The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-150**

Title: *Guide to Cyber Threat Information Sharing*

Publication Date: **October 2016**

- Final Publication: http://dx.doi.org/10.6028/NIST.SP.800-150 (which links to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf).
- Information on other NIST cybersecurity publications and programs can be found at: http://csrc.nist.gov/

The following information was posted with the attached DRAFT document:

Oct. 28, 2014

SP 800-150

DRAFT Guide to Cyber Threat Information Sharing

NIST announces the public comment release of Draft Special Publication (SP) 800-150, *Guide to Cyber Threat Information Sharing*. The purpose of this publication is to assist organizations in establishing, participating in, and maintaining information sharing relationships throughout the incident response life cycle. The publication explores the benefits and challenges of coordination and sharing, presents the strengths and weaknesses of various information sharing architectures, clarifies the importance of trust, and introduces specific data handling considerations. The goal of the publication is to provide guidance that improves the efficiency and effectiveness of defensive cyber operations and incident response activities, by introducing safe and effective information sharing practices, examining the value of standard data formats and transport protocols to foster greater interoperability, and providing guidance on the planning, implementation, and maintenance of information sharing programs.

Please send your comments to sp800-150comments <at> nist.gov by **November 28, 2014** using the following template

Guide to Cyber Threat Information Sharing (Draft)

Chris Johnson
Lee Badger
David Waltermire

C O M P U T E R   S E C U R I T Y

NIST

**National Institute of
Standards and Technology**
U.S. Department of Commerce

Guide to Cyber Threat Information Sharing (Draft)

Chris Johnson
Lee Badger
David Waltermire
Computer Security Division
Information Technology Laboratory

October 2014

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

Public comment period: *October 29, 2014* through *November 28, 2014*

122
123

Abstract

124
125 In today's active threat environment, incident detection and response is an ongoing challenge for many
126 organizations. This publication assists organizations in establishing computer security incident response
127 capabilities that leverage the collective knowledge, experience, and abilities of their partners by actively
128 sharing threat intelligence and ongoing coordination. This publication provides guidelines for coordinated
129 incident handling, including producing and consuming data, participating in information sharing
130 communities, and protecting incident-related data.

131 **Keywords**

132
133

135
136 **Acknowledgements**

137
138

140
141 **Trademark Information**

142
143

Table of Contents

List of Appendices

199
200

List of Figures

211
212

List of Tables

215

Executive Summary

As the magnitude and complexity of cyberspace increases, so too does the threat[1] landscape. Cyber attacks have increased in both frequency and sophistication resulting in significant challenges to organizations that must defend their infrastructure from attacks by capable adversaries. These adversaries range from individual attackers to well-resourced groups operating as part of a criminal enterprise or on behalf of a nation-state. These adversaries are persistent, motivated, and agile; and employ a variety of tactics, techniques, and procedures (TTPs) to compromise systems, disrupt services, commit financial fraud, expose sensitive information, and steal intellectual property. To enhance incident response actions and bolster cyber defenses, organizations must harness the collective wisdom of peer organizations through information sharing and coordinated incident response. This publication expands upon the guidance introduced in Section 4, Coordination and Information Sharing of NIST Special Publication (SP) 800-61, *Computer Security Incident Handling Guide* and explores information sharing, coordination, and collaboration as part of the incident response life cycle.

This publication assists organizations in establishing, participating in, and maintaining information sharing relationships throughout the incident response life cycle. The publication explores the benefits and challenges of coordination and sharing, presents the strengths and weaknesses of various information sharing architectures, clarifies the importance of trust, and introduces specific data handling considerations. The goal of the publication is to provide guidance that improves the efficiency and effectiveness of defensive cyber operations and incident response activities, by introducing safe and effective information sharing practices, examining the value of standard data formats and transport protocols to foster greater interoperability, and providing guidance on the planning, implementation, and maintenance of information sharing programs.

Implementing the following recommendations enables organizations to make more efficient and effective use of information sharing and collaboration capabilities throughout the incident response life cycle.

Organizations should perform an inventory that catalogues the information an organization currently possesses, the information that it is capable of producing, and document the circumstances under which this information may be shared.

By conducting an information inventory, an organization gains a better understanding of where its critical information resides, who owns it, how must it be protected, and when it can be shared. When deciding what incident-related information to share with other organizations, the following factors should be considered:

- Risk of disclosure

- Operational urgency and need for sharing

- Benefits gained by sharing

- Sensitivity of the information

---

[1] NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments* defines a *threat* as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service".

251   • Trustworthiness of the recipients

252   • Methods and ability to safeguard the information

Organizations should exchange threat intelligence, tools, and techniques with sharing partners.

254   Organizations should move from informal, ad hoc, reactive cybersecurity approaches where the
255   organization operates in isolation to formal, repeatable, adaptive, proactive, risk-informed practices where
256   the organization coordinates and collaborates with partners. The Cybersecurity Framework[2] describes an
257   approach that enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity
258   sophistication – to apply the principles and best practices of risk management to improving the security
259   and resilience their infrastructure. Through sharing, an organization benefits from the collective
260   resources, capabilities, and knowledge of its sharing peers. When sharing threat intelligence,
261   organizations have the opportunity to learn from each other; gain a more complete understanding of an
262   adversary's tactics, techniques, and procedures; craft effective strategies to protect systems; and take
263   action, either independently or collectively (i.e., as a sharing community) to address known threats.

Organizations should employ open, standard data formats and transport protocols to facilitate the efficient and effective exchange of information.

266   The use of standard data formats and protocols enables the automated exchange of information at
267   machine-speed and allows different types of information from diverse sources to be readily correlated and
268   analyzed. Standards can provide common identifiers that allow different organizations to unambiguously
269   identify concepts, artifacts, or objects of interest (e.g., vulnerabilities, malware); define a common
270   vocabulary to establish a shared understanding, or describe structures for encapsulating information for
271   exchange. The use of standard formats and protocols fosters interoperability and allows disparate
272   products, data repositories, and tools to rapidly exchange data and enables organizations to identify and
273   mitigate threats in cyber-relevant time[3]. Organizations should choose formats that are widely adopted,
274   readily extensible (i.e., new data elements or features can be incorporated with minimal engineering and
275   design effort), scalable, and secure. Standardized formats are often highly expressive and support a wide-
276   range of data elements; organizations should focus on using a manageable subset of data elements that
277   provide maximum interoperability and the greatest value.

Organizations should enhance their cybersecurity posture and maturity by augmenting local data collection, analysis, and management functions using information from external sources.

280   By enhancing its local data collection and analysis capabilities, an organization can gain a more complete
281   understanding of its systems and networks, and is able to make better use of the information that is
282   available from external sharing partners. Correlating this data with information received from external
283   sources and sensors can enhance data collected within an organization. Through the aggregation and
284   analysis of information from internal and external sources the organization can build richer context about
285   activities on its networks, identify campaigns, or better detect blended threats (i.e. threats that use
286   multiple methods of attack). This enrichment process allows ambiguous data to be transformed into
287   actionable information.

---

[2] See the *Framework for Improving Critical Infrastructure Cybersecurity* for additional information,
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[3] The term *cyber-relevant time* is a relative value that is based on the attack speed of the adversary. If an attack is unfolding then
the network defender must implement response actions at the same speed or faster. This concept is discussed in greater detail in
"Active Cyber Defense: A Vision for Real-Time Cyber Defense", MJ Herring, KD Willett, Journal of Information Warfare,
Volume 13, Issue 2, April 2014.

288 **Organizations should define an approach for adaptive cybersecurity that addresses the full cyber-**
289 **attack life cycle.**

290 Organizations should engage the adversary throughout the cyber attack life cycle and develop and deploy
291 defensive measures that detect, limit, or prevent reconnaissance, delivery of malicious payloads, and the
292 execution of exploits that allow an adversary to establish or maintain a persistent presence on an
293 organization's systems or networks. Organizations should acquire cyber threat intelligence from both
294 internal and external sources and use it to disrupt the adversary's cyber attack life cycle.

295 **Organizations should ensure that the resources required for ongoing participation in a sharing**
296 **community are available.**

297 Participation in an information sharing community may require an organization to commit personnel;
298 deliver training; and provide hardware, software, services and other infrastructure needed to support
299 ongoing data collection, storage, analysis, and dissemination. Organizations must have a sustainable
300 approach that provides the resources needed for ongoing participation to achieve sustained benefits from
301 information sharing activities.

302 **Organizations should protect sensitive information by maintaining an ongoing awareness of**
303 **information security, vulnerabilities, and threats.**

304 Organizations should implement the security controls necessary to protect its sensitive information,
305 enforce its information sharing rules, and ensure that information received from external sources is
306 protected in accordance with applicable data sharing agreements. Organizations should maintain an
307 ongoing awareness of information security, existing vulnerabilities, and threats in the operational
308 environment to support organizational risk management decisions.[4]

309 **Organizations should establish the foundational infrastructure necessary to maintain its**
310 **cybersecurity posture and clearly identify the roles and responsibilities for installing, operating,**
311 **and maintaining these capabilities.**

312 Organizations should have basic asset, vulnerability, and configuration management capabilities in place
313 to ensure that the organization can actively monitor and manage the hardware and software residing on its
314 networks and ensure that vulnerabilities are patched in a timely manner.

315

316

317

---

[4] NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* address the concept of information security risk management from the organization-level, mission/business process-level and the information system-level. NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* is intended to assist organizations in the development and implementation of an ISCM program.

1.   Introduction

Cyber attacks are increasing as evidenced by reports from governments describing the security breaches to their computer systems. Further evidence comes from major corporations that have reported similar successful incursions. In addition, it is likely that many intrusions are undetected, go unreported, or have never been made public. As a consequence, criminal groups cause substantial losses to individuals and businesses and adversaries acquire valuable intellectual property and government secrets. All of these actions have a negative effect on the economic well-being and national security of the United States.

Among the challenges business and governments face is the need for a high degree of interconnectivity. The issue is such interconnectivity can allow attacks to spread quickly. To defend against cyber attacks, it is important for a defender to have timely access to relevant, actionable threat intelligence and the ability to act on that intelligence. This threat intelligence includes indicators (i.e., an artifact or observable that suggests that an attack is imminent, that an attack is underway, or that a compromise may have already occurred); the TTPs of an adversary; and recommended actions to counter an attack. Attackers often use similar strategies, tools, and methods against multiple organizations; therefore, it is important for organizations to share information with their peers.

When an organization identifies and successfully responds to a cyber attack, it acquires information that can be used by other organizations that face the same or similar threats. When information is shared, threatened organizations have access to threat intelligence provided by peer organizations and are able to rapidly deploy effective countermeasures and detect intrusion attempts. As a result, the impact of a successful cyber attack can be reduced.

1.1   Authority

The National Institute of Standards and Technology (NIST) developed this document to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III: *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

1.2   Purpose and Scope

This publication provides guidance that is intended to help organizations share information related to computer security incidents, communicate and coordinate with external groups, and manage the impact of the incidents on their organizations as well as the wider community. This document explores information

359 sharing architectures, examines how the maturity of an organization's cybersecurity capabilities affects its
360 participation in a sharing community, and presents specific considerations for participation in an
361 information sharing community. The guidance in this publication applies primarily to organizations that
362 are familiar with the incident response life cycle presented in NIST SP 800-61, have some basic incident
363 response capabilities in place, and are interested in exchanging information with other organizations.

364 **1.3 Audience**

365 This document is for computer security incident response teams (CSIRTs), system and network
366 administrators, security staff, technical support staff, chief information security officers (CISOs), chief
367 information officers (CIOs), computer security program managers, and others who are responsible for
368 preparing for, or responding to, security incidents.

369 **1.4 Document Structure**

370 The remainder of this document is organized into the following sections and appendices:

371 • **Section 2** discusses the benefits of information sharing and incident coordination as well as the
372   challenges facing organizations as they implement these types of programs. In addition, this section
373   describes the fundamental concepts associated with incident coordination and information sharing
374   including: (i) the cyber attack life cycle; (ii) threat intelligence; (iii) information sharing
375   architectures; and (iv) formal and informal sharing communities.

376 • **Section 3** identifies the characteristics of organizations that have mature cybersecurity capabilities.
377   The maturity of the organizations shapes their ability to effectively participate in incident
378   coordination and threat sharing organizations. Individual organizations can perform a self-assessment,
379   identify gaps, and define a plan to improve their organization's cybersecurity capabilities.

380 • **Section 4** identifies the key activities involved in implementing an incident coordination and
381   information sharing capability. These activities are grouped by: (i) establishing sharing relationships;
382   (ii) participating in sharing relationships; and (iii) maintaining sharing relationships. The section also
383   provides guidance on how to protect shared information throughout the information life cycle.

384 • **Section 5** presents the general recommendations made in the publication.

385 • **Appendix A** contains computer security incident response scenarios that show how sharing threat
386   intelligence and coordinating a response to incidents increases the efficiency and effectiveness of the
387   organizations involved and enhances their network defense by leveraging the cyber experience and
388   capabilities of their partners.

389 • **Appendix B** contains an alphabetical list of terms and their associated definitions

390 • **Appendix C** provides an alphabetical list of acronyms used and their expansion

391 • **Appendix D** lists resources that may be helpful in establishing and maintaining an incident response
392   capability.

