prioritization →Recoverability

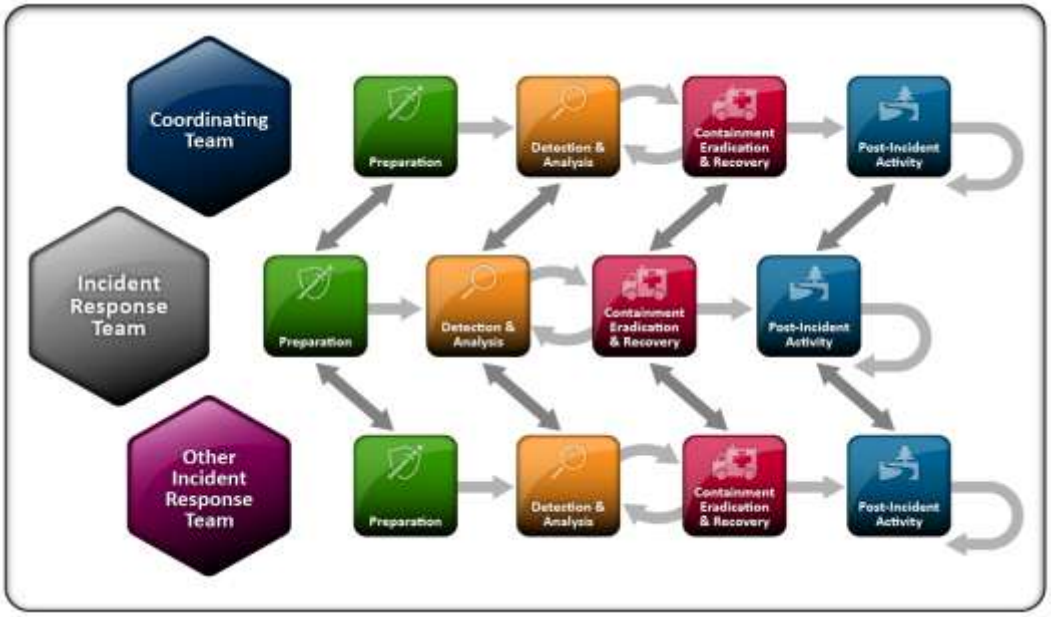
"The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident. In some instances it is not possible to recover from an incident (e.g., if the confidentiality of sensitive information has been compromised) and it would not make sense to spend limited resources on an elongated incident handling cycle, unless that effort was directed at ensuring that a similar incident did not occur in the future. In other cases, an incident may require far more resources to handle than what an organization has available. Incident handlers should consider the effort necessary to actually recover from an incident and carefully weigh that against the value the recovery effort will create and any requirements related to incident handling."

- NIST SP 800-61, Revision 2 (Draft)

Recoverability Effort Categories

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Cross-Organization Coordination and Information Sharing



- Coordination with partner organizations allows a CSIRT to increase knowledge of cross-cutting incidents.
- Effectively crowd-sourcing the incident handling process.

Incentives for Coordination and Information Sharing

- Process external indicator data to identify similar, internal incidents.
- Process external indicator data to gain better understanding of cross-cutting incidents.
- Share internal indicator data to receive advice on containment and remediation.
- Leverage information sharing pipelines to outsource complex malware analysis.

Coordination Relationships

Relationship	Definition
Team-to-team	• Exist whenever technical incident responders in different organizations collaborate with their peers. • The organizations participating in this type of relationship are usually peers and choose to share information, pool resources, and reuse knowledge to solve common problems
Team-to-coordinating team	• Exist between an organizational incident response team and a separate organization that acts as a central point for coordinated incident response and management such as US-CERT or an ISAC. • This type of relationship may include some degree of required reporting from the member organizations by the coordinating body, as well as the expectation that the coordinating team will disseminate timely and useful information to participating member organizations.
Coordinating team-to-coordinating team	• Exist between multiple coordinating teams such as US-CERT and the ISACs to share information relating to cross-cutting incidents which may affect multiple communities.

Information Sharing Automation

- Information Sharing processes can range from ad-hoc to semi-automated.
- Ad-hoc information sharing is normally conducted at the human-to-human level.
  - Individual incident handlers leverage contacts at partner organizations to collaborate on joint incidents.
  - Tools include: phone, email, jabber, etc.
- Automated information sharing is a formalization and machine-supplementation of ad-hoc relationships.