393 • **Appendix E** is the document change log.

394

2. Incident Coordination and Information Sharing Overview

In today's active threat environment, effective incident detection and response is an ongoing challenge for organizations. Information sharing and coordination provides a means of increasing the effectiveness of an organization's cybersecurity capabilities. Through collaborative incident response, organizations forge sharing partnerships that provide access to threat intelligence and tools that might otherwise be unavailable. Using these shared resources, organizations are able to enhance their network security posture by leveraging the knowledge, experience and capabilities of their partners. Allowing one organization's detection to become another's prevention is a powerful paradigm that can advance the overall security of organizations that actively share and coordinate. Threat information exchanged within communities organized around industry sector (or some other shared characteristic) can be particularly beneficial because the member organizations often face adversaries that use common TTPs that target the same types of systems and information.

Attacks may be part of coordinated campaigns targeting related industries or organizations by adversaries using sophisticated tools and techniques that are difficult for a single organization to detect or defend against. An organization whose threat horizon is limited to the activities that occur on their own systems and networks may be unaware of targeted attacks against their industry sector, technology stack, or the specific information that they possess. These attacks, when successful, are often quickly commoditized and directed against other organizations. An organization can gain greater awareness of the larger threat landscape by establishing the communication channels, data sharing agreements, and automation necessary to share information in advance of an incident. These preparations enable the organization to act decisively throughout the cyber attack life cycle.

Network defense is an intrinsically collaborative undertaking that is most effective when organizations coordinate and work together to face well-organized, capable adversaries. Coordination consists of multiple organizations communicating, cooperating, and exchanging information before, during, or after an incident in order to achieve common goals. Organizations can use shared information such as indicators, tactics, and tools to develop proactive defense strategies that focus on predicting an adversary's next move.

Organizations seeking to participate in sharing relationships need to be able to manage both the information they publish and the information they receive through all stages of the information life cycle. The life cycle of information, as described in OMB Circular No. A-130[5], consists of the following six phases:

- **Creation or Collection:** generating or acquiring information

- **Processing:** aggregating, transforming, correlating, and classifying information

- **Dissemination:** publishing and distributing information to authorized recipients

- **Use:** applying information to support organizational decision-making

- **Storage:** short and long-term retention of information in file systems, content management systems, databases, or other repositories

- **Disposition:** implementing and enforcing policies for the retention and disposal of information

---

[5] OMB Circular A-130, Transmittal Memorandum #4, *Management of Federal Information Resources*, http://www.whitehouse.gov/sites/default/files/omb/assets/omb/circulars/a130/a130trans4.pdf

433 The processes, guidelines, and agreements put in place for information sharing and coordination should
434 address each of the information life cycle phases. The life cycle is an ongoing process that directly
435 supports the generation, enrichment, maturation, and exchange of information between organizations.

436 **2.1   Benefits of Information Sharing and Coordination**

437 Incident response activities often include communication and interactions between a variety of
438 organizations. By working together, these organizations can build and sustain the trusted relationships
439 that are the foundation of secure and responsible information sharing and coordination. The benefits of
440 collaboration throughout the incident response lifecycle include:

441 • **Shared Situational Awareness.** Information sharing and coordination enables organizations to
442   leverage the collective knowledge, experiences, and analytic capabilities of their sharing partners,
443   thereby enhancing the defensive capabilities of both organizations. Each member of a cybersecurity
444   community of interest can profit from the knowledge and experience of other community members.
445   Even a single contribution—a new tool or a description of an intrusion artifact—can increase the
446   awareness and security of the entire community.

447 • **Enhanced Threat Understanding.** By developing and sharing threat intelligence, organizations gain
448   a more complete understanding of the threat environment and are able to tailor and deploy security
449   controls, countermeasures, detection methods, and corrective actions based on observed changes in
450   the threat environment.

451 • **Knowledge Maturation.** When raw intelligence in the form of seemingly unrelated observations is
452   shared and analyzed, it can be correlated with other data sets to build robust sets of indicators that are
453   associated with a specific incident or threat and impart valuable insights into the relationships that
454   exist between indicators.

455 • **Greater Defensive Agility.** As cybersecurity technologies advance, adversaries continually adapt
456   their TTPs to counter the protective and detective measures implemented by network defenders.
457   Organizations that possess the agility to rapidly detect and respond to changes in the adversary's
458   TTPs can shift from reactive to proactive cybersecurity strategies.

459 • **Improved Decision Making.** Organizations that are able to consume and act on shared information
460   are generally able to make decisions with greater speed and confidence. When adversaries are better
461   understood, it is sometimes possible to anticipate their actions and deploy defensive measures before
462   they act.

463 • **Efficient Handling of Information Requests.** Information sharing and coordination is an essential
464   activity when reporting or investigating cybersecurity incidents that are criminal in nature.
465   Organizations that have the processes, tools, and trained personnel in place to exchange information
466   are better prepared to handle such information requests that arise and understand ensure that the
467   computers and artifacts involved in the incident are treated as evidence and should be handled in a
468   manner that preserves the chain of custody.

469 • **Rapid Notifications.** In the event an incident results in the release of information about another party
470   (the victim), organizations are typically required to notify their affected customers or business
471   partners. Government agencies and some industry sectors are subject to regulations that levy specific
472   requirements for reporting of cybersecurity incidents. Organizations that understand their notification
473   requirements and have notification procedures, contact information, and communications channels in
474   place are able to rapidly disseminate breach notifications to affected customers or business partners.
475   Appropriate sharing capabilities may be used, at least in part, to support these requirements.

2.2 Challenges to Coordination and Sharing

While there are clear benefits to sharing information, there are also a number of challenges to effective sharing and collaboration that must be considered.

- **Legal and Organizational Restrictions.** An organization's executive and legal teams may restrict the types of information that the organization can share. Restrictions may include limits on the types of information and the level of technical detail provided. Such restrictions are appropriate when they address legitimate business, legal, or privacy concerns; but the imposition of unwarranted or arbitrary restrictions may diminish the quality and timeliness of shared information.

- **Risk of Disclosure.** Knowledge of an adversary's TTPs is advantageous to a network defender but sharing of this information may put the contributor at risk by exposing the protective or detective capabilities of the organization and result in threat shifting by the adversary[6]. Additionally, disclosure of sensitive information, such as Personally Identifiable Information (PII), intellectual property, trade secrets, or other proprietary information can result in financial loss, violation of NDA's or other sharing agreements, legal action, and loss of reputation. Organizations should manage these risks using an appropriate risk management strategy.

- **Preserving Privacy.** Organizations may openly participate in information sharing communities, but still require that their contributions remain anonymous. This lack of disclosure may limit the usefulness of information to others since they cannot query the source of the information or understand the information's original context and provenance.

- **Producing Information**. Organizations seeking to produce information must have the necessary infrastructure, tools, and training to do so. While basic incident data (e.g., indicators, vulnerabilities) is relatively easy to produce; information such as an adversary's motives and TTPs generally requires greater effort.

- **Consuming Information**. Organizations must also have the infrastructure needed to access external sources and incorporate the information provided it into local decision-making processes. Information received from external sources has value only to the extent that an organization is equipped to act on the information.

- **Interoperability**. Standardized data formats and transport protocols help facilitate the interoperability needed for the secure, automated exchange of incident data between organizations, repositories, and tools, but agreement on formats and protocols requires careful analysis of costs and benefits.

- **Classification of Information.** Information received from government sources may be marked as classified information, making it difficult for an organization to use. It is also expensive and time-consuming for organizations to request and maintain the clearances needed for ongoing access to

---

[6] According to NIST SP 800-30, *Guide for Conducting Risk Assessments*, threat shifting is the response of adversaries to perceived safeguards and/or countermeasures (i.e., security controls), in which adversaries change some characteristic of their intent/targeting in order to avoid and/or overcome those safeguards/countermeasures. Threat shifting can occur in one or more domains including: (i) the time domain (e.g., a delay in an attack or illegal entry to conduct additional surveillance); (ii) the target domain (e.g., selecting a different target that is not as well protected); (iii) the resource domain (e.g., adding resources to the attack in order to reduce uncertainty or overcome safeguards and/or countermeasures); or (iv) the attack planning/attack method domain (e.g., changing the attack weapon or attack path).

510 classified information sources. In addition, many organizations employ non-U.S. citizens who are not
511 eligible to hold security clearances and are not permitted access to classified information[7].

512 • **Establishing Trust.** Trust relationships form the basis for information sharing, but can be time
513 consuming to establish and maintain. Ongoing communication, through regular in-person meetings,
514 phone calls, or social media can help accelerate the process of building trust.

515 ## 2.3 Cyber Attack Life Cycle

516 The attacks perpetrated by adversaries are growing in scale, scope, complexity, and frequency. Reactive
517 defense strategies are not suitable for dealing with the advanced persistent threats that leverage
518 sophisticated tools, zero-day exploits, and advanced malware to compromise systems and networks.
519 While vulnerability and configuration management continue to be an important part of an organization's
520 defensive strategy, these practices cannot fully address the threat posed by persistent adversaries who use
521 advanced intrusion techniques. Although it is not feasible to fully predict adversary behavior, a cyber
522 attack life cycle model can provide a simple, but useful abstraction for analyzing potential threats. Each
523 phase in the cyber life cycle is an opportunity for a network defender to take action against an adversary.
524 By using a cyber attack life cycle, in concert with both internal and external threat intelligence, network
525 defenders can craft proactive incident response strategies that focus on disrupting the adversary earlier in
526 the life cycle (i.e., before an exploit has occurred).

527 A number of the cyber attack life cycles exist, including Lockheed Martin's "Cyber Kill Chain®"[8] (shown
528 in Figure 2-1) and the attack phase steps presented in NIST SP 800-115[9]. Figure 2.1 depicts 6 phases of a
529 cyber attack:

530 • **Phase 1—Reconnaissance:** Adversary identifies and selects a target(s).

531 • **Phase 2—Weaponize:** Adversary packages an exploit into a payload designed to execute on the
532 targeted computer/network.

533 • **Phase 3—Deliver:** Adversary delivers the payload to the target system(s).

534 • **Phase 4—Exploit:** Adversary code is executed on the target system(s).

535 • **Phase 5—Install:** Adversary installs remote access software that provides a persistent presence
536 within the targeted environment or system.

537 • **Phase 5—Command and Control:** Adversary employs remote access mechanisms to establish a
538 command and control channel with the compromised device.

539 • **Phase 6—Act on Objectives:** Adversary pursues intended objectives (e.g., data exfiltration, lateral
540 movement to other targets)

---

[7] Executive Order 12968, *Access to Classified Information*, http://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf
[8] "Cyber Kill Chain" is a registered trademark of Lockheed Martin.
[9] The attack phase steps presented in NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment: A Security Life Cycle Approach* are presented in the context of a penetration testing activity, but the activities described are similar to those that would be performed by an actual adversary. This publication is available at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
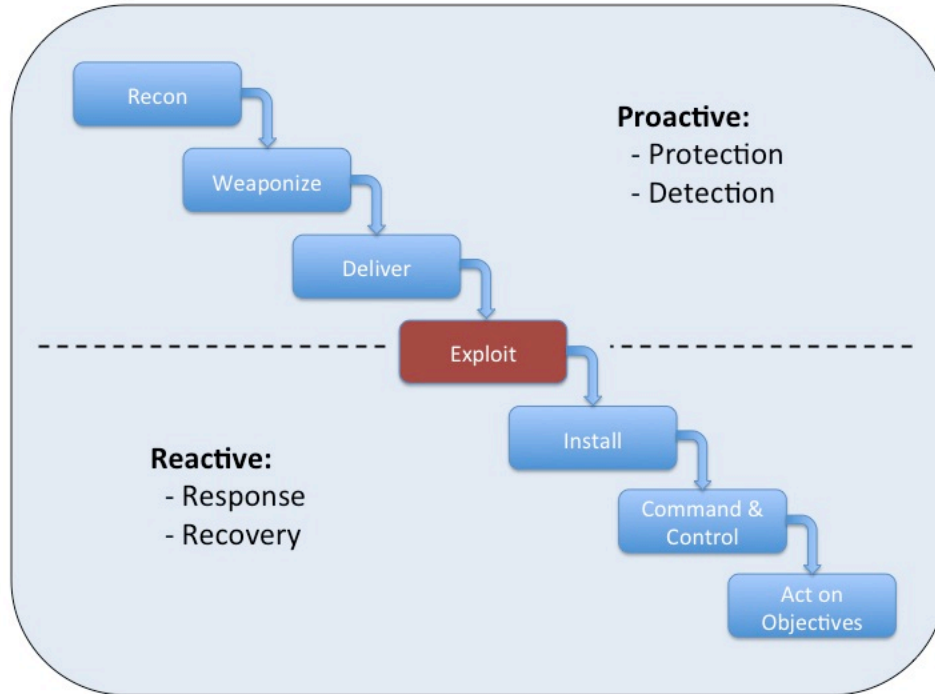
541
542   **Figure 2-1: Cyber Kill Chain[10]**

543   As depicted in Figure 2-1, proactive network defense (i.e., "above the line") consists of deploying
544   protective and detective measures that disrupt an adversary before an exploit has been successfully
545   executed. By recognizing and engaging the adversary during the reconnaissance, weaponization, and
546   delivery phases of the cyber attack life cycle, network defenders are able to deploy mitigations or take
547   some other course of action to ensure that mission-critical assets are protected prior to an adversary
548   successfully executing an exploit. Reactive network defense (i.e., "below the line") relies on the
549   organizations ability to detect the presence of an adversary on their networks and systems and craft an
550   effective response and recovery strategy. Regardless of where interdiction occurs within the kill chain, the
551   network defender must perform a retrospective analysis of the threat across the cyber attack life cycle to
552   ensure that the response was effective. This analysis should include identifying indicators, determining
553   where in the cyber attack life cycle these indicators were observed, and correlating these indicators with
554   other threat intelligence. By understanding how an adversary operates over the cyber attack life cycle a
555   network defender may be able to devise more effective defensive strategies. Examples of such defensive
556   strategies and techniques, and where they can be applied within the cyber kill chain are described below:

557   • Reconnaissance. Perform monitoring and analysis of NetFlow, darknet, and passive DNS data to
558   detect and investigate common network reconnaissance patterns such as port scans or probes. Employ
559   anti-reconnaissance measures such as redirecting an attacker to a network black hole or by blocking
560   specific IP addresses or domains.

561   • Weaponize. Develop, deploy, and refine high-fidelity signatures based on analysis of artifacts
562   observed in malware payloads. Signature-based detection methods are generally fragile; adversaries
563   can evade detection through minor modification to an exploit. By performing a more in-depth
564   analysis of captured malware artifacts, more accurate and lasting detection signatures can be created,

---

[10] *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*,
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

565 and additional techniques can be selected and used, to identify new malware and variants of existing
566 malware.

567 • Deliver. Understand the tools and techniques that an adversary uses to deliver malicious payloads and
568 develop and deploy detective and protective measures that disrupt the adversaries deliver channels.
569 These measures could be a technical (e.g., blacklisting of a site associated with a "watering hole"
570 attack) or procedural (e.g., just-in-time awareness training for emerging threats).

571 • Exploit. Counter zero-day attempts by deploying defenses that help prevent attackers from injecting
572 code into a running program, exploiting buffer overflow conditions, injecting operating system
573 commands, or using access control weaknesses to gain greater system access. Organizations can also
574 employ advanced threat modeling to characterize their attack surface and use fuzz testing to expose
575 vulnerabilities in likely attack vectors.

576 • Install. Expose and actively respond to recently-installed malware by employing host and network-
577 based intrusion detection signatures and tools such as file integrity checking, rootkit detection, and
578 configuration change monitoring.

579 • Command and Control. Establish baselines of normal network and device activity and configure
580 internal networks to detect anomalous inbound and outbound network traffic and changes in user and
581 device behaviors. Monitoring against a baseline provides a means of detecting beaconing (i.e.,
582 outbound traffic on regular intervals) that may be associated with interactions with a command and
583 control server.

584 • Act on Objectives. Deploy advanced data loss prevention solutions to detect abnormal data access,
585 evasion techniques, and data exfiltration attempts to prevent unauthorized transmission or copying of
586 sensitive data.

587 To mount an active defense, an organization should seek to understand an adversary's TTP within the
588 cyber attack life cycle and possess and make use of detailed threat intelligence that is relevant, timely, and
589 accurate. Information sharing among comparable organizations is an effective method for developing this
590 level of intelligence. By observing an adversary's targets, activities, and behaviors over an extended time
591 period a set of known TTPs can be developed for that adversary. Sharing this information with other
592 defenders may enable those defenders to acquire valuable insights into an adversary's strategies and
593 overall plans, thereby increasing the defender's ability to anticipate an intruder's behavior and develop a
594 more vibrant and effective defense.

595 **2.4   Threat Intelligence**

596 Threat intelligence is a vital part of network defense and incident response. Organizations gather
597 intelligence about the active threats to their environment and implement targeted defensive measures,
598 both tactical and strategic. Threat intelligence includes information about threats, TTPs, and devices that
599 adversaries employ; the systems and information that they target; and any other threat-related information
600 that provides greater situational awareness to the network defender and incident responder. Effective
601 threat intelligence exhibits the following characteristics:

602 • **Timely.** Intelligence should be rapidly delivered (i.e., ideally at wire speed), with minimal latency
603 and provide sufficient opportunity for the recipient to anticipate the threat and prepare a suitable
604 response. The timeliness of intelligence is context-dependent (i.e., cyber-relevant) and needs to take
605 into account the volatility of the threat, the speed of attack, and the capabilities and TTPs of the
606 adversary. Some decision cycles may require that tactical intelligence be delivered within seconds or

607　　　minutes to counter a fast-moving adversary, other threats may be more slow-moving and deliberate
608　　　and can be effectively addressed using intelligence that is hours, days, or even months old.

609　　• **Relevant.** Threat intelligence should have applicability within the recipient's operating environment,
610　　　address threats that the organization is likely to face, attacks they are likely to see, and describe
611　　　adversaries that the recipient is likely to encounter. Recipients of threat intelligence should perform a
612　　　risk analysis to determine the degree of risk associated with a particular threat.

613　　• **Accurate.** The threat intelligence should be correct, complete, and unambiguous. Inaccurate or
614　　　incomplete information may prevent critical action, incite unnecessary action, result in an
615　　　inappropriate response, or instill a false sense of security on the part of the recipient.

616　　• **Specific.** Threat intelligence should depict the incident or adversary at a level of detail that addresses
617　　　the salient facts about the threat, allows the recipient to understand how the threat may affect them,
618　　　and allows them to evaluate possible courses of action.

619　　• **Actionable.** Threat intelligence should ideally identify actions the recipient can take to counter the
620　　　threat or provide sufficient information and context to allow the recipient to develop a suitable
621　　　response to the threat.

622　Organizations should not only share information about successful intrusions, but also information about
623　intrusion attempts — regardless of whether the intrusion actually succeeded. Sources of information
624　include darknet servers (i.e., servers configured to capture traffic destined for unused address space or
625　unallocated IP addresses), firewall, and IDS/IPS logs. Reports of attempted intrusions are often deemed
626　less sensitive because sharing partners cannot readily draw conclusions about organization vulnerabilities
627　or security resources from the information provided. Since information about attempted intrusions
628　generally requires less sanitization and analysis, it can often be shared and acted on by the recipient more
629　quickly.
630
631　There are many sources for cyber threat intelligence; organizations can collect and develop intelligence
632　internally or acquire it externally through sharing communities, open sources, business partners; industry
633　sector peers, product vendors, commercial cyber threat intelligence services, customers, law enforcement
634　agencies, or other incident response teams.
635
636　Any insights regarding the motives and goals of the adversary are extremely valuable and should be
637　documented. Personal relationships with trusted individuals or organizations are excellent sources of
638　information, with the caveat that informal relationships may not be an enduring source of threat
639　intelligence because individuals may move to other organizations or take on a new role within their
640　current organization that no longer affords them access to the information that was previously shared.
641　Internal threat intelligence sources include intrusion detection or protection systems, security information
642　and event management products, antivirus software and file integrity checking software alerts; and
643　operating system, network, service, and application logs[11]. The internal threat intelligence and related
644　artifacts that are gathered should be retained and shared with partners as permitted by organizational
645　policy.

646　Threat intelligence can also be acquired through sharing communities organized around industry sectors
647　such as financial, electricity, or health. Organizations that operate within a specific sector should consider
648　joining an established sector sharing community or, if none exist, consider forming one with other sector

---

[11] See NIST SP 800-61, *Computer Security Incident Handling Guide*, Section 3.2.3, for additional information on common
sources of precursors and indicators.

649 peers. Organizations that operate in the same sector often have similar missions, operational
650 environments, and data and often face the same threats and adversaries. In addition to industry sector
651 groups, there are other communities that serve local, regional, and federal law enforcement; state and
652 local governments; emergency responders, and other affiliations (see Appendix D for information on
653 some incident response organizations).

654 There are many Internet-accessible open source threat intelligence outlets that publish indicators of
655 compromise, blacklists, malware and virus information, spammer lists, and other information regarding
656 emerging threats. Information originating from these sources may need to be manually collected and
657 analyzed; a process that is time-consuming, labor-intensive, and potentially error-prone. Organizations
658 that are unable or unwilling to take on such an effort may want to consider the use of a commercial cyber
659 threat service provider that offers similar threat intelligence and other value-added capabilities for a fee.

660 **2.5 Information Sharing Architectures**

661 Most sharing communities exchange information using some variant of the following basic information-
662 sharing architectures: (i) centralized; and (ii) peer-to-peer shown in Figure 2-2. The characteristic,
663 benefits and challenges of each of these approaches are further explored in Sections 2.5.1 and 2.5.2.
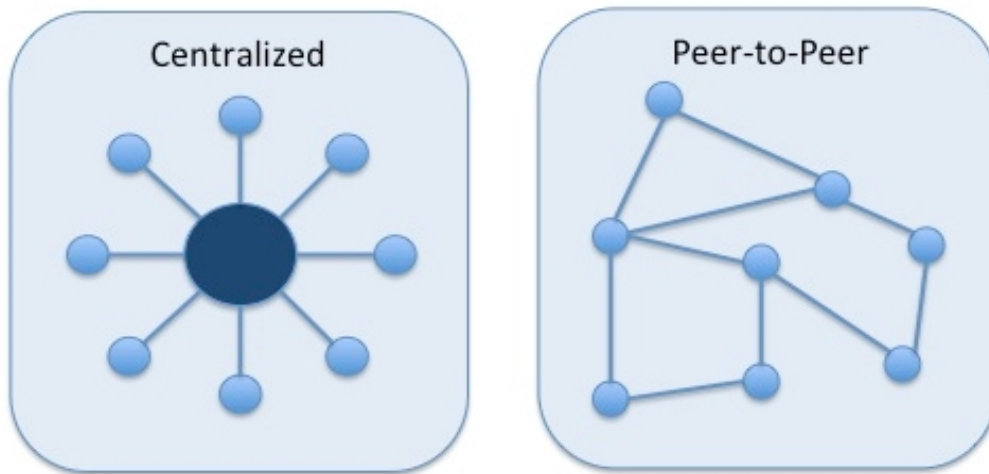
664

665 **Figure 2-2: Information Sharing Architectures**

666 The information sharing requirements for a community help determine the architecture that is most
667 suitable. Some communities may benefit from a centralized approach; others may choose to exchange
668 information directly among peers; still others may employ an approach that incorporates features and
669 characteristics of both. When selecting an architecture for a sharing community, the following key factors
670 should be considered:

671 • The characteristics, trustworthiness, capabilities, and composition of the participants

672 • The level of commitment of government, member organizations, and sponsors to support the
673 community

674 • The type and sensitivity of information that will be shared

675 • The required frequency, volume, and speed of information distribution

676
677 **2.5.1 Centralized Architecture**

678 The centralized architecture is commonly described as a "hub-and-spoke", where a central "hub" serves
679 as a repository or clearinghouse for information that it receives from the "spokes" (i.e., participating
680 members) or other sources. Information provided to the hub by participating members is either directly
681 forwarded to other community members (i.e., without any additional processing) or the hub may enhance
682 the information in some way and then distribute it to designated community members. The enhancements
683 performed by the hub may include aggregation and correlation of information from multiple sources,
684 sanitization, de-attribution, enrichment of information by providing additional context, or trending and
685 analysis that identifies common trends, threats, and malicious activity within the larger community.

686 Sharing communities based on this architecture usually establish formal data sharing agreements that
687 stipulate what information can be shared, who it can be shared with, whether attribution is allowed, and
688 the level of detail permitted. Information received by the central repository may be quite detailed,
689 voluminous, and contain data elements that would enable attribution. The repository's summarization,
690 sanitization and distribution processes should handle data in accordance with the data sharing agreements
691 and provide abstracted, unattributed summary information to the sharing community as required. Central
692 repositories that receive frequent, high volume submissions may choose to automate aspects of the
693 summarization and sanitization process.

694 The benefits conferred by a hub-and-spoke architecture are largely determined by the services performed
695 by the hub. The services provided by the central hub vary by community; some hubs may simply broker
696 the information exchange, others may perform additional processing to enrich the information. In a hub-
697 and-spoke community the central hub services can include consuming, aggregating, correlating,
698 analyzing, validating, sanitizing, distributing, and archiving information from a multitude of sources.

699 Hubs that use open, standard data formats and transport protocols alleviate the need for participants to
700 adopt multiple formats and protocols to exchange information with other community members.
701 Additionally, participants have fewer connections to manage – once a connection to the hub exists,
702 community members are connected to each other through the hub infrastructure.

703 The cost of the hub infrastructure is typically covered through membership or service fees paid by
704 community members. If these fees are too high, they may present a barrier to entry and preclude
705 organizations from participating in the community. A potential drawback to this architecture is that the
706 information exchange system is entirely dependent on the hub's infrastructure, making it vulnerable to
707 system failures, delays (e.g., due to network congestion, processing backlog, or other resource
708 contention), or compromise at the hub. Though the time sensitivity of information varies, when the hub is
709 not functioning or performance is degraded, all members of the sharing community are affected. A final
710 consideration is that the hub, as a repository of threat intelligence, becomes an attractive target for attack.