Types of Information to Share

- Technical Information → Indicators
  - Classification and impact information pertaining to known indicators.
  - Machine-readable data for searching for indicator on internal systems.
  - Normally sanitized data, shared between teams at all levels.
- Business Information → Impact
  - Functional, Information and Recoverability Impact
  - Informs receiving organization on scope and required resources for containment/recovery.
  - Normally only shared for reporting reasons between teams and coordinating teams.

Information Sharing Exemplars

- Anti-Phishing Working Group (APWG)
  - http://www.antiphishing.org/
- Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)
  - http://www.ren-isac.net/
  - http://code.google.com/p/collective-intelligence-framework/
- Others exist as well.

Sharing Agreements and Legal Considerations

- Before sharing information it is normally necessary to have a legal sharing agreement in place between the partner organizations.
- Organizations should check with their internal legal departments before sharing data.

Current US-CERT Reporting

Table J-1. US-CERT Incident Categories and Reporting Timeframes

Category	Name	Description	Reporting Timeframe
CAT 0	Exercise/Network Defense Testing	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not applicable; this category is for each agency's internal use during exercises.
CAT 1	*Unauthorized Access	A person gains logical or physical access without permission to a federal agency network, system, application, data, or other technical resource.	Within one (1) hour of discovery/detection.
CAT 2	*Denial of Service (DoS)	An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	*Malicious Code	A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection if widespread across agency.
CAT 4	*Inappropriate Usage	A person violates acceptable use of any network or computer use policies.	Weekly
CAT 5	Scans/Probes/ Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

Problems with Current Reporting

- 2006-era categories conflate *Effects* (root access, denial of service) with *Causes* (malware, inappropriate usage).
  - Cause = Method (or Attack Vector)
  - Effect = Impact
- Data about the *Cause* will drive technical response process and remediation.
- Data about the *Effect* will drive prioritization and resourcing.

Solution

- Separate *Cause* and *Effect* reporting streams.
  - *Cause* data can be captured using new NIST SP 800-61, rev.2 Attack Vectors.
  - *Effect* data can be captured using new NIST SP 800-61, rev.2 impact metrics.
- By separating cause from effect, and allowing for multiple dimensions of effect/impact, we can begin to develop better tailored data models for incidents.

More Specifically:

- Need to capture data pertaining to the following:
  - Cause →Attack Vector data
  - Effect →Functional Impact data
  - Effect →Information Impact data
  - Effect →Recoverability data

Attack Vectors

- External/Removable Media
- Attrition
- Web
- Email
- Impersonation
- Improper Usage
- Loss or Theft of Equipment
- Other

Functional Impact Types

- High = “Closed for Business”
- Medium = Restricted
- Low = Loss of efficiency
- None

Information Impact Types

- Privacy Breach = PII, PHI
- Proprietary Breach = Unclassified proprietary information/Intellectual Property
- Classified = S, TS, SCI
- Integrity Loss = Sensitive info was changed or deleted.
- None

Recoverability Effort Types

- Not Recoverable = Recovery not possible (e.g., sensitive data leaked and posted publically).
- Extended = Time to recover is unpredictable, outside resources needed.
- Supplemented = Time to recover is predictable with additional resources.
- Regular = Time to recover is predictable with existing resources.

Goals for revised reporting:

- Enable useful coordination earlier in the process.
- Rich, consistent data to support both tactical and strategic decisions.
- Clearer guidance for reporters to improve all-around communications: lowering the data entry workload while increasing quality and relevance.

What Managers should be doing

- Consider SP 800-61 rev.2 and this presentation as a draft of the new incident reporting guidance and plan accordingly with your SOC and CSIRT team leads.
- Let me know your recommendations on how we can successfully transform together.
- Proposed target for completing transition to revised reporting guidelines: FY14.

Community Information Sharing Efforts

- IETF Managed Incident Lightweight Exchange (MILE) Working Group
  - Focused on developing standards for enabling automated incident info sharing (e.g., IODEF, RID). More info here: http://tools.ietf.org/wg/mile/
- Incident Data Exchange Working Group (idxwg@nicwg.org)
  - incident handlers developing technical solutions for coordinated incident handling.
  - Contact Tom Millar to be added to the list.
- Joint Analysts' Collaborative Knowledge Exchange (JACKE)

Questions?

Paul Cichonski (NIST)

IT Specialist

paul.cichonski@nist.gov

(301) 975-5259

Tom Millar (US-CERT)

Chief of Communications

Thomas.Millar@us-cert.gov