711 *Federal Government Response Teams*

712 The hierarchical hub-and-spoke architecture (i.e., where security incidents are reported to centralized
713 hierarchies within the government) is widely used within the Federal government. Figure 2-3 depicts a
714 notional hub-and-spoke reporting structure for incident response teams operating across the Federal
715 government and within specific departments and agencies. In this example, response teams participate as
716 both a hub (to subordinate organizations) and a spoke (to a parent organization), depending upon where
717 the team resides within the reporting hierarchy. In the Federal government, information flows from the
718 agencies to the United States Computer Emergency Readiness Team (US-CERT) and/or the Industrial
719 Control Systems Cyber Emergency Response Team (ICS-CERT). In the DOD, information flows from

720   the combatant commands, services, agencies, and field activities to United States Cyber Command
721   (USCYBERCOM). USCYBERCOM coordinates with the US-CERT and ICS-CERT on cybersecurity
722   incidents, intelligence, and reporting involving the DoD[12].
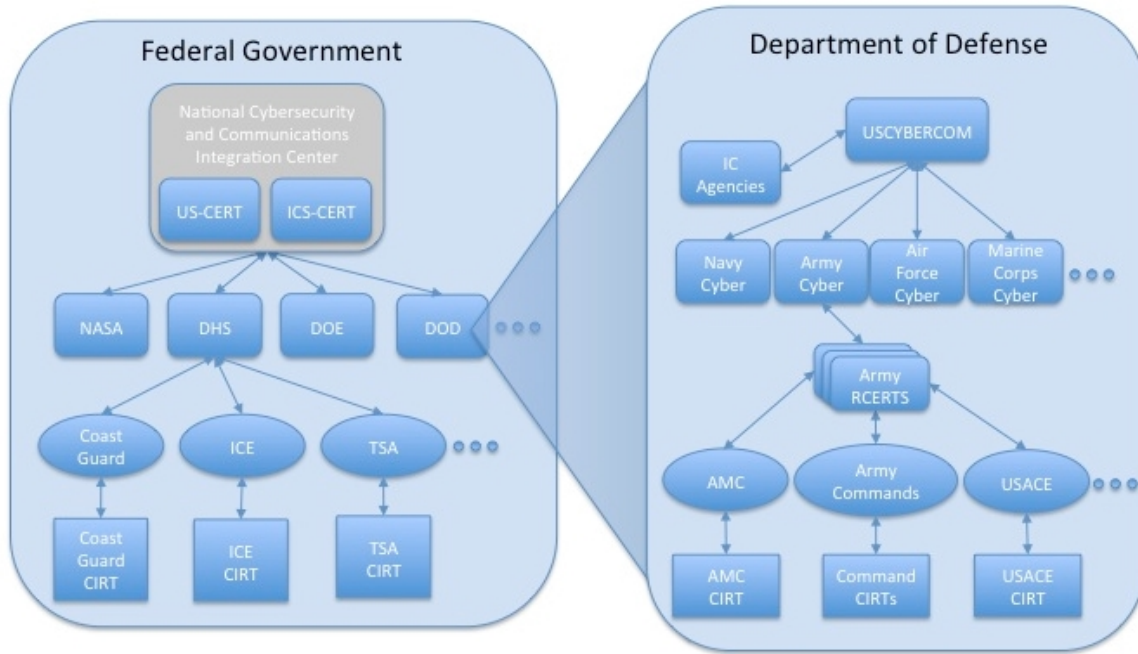
723
724
725   **Figure 2-3: Notional Federal Government Hub-and-Spoke Hierarchical Incident Reporting**

726   ***Information Sharing and Analysis Centers***

727   Another example of the hub-and-spoke model is the Information Sharing and Analysis Center (ISAC)
728   activities. Presidential Decision Directive-63 (PDD-63), published in 1998, describes ISACs as centers
729   for collecting, analyzing, sanitizing, and distributing information from the private sector to industry and
730   government. ISACs may also disseminate data from the government to the private sector. The private
731   sector participants determine the design and functions supported within the ISAC, with advice and
732   assistance from the Federal Government. Participation in an industry ISAC is voluntary. The National
733   Council of ISACs identifies 17 member ISACs[13].

---

[12] Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program, 10 July 2012
[13] http://www.isaccouncil.org/memberisacs.html
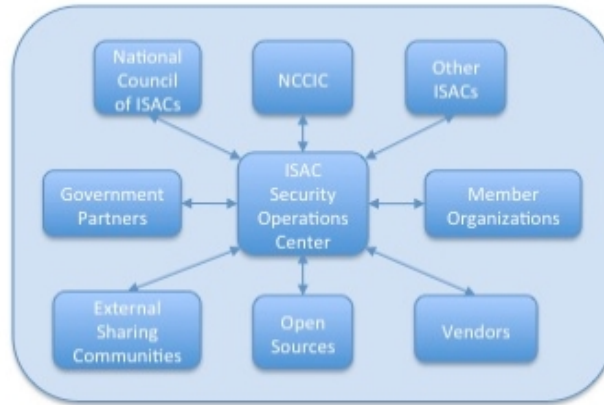
734

735   **Figure 2-4: Notional ISAC Hub-and-Spoke Incident Reporting Model**

736   In the notional ISAC model, illustrated in Figure 2-4, an ISAC Security Operations Center shares
737   incident, vulnerability and threat information with a variety of sources, including member organizations,
738   government partners, external sharing communities, vendors, and other ISACs. For example, a public or
739   private electrical utility company can join the Electrical Sector ISAC (ES-ISAC) and share information on
740   incidents and intelligence with that specific ISAC. The ES-ISAC would then share that information with
741   North American Electric Reliability Corporation (NERC), other ISACs, and the Federal government.

742   ### 2.5.2   Peer-to-Peer Architecture

743   Rather than routing data through a central hub, peer-to-peer participants share directly with each other.
744   Since no hub is present, each organization is responsible for consuming, aggregating, correlating,
745   analyzing, validating, sanitizing, protecting, and exchanging information with their peers. The
746   information that is exchanged between peers is limited to the data acquired, analyzed, and disseminated
747   by the participants. The dynamics of information exchange (e.g., security, speed, and frequency) will vary
748   according to the requirements and abilities of the communicating peers.

749   In a peer-to-peer relationship, trust is directly established with individual peers rather than brokered
750   through a central repository. Based on the level of trust established and the type of information being
751   exchanged, an organization may choose to share with a specific community member, a designated group
752   of recipients, or with all peers. Peer-to-peer trust is based on the belief that peers support a common
753   mission, respect the established sharing rules, and demonstrate a willingness participate in reciprocal
754   sharing.

755   The peer-to-peer architecture offers many benefits: (i) Peer-to-peer participants share directly with each
756   other (i.e., no intermediary such as the hub); this provides great agility and allows information to be
757   rapidly distributed as the receiver gets the information directly from the source. (ii) Peer-to-peer
758   architectures generally demonstrate greater resiliency since information is available through multiple
759   communication channels and there is no central hub that represents a potential single point of failure or
760   high-value target of attack.

761   The peer-to-peer architecture has some drawbacks including: (i) Peer-to-peer implementations that do not
762   employ standard methods of information exchange are difficult to scale since peers must support multiple
763   formats and protocols (ii) As the number of peer-to-peer sharing partners grows, the operating costs of
764   managing numerous connections, data (e.g., consuming, aggregating, correlating, analyzing, validating,
765   sanitizing, protecting, and exchanging), and trust relationships can grow exponentially.

766 Information exchanges between an organization and its Internet service provider (ISP), hosting provider,
767 business partner, industry sector peers, law enforcement agencies, and other incident response teams and
768 personnel often consist of peer-to-peer interactions. Such sharing, though not orchestrated through a
769 sharing community, is nonetheless an important component of an effective incident response capability.

770 ### 2.5.3 Hybrid Implementations

771 The two architectures previously described, are sometimes often in hybrid implementations that combine
772 characteristics of both hub-and-spoke and peer-to-peer. Both centralized and decentralized P2P
773 implementations exist. In a centralized peer-to-peer implementation, a central server(s) may be used for
774 resource discovery, to broker requests, or as a trusted 3rd party for authentication. In a purely
775 decentralized implementation, participants manage all aspects of their interactions with community peers.

776 An organization, for example, might exchange low-level intrusion indicators using a peer-to-peer
777 architecture but send high-level incident reports to a central hub. Another scenario involves sending the
778 same information directly to individual group members, as well as to the central hub. Such an approach
779 enables both an effective tactical response (i.e., rapid action on time-sensitive data through direct, joint
780 sharing) and makes use of the hub's ability to gather, combine, and analyze data received from multiple
781 members to craft longer term strategies and courses of action. While the use of a hybrid approach may be
782 advantageous in some cases, it can also increase costs and be more difficult to implement and operate.

783 ### 2.6 Formal vs. Informal Communities

784 Information sharing communities exhibit varying degrees of formality. Some of the characteristics of
785 formal and informal communities are presented below.

786 Informal sharing communities are generally self-organizing groups that operate through voluntary
787 cooperation. Membership is mutable (i.e., no formal fixed membership), sometimes anonymous, and the
788 members maintain full autonomy with minimal central coordination. These communities use informal
789 data sharing agreements (i.e., rules of conduct rather than legally binding instruments) that establish the
790 basic parameters for sharing information with the community.

791 Participants in an informal community publish information to a repository on a voluntary, ad hoc basis
792 and are responsible for ensuring that content submitted to the repository is suitable for sharing. The
793 repository operators maintain the repository but generally make no assertions regarding the quality and
794 accuracy of the data contained within the repository; trust in the information is based on the reputation of
795 the submitter. Organizations that wish to consume information subscribe to specific data sources hosted
796 by the repository (e.g., email, RSS feed).

797 Formal sharing communities are often organized around a common characteristic (e.g. industry sector)
798 and have official membership requirements that may define:

799 • Eligibility for institutions (e.g., specific industry sector)

800 • Eligibility for individuals (e.g., must have enterprise-wide security responsibilities)

801 • Nomination or sponsorship requirements (i.e., brokered trust)

802 • Probationary membership period

803 • Required organizational cybersecurity capabilities

804 Membership in such communities is generally fixed with minimal volatility in the membership rosters.
805 Information exchange within the community is governed through SLAs, NDAs, and other agreements.
806 Some communities collect an annual membership fee to cover the services and administrative costs of the
807 community. These fees vary by community and the fee structure is sometimes tiered, providing for
808 different levels of membership based on the organization type or size.

809 ## 2.7   Recommendations

810 The key recommendations presented in this section are summarized below:
811

812 • Leverage the knowledge, experience, and capabilities of sharing partners to exchange threat
813   intelligence, mitigation strategies, and tools, to enhance the cybersecurity posture of participating
814   organizations and reduce the overall cost of cyber attacks.

815 • Establish and maintain information sharing relationships to enhance the organization's situational
816   awareness and to foster a proactive approach to incident response.

817 • Use a cyber attack life cycle as a framework for observing and understanding an adversary's actions
818   and for defining an active defense strategy that makes effective use of information available through
819   both internal and external sources throughout the life cycle.

820 • Share information about intrusion attempts (regardless of whether the intrusion actually succeeded)
821   rather than information about a specific intrusion. Intrusion attempt information is less sensitive and
822   requires less sanitization and analysis; therefore it can be shared more quickly.

823 • Different sharing architectures exist for the sharing of information (e.g., centralized, peer-to-peer), as
824   a participant in an information sharing community, understand both the benefits and drawbacks of
825   these architectures.

826 • Seek out threat intelligence sources that provide information that is timely, relevant, accurate,
827   specific, and actionable.

828

3.   Understanding Current Cybersecurity Capabilities

Organizations should regularly assess the maturity of their cybersecurity capabilities and identify opportunities to enhance their overall security posture through information sharing and coordination. The purpose of this section is to describe the characteristics of a mature cybersecurity capability and a process by which an organization might become both a consumer and producer of actionable threat intelligence.

3.1   Characteristics of Mature Cybersecurity Capabilities

The maturity of an organization's cybersecurity practices is determined by its ability to establish and maintain an operational culture and the infrastructure necessary to actively manage cybersecurity risk. An organization must understand the cybersecurity threats to its systems, assets, data, and capabilities and prioritize its efforts, consistent with its risk management strategy and business needs. An organization should develop and implement protective measures that mitigate the impact of a potential cybersecurity incident, deploy capabilities that enable the timely detection and response to cybersecurity incidents, and be able to rapidly restore capabilities or services that were impaired due to a cybersecurity incident.

An organization should move from informal, ad hoc, reactive cybersecurity approaches where the organization operates in isolation to formal, repeatable, adaptive, proactive, risk-informed practices where the organization coordinates and collaborates with partners; such an approach is described in the Cybersecurity Framework.[14] The Cybersecurity Framework describes a process by which an organization can efficiently manage cybersecurity risk by selecting security controls that are consistent with the organization's risk management processes, legal/regulatory requirements, business/mission objectives, and organizational constraints. Security operations personnel should use information that originates from both internal and external sources to develop and deploy effective protective measures, detect network reconnaissance and attacks, identify threats, vulnerabilities, and indicators of compromise; and respond and recover from cyber attacks. Organizations that have high-performing security personnel in place are better poised to leverage sharing and coordination opportunities.

By participating in information sharing relationships an organization has access to a more extensive collection of cyber threat intelligence that can be used to help bolster its defenses. However, an organization that participates in sharing relationships does not thereby reduce or alleviate the need to deploy its own cybersecurity capabilities; it must still develop the local expertise and infrastructure to produce internal threat intelligence and to act on the information that it receives from external sources. Sharing and coordination is effective only if the recipient can act the information being shared; information is actionable when an organization possesses the core capabilities through which shared information can influence its detection, analysis, response, and recovery efforts. For example, shared threat intelligence that contains data elements, such as the IP addresses of a known or suspected adversary, is helpful only if the organization is monitoring IP addresses, has the ability to apply this information to a sensor device, and can identify what end points in the computer network were impacted. In another example, an organization may receive threat intelligence reporting that a compromise can be detected by observing the presence of a specific system artifact or a configuration setting holding a certain value. If the organization has no means of monitoring system artifacts or configuration settings, the shared information has no immediate value to the organization. Without core cybersecurity capabilities in

---

[14] The Cybersecurity Framework Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit these characteristics (e.g., risk and threat aware, repeatable, and adaptive). See the *Framework for Improving Critical Infrastructure Cybersecurity* for additional information, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

868 place, sharing and coordination provides minimal benefit to an organization, since the information
869 received is not actionable.

3.2   Consumer, Producer, and Capability Evolution

871 Often, entrants to a sharing community are primarily consumers of threat intelligence rather than
872 producers of information. Sharing communities benefit from the dynamic and symmetric exchange of
873 information, so an organization should seek to evolve from being a consumer only to become both a
874 consumer and producer of threat intelligence. By producing threat intelligence, an organization gains
875 greater expertise, helps other organizations more effectively respond to threats in their environment, and
876 fosters trust with other community members.
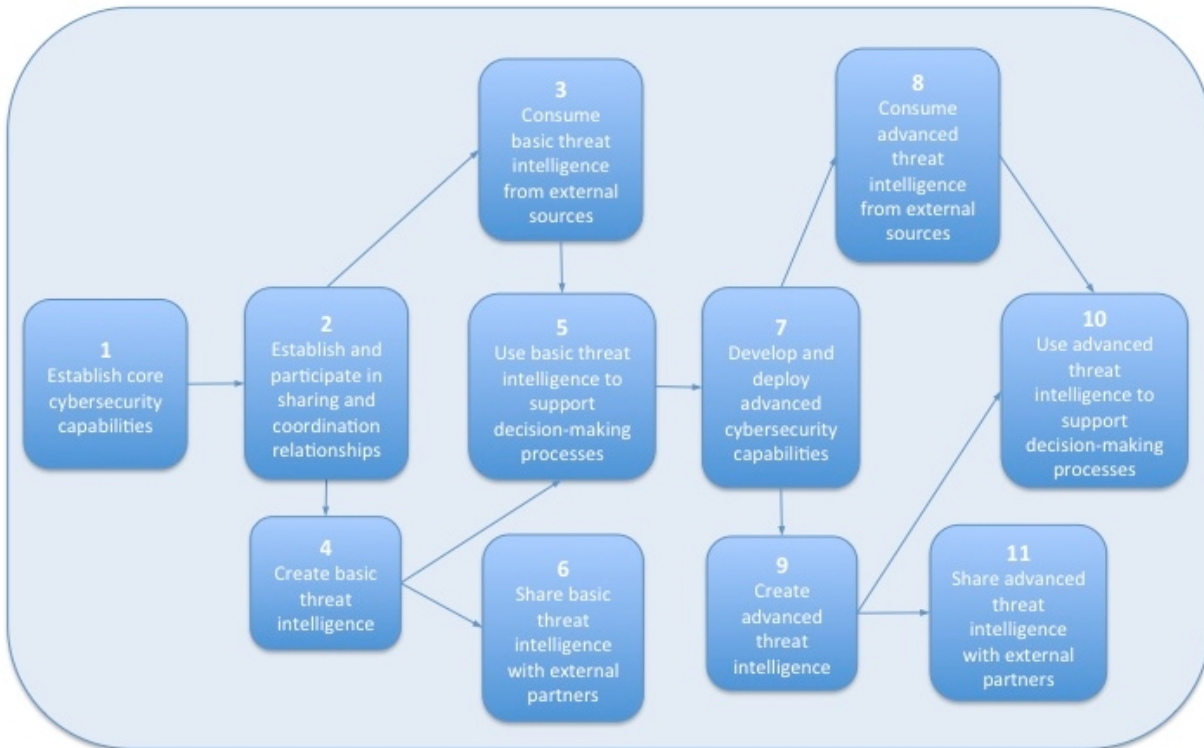
877

878   **Figure 3-1: Notional Information Sharing Process**

879 Figure 3-1 illustrates a process by which an organization can progress from an organization that initially
880 possesses a set of core cybersecurity capabilities to become a more mature organization that consumes,
881 creates, and shares cyber threat intelligence. The steps in this progression are described below:

882 1. **Establish core cybersecurity capabilities[15].** An organization should deploy the infrastructure and
883   processes necessary to support the core cybersecurity capabilities required to participate in
884   information sharing and collaboration activities. These core capabilities include a monitoring
885   infrastructure that is capable of supporting basic event and incident detection, analysis, and response

---

[15] The Computer Security Division's (CSD) Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.

886 efforts. Examples are implementing boundary network monitoring capabilities such as an intrusion
887 detection system (IDS) or a network-based antivirus (AV) appliance using vendor-provided
888 signatures, and monitoring and responding to the alerts issued by these devices.

889 2. **Establish and participate in sharing and coordination relationships.** An organization should
890 identify external sources of information that could be used to augment existing internal threat
891 intelligence and enter into information sharing and coordination relationships. Section 4 of this
892 document describes the process for establishing, participating, and maintaining information sharing
893 relationships.

894 3. **Consume basic threat intelligence from external sources.** An organization should establish the
895 infrastructure, processes, and training necessary to consume basic threat intelligence (e.g., simple
896 indicators such as IP addresses, domains) from its sharing partners. External threat intelligence
897 sources could include commercial, sector-based, or open source vulnerability, threat, and signature
898 feeds.

899 4. **Create basic threat intelligence.** An organization should establish the infrastructure, processes, and
900 training necessary to produce basic threat intelligence and disseminate it, as appropriate, to sharing
901 partners.

902 5. **Use basic threat intelligence to support decision-making processes.** An organization should
903 integrate the threat intelligence received from both internal and external sources into its current
904 incident response processes and capabilities. For example, an organization might deploy enhanced
905 IDS signatures, expand monitoring and assessment activities, or block IP addresses/ports based on the
906 threat intelligence it possesses. The organization should use the threat intelligence to help prioritize
907 response operations, enhance detection capabilities, and to develop and deploy effective courses of
908 action.

909 6. **Share basic threat intelligence with external partners.** An organization should establish the
910 infrastructure, processes, and training necessary to disseminate basic threat intelligence, as
911 appropriate, to sharing partners.

912 7. **Develop and deploy advanced cybersecurity capabilities.** In some cases, external sources will
913 possess threat intelligence that an organization has no means of consuming or acting on because of
914 lack of infrastructure or expertise. In such cases, the threat intelligence is available only after the
915 organization has expanded the scope of monitoring (e.g., monitor new sources or additional data
916 elements or more frequently), performed skills development, or deployed more capable security tools.
917 For example, the organization's host-based monitoring product may not be configured to (or able to)
918 examine specific system artifacts and settings of interest. In addition, as an organization begins to
919 engage more fully with its community peers, relationships grow and trust can be established which
920 can help foster technical exchanges. Examples of advanced capabilities are establishing a forensics
921 team that performs detailed network and computer forensics and malware analysis; deploying
922 defensive capabilities such as honeypots, honeynets, and detonation chambers; or implementing
923 advanced analytics and visualization functions that help expose an adversary's TTPs.

924 8. **Consume advanced threat intelligence from external sources.** An organization should establish the
925 infrastructure, processes, and training necessary to consume advanced threat intelligence (e.g., TTPs,
926 NetFlows) from its sharing partners.

927 9. **Create advanced threat intelligence.** An organization should establish the infrastructure, processes,
928 and training necessary to produce advanced threat intelligence (e.g., TTPs, malware artifacts). As an
929 organization develops new threat intelligence sources and new analysis techniques, they gain the

930   expertise needed to create and publish advanced threat intelligence and the ability to perform a more
931   detailed and sophisticated analysis of incident data.

932   10. **Use advanced threat intelligence to support decision-making processes.** An organization should
933   integrate the advanced threat intelligence received from both internal and external sources into its
934   current incident response processes and capabilities. The use of advanced threat intelligence may
935   allow the network defender to engage the adversary earlier in the attack life cycle and to deploy
936   countermeasures or corrective actions that disrupt, delay, or prevent the adversary from achieving
937   their goals.

938   11. **Share advanced threat intelligence with external partners.** Organizations that produce advanced
939   threat intelligence possess information that may benefit others and should share it with others when
940   possible. By acting as both a producer and publisher of information the organization is able to
941   contribute new or enriched threat intelligence to the community.

942   3.3   Managed Security Services Providers Considerations

943 An organization's cybersecurity capabilities (core or advanced) may, in some cases, be implemented and
944 maintained by a Managed Security Service Provider (MSSP). An organization may use a MSSP to
945 provide capabilities that cannot be practically or cost-effectively developed in-house. MSSPs offer a
946 variety of cybersecurity services and expertise that can be used to augment and enhance an organization's
947 security capabilities.

948 There are many approaches to using MSSPs, and the degree to which an organization depends on an
949 MSSP for their information sharing and incident coordination varies. Some organizations may choose to
950 outsource all cybersecurity operations, while others only specific components or capabilities. Small to
951 medium sized organizations may use an MSSP or a turnkey solution when the personnel and skills
952 necessary to perform a task are not readily available within the organization, or in cases where the desired
953 services can be provided by a MSSP at a lesser cost. When selecting a MSSP, the following factors
954 should be considered:

955 •   The MSSP should be engaged with information sharing communities and have ready access to
956   actionable threat intelligence.

957 •   The MSSP service level agreement (SLA) should clearly describe the responsibilities of the parties
958   entering into the agreement and establish a dynamic, adaptive cybersecurity strategy that utilizes
959   information received from both internal and external sources.

960 •   An organization that relies on an MSSP to provide some portion of its cybersecurity operations needs
961   to integrate the MSSP-provided capabilities with the organization's internal cybersecurity capabilities
962   and support the exchange of threat intelligence between the organization and the MSSP.

963   3.4   Capabilities Self-Assessment

964 When considering incident coordination and sharing opportunities, an organization should determine if
965 they have the capabilities necessary to effectively engage in these communities. The maturity of an
966 organization's cybersecurity capabilities can be evaluated through an informal self-assessment. The self-
967 assessment helps an organization better understand the maturity of its cybersecurity capabilities, which in
968 turn helps determines its readiness to coordinate and share with external partners. For the purposes of the
969 self-assessment process, maturity is defined at three levels: (i) underlying foundations and infrastructure;
970 (ii) core cybersecurity capabilities; and (iii) advanced cybersecurity capabilities.

3.4.1 Underlying Foundation and Infrastructure Capabilities

Participation in an information sharing and incident coordination may require changes to an organization's policies and procedures, technology deployments, and personnel training. An organization must establish the groundwork and infrastructure necessary to maintain its cybersecurity posture and clearly identify the roles and responsibilities for installing, operating, and maintaining these capabilities. The underlying foundation and infrastructure, at a minimum, includes:

- **Organizational Structure for Incident Coordination.** An organization should have policies in place that: (i) define the management structures, roles, responsibilities, and authorities conferred to incident response team personnel; (ii) describe handoff and escalation procedures between team members and teams; (iii) identify the primary and backup communication mechanisms that allow incident response personnel to effectively coordinate with both internal and external stakeholders.

- **Asset, Vulnerability and Configuration Management.** An organization should have rudimentary asset, vulnerability, and configuration management capabilities in place to ensure that the organization can actively monitor and manage the hardware and software residing on its networks and ensure that vulnerabilities are patched in a timely manner.

- **Log and Alert Collection.** An infrastructure that supports the enterprise-wide collection of relevant log data and alerts generated by security products. The collection capability should provide wide coverage of the enterprise's computer network infrastructure; allow new log data sources to be incorporated with minimal effort; and allow the security analyst to change the type of data collected, the frequency of collection, or to discontinue the collection of certain data elements altogether.

- **Log and Alert Search and Retrieval**. Organizations should consider the use of a security information and event management solution that aggregates, analyzes, and correlates log and alert data and provides situational awareness for incident response personnel and network defenders and allows them to search and retrieve log and alert data and use the data to detect malicious activity, protect systems and data, and support incident response and recovery efforts.

- **Response Tools.** An organization should have the infrastructure and tools necessary to effectively contain, eradicate, and recover from a cyber incident. This includes tools and infrastructure for containment (e.g., sandbox network), digital system forensics, malware removal, and current system backups to support recovery efforts.

3.4.2 Core Cybersecurity Capabilities

Organizations that have the foundational infrastructure in place should monitor their infrastructure and establish a baseline for normal user, system, and network activities. By establishing a baseline, sensors can be configured to raise alerts when observed behaviors and activities significantly depart from the established baseline or exceed established thresholds for reporting.

Core cybersecurity capabilities include the ability to:

- **Deploy, configure, monitor, and update sensors.** An organization should have host-based sensors capable of collecting information regarding the status of processes, ports, files, services, hardware, software, and configuration settings on endpoint systems, and should have network-based sensors capable of active/passive monitoring of network activities to provide enhanced situational awareness. Operations personnel should review and respond to the alerts generated by these sensors and update the signature files and configuration of these devices to address false positives/negatives and to address emerging threats.

1013 • **Manage log data.** An organization should generate, collect, aggregate, and manage relevant log,
1014   alert, and event information from across the enterprise. An organization may use a dedicated logging
1015   server, log management software, or a Security Information and Event Management product to allow
1016   the efficient collection, aggregation, analysis, and storage of log data.

1017 • **Document, prioritize, and manage incidents**. An organization should have incident response
1018   procedures in place that document the incident handling process. These procedures should cover all
1019   phases of the incident response life cycle.

1020 • **Perform basic network traffic forensics.** An organization should possess the tools (e.g., sniffer), log
1021   data and expertise necessary to correlate and analyze network events; identify common adversary
1022   techniques such as port scanning, probing, and IP address spoofing; and should possess a basic
1023   understanding of how adversaries use specific ports, protocols, and services to stage attacks.

1024 • **Coordinate with system/information owners.** An organization should have processes and
1025   communication mechanisms in place that allow incident response personnel to effectively
1026   communicate with the owners of systems and information during an active incident. The owners may
1027   need to be consulted when response decisions may cause a service disruption or have some other
1028   operational impact.

3.4.3 Advanced Cybersecurity Capabilities

1030 The distinctions between basic and advanced defensive capabilities are primarily based on the depth of
1031 analysis being performed and the role that information sharing and incident coordination plays in
1032 cybersecurity activities. Organizations practicing advanced cybersecurity capabilities are distinguished by
1033 their ability to:

1034 • **Conduct "deep dive" digital forensics analysis of a compromise**. Advanced digital forensics
1035   includes the use of a full suite of tools, tactics, and procedures including:

1036   − Analysis of non-volatile data such as computer media, hard drives, USB sticks, and DVDs/CDs.

1037   − Analysis of volatile data including random access memory (RAM), running processes, open
1038   ports, open files, and network connections.

1039   − Export, analysis, and identification of malware and associated artifacts

1040   − Advanced packet capture analysis and network activity reconstruction

1041   − Dissecting network traffic and identify and export items of interest including command and
1042   control traffic and malware

1043   − Engaging in network traffic flow analysis (e.g. NetFlow)

1044 • **Actively collect, produce, use, and share threat intelligence**. An organization should be actively
1045   engaged in the sharing of threat intelligence by:

1046   − Participating in coordination and sharing groups and forums

1047   − Acquiring and using threat and vulnerability information from external sources

1048   − Active coordination among computer network defenders, analysts, and operators

1049   − Using threat intelligence to drive sensor configuration and signature generation

1050   − Facilitating the production and sharing of threat intelligence within the organization and with
1051   external partners

- **Develop threat intelligence that reveals an adversary's TTPs, behaviors, and motives.** An advanced organization may seek to expose an adversary's TTPs through:

  - Malware capture, inspection, sanitization, and analysis

  - The use of a detonation chamber to explode files of interest (e.g., PDF, Word documents) for the purposes of malware and exploit detection, generally in temporary virtual environments

  - The deployment and monitoring of honeynets and honeypots

- **Use knowledge management practices to enrich data, mature knowledge, and inform cybersecurity decision-making.** An organization should develop and effectively use actionable information by:

  - Constantly refreshing and adapting defensive capabilities based on emerging threat intelligence

  - Using the knowledge of an adversary's TTPs to impede their progress, contain them, or prevent them from achieving their objectives

  - Using threat intelligence to inform the configuration of sensors, analysis platforms, and defensive measures

3.4.4 Information Sharing Capabilities

To consume and publish threat intelligence, an organization must demonstrate the ability to:

- **Coordinate the exchange of threat intelligence.** An organization should have the communication channels and business procedures in place that allow them to facilitate the exchange of information with both internal and external stakeholders.

- **Appropriately handle sensitive or classified information.** An organization should have the infrastructure and access control policies in place to preserve privacy and to ensure that sensitive information is afforded the required degree of protection.

- **Normalize or transform information**. An organization should have the ability to perform the data transformations necessary to make use of data received from external sources. These transformations may include, time synchronization, filtering, or rendering the information in alternate forms or formats.

- **Ingest information from external threat intelligence sources.** An organization should have the infrastructure and processes in place to ingest, store, and analyze the threat intelligence that it receives. Insufficient network, input/output, or processing capacity may result in information loss, data quality issues, and delays.

- **Produce and publish threat intelligence.** An organization should have the infrastructure and processes in place to produce and publish actionable threat intelligence.

- **Acquire actionable threat intelligence.** An organization must be able to acquire and use the threat intelligence from internal and external sources to:

  - Inform the development of signatures for intrusion sensors
  - Identify new artifacts and search terms during forensic analysis
  - Drive the configuration of honeypots and honeynets
  - Shape the tuning strategy for sensors and other monitoring instrumentation

1091
3.5   Recommendations

1093   The key recommendations presented in this section are summarized below:
1094

1095   • An organization should have, or develop, the underlying foundation and infrastructure in place to
1096   support information sharing and coordination activities

1097   • An organization should seek out external information sources and enter into various information
1098   sharing and coordination relationships as their cybersecurity capabilities mature.

1099   • An organization should consume information from external sources and apply the information to
1100   enhance their existing internal incident response capabilities

1101   • An organization should expand their internal data collection, perform more sophisticated analysis,
1102   and begin to develop and publish their own indicators

1103   • An organization may consider the use of an MSSP or outsourcing arrangement when the personnel
1104   and expertise necessary to perform a task are not readily available within the organization, or in cases
1105   where developing or maintaining a specific security capability in-house is not financial feasible

1106   • An organization should perform routine self-assessments to identify opportunities for improved
1107   cybersecurity practices and more effective information sharing

1108

1109

4. Establishing, Maintaining, and Using Information Sharing Relationships

As defined in NIST SP 800-61, incident handling is structured as a four-phase life cycle: i) preparation; ii) detection and analysis; iii) containment, eradication, and recovery; and iv) post-incident activity, illustrated in Figure 4-1. Information sharing and coordination may occur in any or all of these phases. This section describes how an organization can establish, participate in, and maintain incident coordination and information sharing relationships throughout the incident response life cycle.
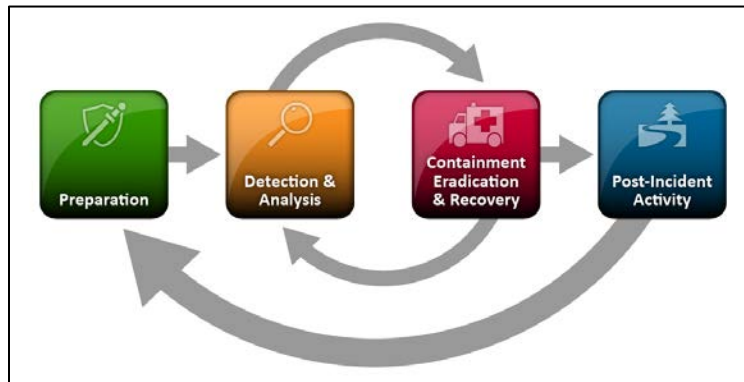
Figure 4-1: Incident Response Life Cycle

4.1 Establishing Sharing Relationships

When launching an information-sharing program, the following planning and preparation activities are necessary to help ensure the success of the initiative:

- Defining the goals, objectives, and scope of information sharing

- Conducting an information inventory

- Establishing information sharing rules

- Joining a sharing community

- Supporting an information sharing capability

These preparatory information-sharing activities are explored in greater detail in the following sub-sections.

4.1.1 Defining the Goals, Objectives, and Scope of Information Sharing

The first step in establishing an information sharing relationship is to set forth basic goals and objectives that describe what the organization hopes to accomplish. This need not be an onerous process; it is simply a matter of stating the desired outcomes of information sharing. In framing the information sharing initiative, the organization should also establish the general scope of the effort by identifying the resources (e.g., information, services, capabilities) that the organization could share, the resources that the

1135 organization needs, the general conditions under which sharing is permitted, and potential sharing
1136 partners.

1137 When establishing the initial parameters for information sharing, it is important to obtain approval from
1138 the management and legal teams (i.e., those with the authority to enter into commitments) and the support
1139 of key organizational stakeholders (i.e., those who will satisfy these commitments). Management
1140 commitment and authorization is generally easier to obtain when it can be demonstrated how information
1141 sharing helps to better protect the organization's critical assets, its reputation, and the well being of its
1142 customers, employees, and business partners. The leadership team plays an integral role and is
1143 responsible for providing continued oversight for the information coordination and sharing activities and
1144 for ensuring that resources are available to achieve specific objectives related to the organization's
1145 information sharing goals. The program's goals, objectives, and scope should be reevaluated and adjusted
1146 as needed, as mission or business requirements, priorities, technology, and regulations change.

1147 Information sharing and coordination initiatives often require the participation of stakeholders from
1148 different internal organizational units. The stakeholders should possess a sound collective knowledge of
1149 cybersecurity operations; organizational business processes, procedures, and systems; and the ability to
1150 promote and support information sharing and collaboration within their functional units. The roles,
1151 responsibilities, and authorities (both scope and duration) of the stakeholders should be well understood,
1152 enabling decisive action before, during, and after an incident. Handoff and escalation procedures should
1153 be in place to allow the effective transfer of authority and flow of information to key decision makers
1154 throughout the incident response life cycle. The specific authorities given to team members should be
1155 enumerated; describing both the internal actions (e.g., empowered to add rules to an organization's
1156 firewall or temporarily disable specific systems or applications during an incident) and external
1157 collaboration (e.g., permission to share designated types of information with a specified sharing
1158 community, such as the US-CERT, law enforcement, legal teams, or the media) that team members are
1159 permitted to perform.

1160 When possible, dedicated resources should be assigned to key leadership roles within the incident
1161 coordination and information sharing team, providing a trusted, consistent point of contact (POC) for
1162 internal and external sharing partners since high rates of personnel turnover can adversely affect the
1163 dynamics of sharing communities[16].

4.1.2 Conducting an Information Inventory

1165 An organization initiating a sharing and collaboration effort should perform an inventory that identifies
1166 information that supports key business functions (e.g., financial, employee, or customer data that may
1167 contain PII; intellectual property) and security operations (e.g., security alerts, logs, analysis results, threat
1168 intelligence). Information should have an assigned owner who serves as the organizational point of
1169 contact for the information and is responsible for determining its sensitivity, the level of protection
1170 required, and for managing it throughout the information life cycle.

1171 The inventory should identify the physical location (i.e., the geographic location of the server or storage
1172 media) and logical location (i.e., the network on which it resides) of the information. The inventory
1173 should identify how the information is stored; either as structured, machine-readable data (e.g., extensible
1174 markup language (XML), comma-separated values (CSV), JavaScript Object Notation (JSON)) or as
1175 unstructured data that has no pre-defined format (e.g., email message body, free text and images on web

---

[16] Merminod, V., Rowe, F., and Te'eni, D. *Knowledge Sharing and Knowledge Maturation in Circles of Trust: The Case of New Product Development*, 33rd International Conference on Information Systems, 2012

1176 pages, business documents). The format of the information plays a significant role in determining the ease
1177 and efficiency of information exchange, analysis, and use. Information stored using open, machine-
1178 readable, standard formats can generally be more readily accessed, searched, and analyzed. As the
1179 number of sharing partners, frequency of sharing, and data volumes increase the need for standard data
1180 formats and interoperable protocols becomes more pronounced.

1181 The inventory of information that supports security operations may include information derived from
1182 multiple sources within the organization including, IDSs, firewalls, antivirus software, and application
1183 logs. Specific data types and elements commonly of interest to incident handlers and network defenders
1184 include:

1185 • IP addresses and domain names

1186 • URLs involved with attacks

1187 • Simple Mail Transport Protocol (SMTP) headers, email addresses, subject lines, and contents of
1188   emails used in phishing attacks

1189 • Malware samples and artifacts

1190 • Adversary Tactics, Techniques, and Procedures (and effectiveness)

1191 • Response and mitigation strategies

1192 • Exploit code

1193 • Intrusion signatures or patterns

1194 • Packet captures of attack traffic

1195 • NetFlow data

1196 • Malware analysis reports

1197 • Campaign/actor analyses

1198 • Disk and memory images

1199 The information inventory is useful in a number of ways: (i) network defenders are able to develop
1200 prioritized monitoring and analysis strategies that focus on protecting the organization's most important
1201 information assets, (ii) an organization's resources can be more effectively allocated, (iii) ownership of
1202 information within the organization is formally established, (iv) information security analysts gain a better
1203 understanding of the likely value of the data source and the amount of effort required to acquire the
1204 information, (v) the organization is able to identify, understand, and document the information that is
1205 produced and consumed as part of business-specific workflows, (vi) the inventory can be used to develop
1206 guidelines, procedures, and mechanisms for information exchange.

1207 As part of the inventory process, organizations consider how existing information sources might be used
1208 more effectively. For example, could information that the organization currently possesses be enhanced
1209 through additional analysis, through more frequent collection, or by aggregating and correlating
1210 information with other sources? Another consideration is to determine if incident response activities and
1211 defensive capabilities are adequately served by current sources of information. Any observed gaps should
1212 be documented and addressed through enhancements to local data collection capabilities, updates to

1213 policy, or through external information sources as needed. The information inventory, once initially
1214 created, should be regularly updated to ensure that it is current, complete, accurate, and readily available.

1215 ### 4.1.3   Establishing Information Sharing Rules

1216 Organizations should work with information owners, key management personnel, and the organization's
1217 legal team to establish and vet the rules governing the handling of sensitive information. This review
1218 should focus on identifying the general types of information that the organization may want to share with
1219 an incident response community and determining its sensitivity based on the risks of sharing the
1220 information inside and outside of the organization. Such risks may include, revealing the organization's
1221 network architecture and defensive capabilities to an adversary, exposing intellectual property, or the
1222 inadvertent release of PII.

1223 #### 4.1.3.1   Information Privacy

1224 From a privacy perspective, one of the key challenges with sharing incident information is the potential
1225 for unauthorized disclosure of PII[17]. In the context of internal sharing, unauthorized disclosure could be
1226 disclosure to people who, by virtue of their job functions, would not typically have access to that PII in
1227 the normal course of business. They are performing a legitimate business function in terms of addressing
1228 the incident, but access to PII may not be truly necessary to adequately investigate the incident. For
1229 example, in conducting a forensics review of a hard drive, an analyst may review a file containing a list of
1230 employees that are under investigation for workplace hostility. The analyst does not have a need to know
1231 about the investigation, but may have a need to review the file for threat indicators associated with it.
1232 Generally, threat information that is shared externally is focused on actionable information for other
1233 organizations and should not contain PII.

1234 Table 5.1 introduces various types of incident data, provides specific examples of each data type, and
1235 briefly discusses some of the sensitivity and privacy considerations when handling each type of data.

Type of Incident Data	Incident Data Elements	Sensitivity Considerations	Privacy Considerations[18]
Network Indicators	URLs, domains, IP addresses, script file names	Generally, information about the attackers is deemed less sensitive than information about the victim, so it can often be more readily shared. Before releasing information, the organization should consider the potential net intelligence-gain/loss. (e.g., a public	Attackers may possess personal information gleaned from open sources, acquired through social engineering techniques, or acquired from previous successful attacks (i.e., from a compromised system)

---

[17] OMB Memorandum 07-16 defines PII as information which can be used to distinguish or trace an individual's identity such as
their name, social security number, or biometric records, alone, or when combined with other personal or identifying
information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.
OMB Memorandum 10-22 further states that "the definition of PII is not anchored to any single category of information or
technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining
the context of use and combination of data elements. In performing this assessment, it is important for agencies to recognize
that non-PII can become PII, whenever additional information is made publicly available, in any medium and from any source
that, when combined with other available information, could be used to identify an individual." NIST SP 800-122 includes a
slightly different definition of PII that is focused only on the security objective of confidentiality and not privacy in the broad
sense. Definitions of PII established by organizations outside of the federal government may vary based on the consideration
of additional regulatory requirements. The guidance in this document applies regardless of the definition of PII by
organizations.
[18] The PII confidentiality impact level as discussed in NIST SP 800-122 is a useful tool for gauging sensitivity of PII.

Type of Incident Data	Incident Data Elements	Sensitivity Considerations	Privacy Considerations[18]
		announcement that attacks are originating from a particular IP address will likely result in the adversary simply launching their attacks from an alternate IP address.)	
Packet capture	Network packet headers and payloads	Shared samples should filter on malicious traffic	Unencrypted or decrypted packets may contain PII such as logon credentials, financial information, health information, security investigation information, or information submitted via web forms
Phishing Email samples	Employee email	Email headers may contain infrastructure information such as internal IP address or hostnames	Consider anonymizing email samples and removing any sensitive information that is not relevant to incident responders
Webproxy logs	Logs of an organization's web activity, possibly including full URL's and parameters passed in requests	Log data may reveal business partner associations and contain logon credentials, portions of financial transactions, and other activities captured in URL parameters	Log data may contain PII regarding personal and business activity such as logon credentials, ID numbers used in URL parameters
Network traffic / "NetFlow"	NetFlow records provide a connection history between two IP addresses, including the time, duration, protocols used, number of packets exchanged, and number of bytes exchanged.	Generally less sensitive, though some organizations may not want to share full connection history and may "zero-out" low order bits in the IP addresses so that it is not possible to identify the network subnet.	NetFlow data may provide insight into employee behaviors or conditions that are not relevant to the investigation (e.g., access to websites about medical conditions)
Malware samples	Some artifacts associated with malware (e.g., log or staging files) may contain sensitive information from the victim's system.	Generally not considered sensitive, though proper handling, storage and encrypted transport should be used.	Context dependent based on a particular user's business and personal use of the resources that generate those artifacts

1236

Table 5-1: Commonly Used Incident Data

1237

1238 The type of PII that may appear in incident data is situation-dependent, but the requirement to protect PII
1239 remains. To ensure adequate protection of PII in incident data, it is important to include the organization's
1240 privacy official in planning and development of an incident response program. Incident response policies
1241 and procedures should incorporate guidance from the organization's privacy official so that they address
1242 requirements for handling PII during incident response, including whether and how to share that
1243 information internally and externally. For example, incident response processes may include steps for
1244 identifying the incident data types that contain or are likely to contain PII similar to the table above and
1245 acceptable measures for addressing privacy risks associated with those data types.

1246 When practicable, PII that is not relevant to investigating or addressing the incident should be redacted
1247 from incident data (e.g. working from a copy of incident data that has been scrubbed of known PII fields).
1248 Education and awareness activities are critical to ensuring incident response and sharing teams understand
1249 how to recognize and safeguard PII that is commonly encountered within the organization and are
1250 familiar with procedures for handling of PII.[19]

1251 An organization may benefit from integrating security and privacy incident and breach response
1252 processes, as the processes are mutually supportive. Often times, incident response teams are in the
1253 position to first know when a security incident is also a privacy incident or breach. Privacy breaches carry
1254 an additional set of privacy requirements that must be addressed in close coordination with the
1255 organization's privacy official.[20]

1256 **4.1.3.2 Information Sensitivity**

1257 When participating in an information sharing community, it is sometimes necessary to share data
1258 collected from the business-critical computers and networks; data that could possibly contain sensitive
1259 information. It is therefore important that an organization document the circumstances under which
1260 information sharing is permitted by evaluating the risks of disclosure, the urgency of sharing, the
1261 trustworthiness of the information sharing community, and the methods available to safeguard shared
1262 information.

1263 The information owner, management, and legal teams should adjudicate all sharing decisions using
1264 established procedures. The rules governing the sharing of information produced by the organization
1265 should be documented in local policies and procedures and expressed to external sharing partners through
1266 Memoranda of Understanding (MOUs), NDAs, Framework Agreements[21] or other agreements. Such
1267 agreements should established in advance of an actual incident and pre-vetted decision-making criteria
1268 should be in place, where possible, to control the risks of sharing while also enabling prompt coordination
1269 during an incident.
1270
1271 Many organizations handle information that is afforded specific protections under regulation or law.
1272 Examples of information requiring protection are privacy-related information such as PII, and information
1273 regulated under the Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI
1274 DSS), the Health Information Portability and Accountability Act (HIPAA), the Federal Information
1275 Security Management Act of 2002 (FISMA), and the Gramm-Leach-Bliley Act (GLBA). An organization
1276 should consult its legal team and experts familiar with the various regulatory frameworks to identify
1277 protected classes of information within the organization.
1278
1279 The handling procedures established by an organization should specifically address the types of sensitive
1280 information that are likely to be encountered by incident response personnel and explicitly state the
1281 conditions (e.g., risk, urgency, trustworthiness of the information sharing community) under which
1282 management authorizes sharing of protected information, and the circumstances that require decisions be
1283 escalated to management. Information sharing rules are often context-dependent and require careful

---

[19] For additional guidance and examples of controls for protecting PII during incident response and sharing, see the following controls in NIST SP 800-53, Rev 4: IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, IR-8, IR-10, AR-3, AR-5, DM-1, DM-2, SE-2, TR-2, UL-2.

[20] See NIST SP 800-53, Revision 4, control SE-2, Privacy Incident Response

[21] An example of such an agreement is the Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Program standardized Framework Agreement which implements the requirements set forth in Title 32 Code of Federal Regulations, Part 236, Section 236.4 through 236.6. See Federal Register at http://www.gpo.gov/fdsys/pkg/FR-2013-10-22/pdf/2013-24256.pdf for additional information.

1284 consideration of the nuances of the proposed sharing scenario to determine the extent or degree to which
1285 information should be shared. An organization's mission, legal requirements, regulatory environment,
1286 privacy concerns, and intellectual property considerations help shape these sharing policies. Through
1287 careful consideration of these factors, an organization must determine when the exchange of information
1288 is encouraged, limited, discouraged, or in some cases, forbidden. An organization may, for example,
1289 when a party in a lawsuit or other legal proceedings, chose not to share information that might under
1290 normal circumstances be readily shared. In some cases, information may be shared, but with specific
1291 restrictions (e.g., no attribution is permitted, specific data elements must be obfuscated before sharing).
1292
1293 These handling procedures seek to prevent the inappropriate release or mishandling of information,
1294 stipulate what information can be shared, when it can be shared, and how it must be protected. An
1295 organization's formal and informal information sharing agreements should stipulate protections consistent
1296 with approved information sharing rules. Should conditions change after a sharing agreement is in place,
1297 an organization should reserve the right to modify the agreement to accommodate emerging requirements.
1298 The documentation should be at a level of detail commensurate with organizational needs and updated at
1299 a frequency that does not impose an undue administrative burden. Incident responders, threat cell
1300 analysts, and operations personnel should, where possible, use automation to enforce information sharing
1301 rules to enable prompt, risk-managed, information coordination.
1302

4.1.3.3   Marking

1304 There are a variety of ways data can be marked-up or annotated in order to communicate how a message
1305 or document should be handled, or what specific elements might be considered sensitive and suitable for
1306 redacting, depending on an organization's needs.

1307 Clear handling guidance should accompany any data that is intended for exchange. Examples of handling
1308 guidance or designations are:

1309 • For Official Use Only

1310 • Distribution limited to first responders

1311 • Investigation underway, do not perform queries or active reconnaissance against these indicators

1312 Data marking and handling procedures should be clearly documented and approved by management. The
1313 personnel responsible for handing data should be trained in these procedures. For some incidents or threat
1314 intelligence, the collection methods may be considered confidential or proprietary, but the actual
1315 indicators observed may be shareable. In such cases it is useful to organize reports with a so-called "tear-
1316 off" sheet of shareable items.

4.1.3.4   Procedures for Sharing and Tracking Incident Data

1318 Over the course of time, an organization may face numerous attacks, participate in a large number of
1319 incident response efforts, and accumulate volumes of associated data. This data may be internally
1320 collected or may come from an external source. Tracking the source of data is important for both the
1321 protection of the information owners as well as for the enforcement of legal commitments such as NDAs.
1322 A balance must be struck between the need for rapid response and the obligations for protecting
1323 potentially sensitive data. When considering the capabilities of an organization's knowledgebase and data
1324 sharing processes:

1325 • Develop a list of data types and content, such as indicators, that can be shared quickly with relatively
1326   minor review with established sharing partners.

1327 • Develop a process for reviewing and protecting data that is likely to contain sensitive information.

1328 • Store and track information regarding the sensitivity of data to be shared, including any relevant
1329 NDAs or other handling constraints.

1330 • Track sources of data and with whom that data has been shared.

4.1.4 Joining a Sharing Community

1331

1332 Through the previous activities, an organization can better understand the information it currently collects
1333 and analyzes, the degree to which this information can be shared, and the additional information it needs
1334 to prevent incidents from occurring and to support the incident handling life cycle when they do occur.
1335 An organization can use this understanding to identify peers and other organizations with whom
1336 coordination and information sharing relationships would be beneficial. When evaluating potential
1337 sharing partners an organization should look to sources that complement the information collected
1338 internally (e.g., provides additional context), provide actionable information (e.g., indicators that an
1339 organization can readily use), and deliver information in a format and at a frequency that the organization
1340 is able to accept.

1341 An organization may consider the use of open source information repositories, commercial services,
1342 government resources, and public/private sharing communities to enhance its IT, security, and incident
1343 handling processes. The public/private sharing communities often organize around some shared
1344 characteristic such as a geographic or political boundary, industry sector, business interest, threat space,
1345 or other common attribute. The coordination relationships may be team-to-team, team-to-coordinating
1346 team, or coordinating team-to-coordinating team. Potential sharing partners include: ISACs, CERTs,
1347 external CSIRTs, Product Security Incident Response Teams (PSIRTs), media outlets, security websites,
1348 social media, threat and vulnerability repositories, vendor alerts/advisories, commercial threat feeds,
1349 malware/antivirus vendors, supply chain partners, sector peers, customers, and known victims of cyber
1350 incidents.

1351 When choosing a sharing community consideration should be given to the type of information that is
1352 shared within the community, the structure and dynamics or the community, and the cost of entry and
1353 sustainment. When evaluating the information that is shared within the community, consider the
1354 following questions:

1355 • What information does the community provide/accept?

1356 • Is the information relevant and does it complement locally-collected information? (i.e., provides
1357 meaningful insights into your organization's threat environment)

1358 • Is the information actionable?

1359 • Is the information timely, reliable, and of known quality?

1360 • What is the frequency and volume of data disseminated?

1361 • Does the organization have the capacity to ingest/analyze/store the information?

1362 In addition to the information shared within the community, consideration should also be given to the
1363 dynamics of the community and its participants, including:

1364 • What information-sharing model does the community use? (see section 2.5)

1365 • What is the size and composition of the community? (e.g., number of participants, information
1366 producers, and information consumers)

1367 • How active is the community? (e.g., number of content submissions/requests)

1368 • How trustworthy are the community members?

1369 • What are the technical skills and proficiencies of the community members?

1370 • How are decisions made within the community?

1371 • How is information communicated to its participants? (e.g., delivery mechanisms, formats, protocols)

1372 • What is the cost of entry and sustainment? (e.g., commercial service offerings, resources)

1373 • What type of sharing agreement does the community use? (e.g., formal vs. informal)

1374 • Is the sharing agreement well aligned with organizational goals, objectives, and business rules?

1375 When evaluating potential sharing partners, a great deal can be learned by observing the dynamics of the
1376 sharing community. Conversations with current or former community members may also provide
1377 valuable insights into community dynamics and the trustworthiness of its members. The trustworthiness
1378 of a community and its constituents is manifested in a multitude of ways, including the knowledge, skills,
1379 experience, integrity, reliability, communication abilities, and level of commitment of the community's
1380 members. NIST SP 800-39, *Managing Information Security Risk; Organization, Mission, and*
1381 *Information System View*, describes the following trust models that can be used to establish and maintain
1382 the level of trust needed to form partnerships, collaborate, share information, or receive services.

1383 • **Validated Trust.** One organization obtains a body of evidence regarding the actions of another
1384 organization and uses that evidence to establish a level of trust with the other organization.

1385 • **Direct Historical.** The track record exhibited by an organization in the past is used to establish a
1386 level of trust with other organizations.

1387 • **Mediated Trust.** An organization establishes a level of trust with another organization based on
1388 assurances provided by some mutually trusted third party.

1389 • **Mandated Trust.** An organization establishes a level of trust with another organization based on a
1390 specific mandate issued by a third party in a position of authority.

1391 • **Hybrid Trust.** An organization uses one of the previously described models in conjunction with
1392 another model(s).

1393 Mature sharing communities communicate regularly (e.g., using conference calls, email, portals with
1394 forums, social networking tools, and face-to-face meetings) to distribute and discuss current security
1395 threats, provide training and skills development, develop and share mitigation strategies, and define
1396 incident handling best practices. The level of maturity of the participating organizations often varies:
1397 some possess advanced monitoring, analytical, and forensic capabilities that allow them to produce
1398 information to share; other less mature organizations will participate primarily as information consumers.

1399 One mechanism for building trust is to orient the information exchange around a shared mission or
1400 business objective—creating a setting where members often confront common threats. This focus on
1401 common threats fosters greater cohesion within the community and provides greater focus. Trust can be

1402 further established and strengthened through face-to-face meetings between members and other events
1403 that help establish a level of personal rapport. Trust is also built as members share relevant technical
1404 insights, collaboratively build greater competency, work together to solve common problems, and lay a
1405 foundation to strengthen relationships through ongoing interactions with their peers.

1406 The expectations and responsibilities of the participants in these sharing relationships may be expressed in
1407 a variety of ways, including data sharing agreements, association bylaws, or other agreements. Although
1408 some information sharing communities operate informally, based on personal reputation and verbal
1409 agreements, others are based on more formal expressions of policy such as NDAs, SLAs, or other
1410 agreements. Small informal circles of trust are generally tight-knit sharing communities where reputation-
1411 building occurs over time through personal relationships and the demonstrated technical prowess of its
1412 members. Regardless of the degree of formality, when entering into any type of information sharing
1413 agreement it is important to adhere to the organization's information sharing and handling rules and
1414 ensure that incident coordination personnel have clear guidance regarding redistribution of information
1415 received from the community.

1416 As given in SP 800-61, having contact lists of key personnel is important when responding to an incident.
1417 If contact information must be supplied to a community, be sure to understand the degree of control that
1418 is provided over the visibility of this information to external users, community partners, and operators of
1419 the community (e.g., moderators, administrators). In bi-directional information sharing and coordination
1420 communities, the need for individual contact information may be necessary but a balance must be
1421 maintained between visibility, accessibility, and privacy. Participants in communities employing the hub-
1422 and-spoke model may not know other community members and only interact with the community's
1423 moderators or administrators. In addition to keeping contact information for selected peer organizations
1424 within an information sharing community, alternate communications mechanisms should be identified in
1425 case an incident compromises, disrupts, or degrades the community's primary communication channels.

4.1.5 Support for an Information Sharing Capability

1427 The threat intelligence that an organization receives should be applied as part of an overall computer
1428 network defense strategy, not simply in response to a known incident. An organization should have
1429 personnel, infrastructure and processes in place to collect and analyze the information from both internal
1430 and external sources. This information should be used proactively throughout the incident response life
1431 cycle to design and deploy better protective measures, to more effectively perform signature and
1432 behavior-based detection, and to inform containment, eradication, and recovery operations. An
1433 organization will incur costs related to its participation in information sharing and coordination activities
1434 but may avoid larger costs from successful attacks. It is important for an organization to approach
1435 processes and technology in a way that is sustainable based on their resourcing levels and overall goals.
1436 Human and IT resources should be applied in a way that maximizes their benefit. Once a sustainable
1437 approach is developed, it is important to ensure that adequate funding exists to cover personnel; training;
1438 hardware, software, and other infrastructure needed to support ongoing data collection, storage, analysis,
1439 and dissemination; and any membership or service fees required for participation in these communities.

4.2 Participating in Sharing Relationships

1441 An organization must establish operational practices that are compatible with those of the information
1442 sharing communities in which it is a member to make the most effective use of this additional
1443 information. Some practices are related to the types of information that are exchanged, the information's
1444 structure, the mechanisms for exchange, or semantics; others focus on the protection of information
1445 exchanged within the information-sharing community, or with the governance of the community.

1446 Participation in an information sharing community encompasses a number of related activities:

1447 • Engaging in on-going communication

1448 • Implementing access control policies for shared information

1449 • Storing and protecting threat intelligence, incident data, corrective measures, and evidence

1450 • Consuming and responding to alerts and incident reports

1451 • Consuming and analyzing indicators, TTPs, and corrective measures/course of actions

1452 • Creating written records

1453 • Performing local data collection

1454 • Producing and publishing indicators, TTPs, and corrective measures/course of actions

1455 • Producing and publishing incident reports

1456 The following sections expand on each of these activities.

4.2.1 Engaging in On-going Communication

1457

1458 Information sharing communities use a variety of methods for communicating, depending on the nature of
1459 the information to be shared and the speed with which it must be disseminated; some methods, such as
1460 email lists or portals, make it possible to participate in a relatively passive, low-cost manner for some
1461 organizations. Other methods, such as conferences and workshops, require dedicated staff and travel. For
1462 organizations that actively produce information for other community members, communication costs are
1463 likely to be relatively higher. Communications may be event-driven, e.g., in response to the actions or
1464 behavior of an adversary, or they may be periodic, such as bi-weekly reviews, teleconferences, and annual
1465 conferences.

1466 Message volume and frequency can vary widely across information sharing communities and largely
1467 depends upon the volatility of the attributes being observed, the importance that the community places on
1468 having the most current information, and the intended audience of the information. High volume sharing
1469 communities may publish summary information or digests (i.e., instead of sending individual messages, a
1470 collection of messages are sent that cover a specified period of time) to reduce the frequency of message
1471 traffic. Some recipients may be seeking only summary data (e.g., rollups) and have no need for detailed
1472 information. For an organization that has recently joined an information sharing community, just keeping
1473 up may be a significant effort, particularly until the organization has developed the skillsets needed to
1474 evaluate messages received (or found on a portal). In the early phases of participation, an organization
1475 may wish to focus on studying any best-practices guidance offered by the community, observing the
1476 messages sent by more experienced members, and querying databases made available by the community.

1477 An organization's personnel should possess the technical skills needed to effectively communicate within
1478 their information sharing communities. The specialized skills required for incident handling and
1479 coordination are acquired over time through hands-on experience and training. Organizations should seek
1480 to minimize turnover within this team to foster enduring information sharing relationships, minimize
1481 knowledge loss, and preserve investments in training. Stability within the incident coordination team
1482 facilitates the formation of trusted professional relationships that span different CSIRTs and organizations
1483 — relationships that can be crucial during incident response.

1484 In addition to developing technical skill sets and professional relationships, information sharing
1485 communities should employ communications protection measures when coordinating. Some communities
1486 issue authentication credentials for a web portal that can be used for coordination; in this case, the
1487 security of the portal itself (and the implementation of secure communication channels between clients
1488 and the portal) provides communications security. Other communities may issue or rely on a certificate
1489 hierarchy allowing participants to use public key cryptography to allow message senders to encode
1490 messages so that only designated receivers can decrypt. Other communities may use a web of trust
1491 model[22], in which certificates are distributed without a single hierarchy. Other communities may use
1492 dedicated physical networks, virtualized networks (e.g., peer, overlays), or a message bus as a secure
1493 media for conducting coordination activities. Protecting communications among participants is extremely
1494 important, particularly when the messages may contain information about techniques used by an
1495 adversary, PII, proprietary, or other sensitive information.

1496 When one or more organizations are under attack or have been compromised, it is important for defenders
1497 to establish a means of secure communications, ideally physically and logically separate from the
1498 enterprise's infrastructure. An alternative cellular phone provider and externally managed collaboration
1499 portal are examples of such independent communication channels. If one believes that
1500 telecommunications services may be subject to eavesdropping, one may consider encrypting the voice
1501 channel as well. It is important to establish these communications amongst defenders before an incident
1502 takes place. Alternate data communications channels to share breaking threat indicators in the event of
1503 compromise may also be necessary to avoid eavesdropping by an adversary.

1504 In addition to managing the communications mechanisms in a secure way, it is also necessary to ensure
1505 the efficient dissemination of information within the organization. Drawing on some of the key concepts
1506 presented in NIST SP 800-39, coordinated incident management processes should aim to operate
1507 seamlessly across all tiers of the organization at the (i) organization level; (ii) mission/business process
1508 level; and (iii) information system level. Inter-tier and intra-tier communication should be employed to
1509 create a feedback loop for continuous improvement and to help ensure that all stakeholders in the
1510 intrusion response are fully informed and effectively engaged in decision-making processes.
1511
1512 Decision-making in support of incident handling follows a similar model, where multiple incident
1513 response decision-making loops are executed concurrently with coordination and communication
1514 occurring in and between organizational tiers[23]. The established roles, responsibilities, and scope of
1515 authorities conferred to participants determine, to a large extent, how information sharing and
1516 coordination occurs within an organization. For example, operations personnel may be permitted to make
1517 decisions regarding configuration changes without seeking approval from the management or legal teams,
1518 provided the changes do not negatively affect customers or business partners, or prevent the organization
1519 from satisfying its business, legal, or regulatory obligations. The goal is to provide information that can
1520 be acted upon by stakeholders in the incident response process across all organizational tiers. The
1521 information provided can be used to inform policy changes at the organizational level, process changes at
1522 the mission/business level, or actions at the information system level, including patching, system
1523 configuration changes, introducing additional access control rules, removing devices from the network, or
1524 making network architecture changes.
1525

---

[22] The web of trust concept was introduced by Pretty Good Privacy (PGP).
[23] Information regarding the Coordinated Incident Handling model is available in the IEEE publication titled *Operationalizing the Coordinated Incident Handling Model*

4.2.2 Implementing Access Control Policies for Shared Information

In order to address the risk of unauthorized disclosure of information, organizations should establish and enforce access control policies appropriate for the information being protected. The organization must ensure that access controls are in place, functioning as intended, and that processes are in place to establish oversight and accountability for the controls. Access control policies should take into consideration the information sharing rules and handling requirements established by the organization (see Section 4.1.3, Establishing Information Sharing Rules) and those expressed in information sharing agreements executed with partners. Multi-national organizations need to consider the national or regional policies related to privacy and information sharing when establishing and enforcing access control policies (e.g., sharing between business units operating in different countries). Additionally, access to information of a certain categorization or classification may be limited by business unit or department, role, or group membership.

When exchanging information with external entities, organizations must protect and distribute two basic types of information:

- Information produced within the organization (i.e., locally-produced)

- Information received by the organization from external sources

4.2.2.1 Locally-Produced Information

Locally-produced information may contain sensitive information, including critical business information, technical information that could reveal vulnerabilities in an organization's computing infrastructure, and information that is protected under regulation or law. Information that is determined to be sensitive must be protected through the implementation of security controls or mechanisms and through the enforcement of the organization's information sharing rules. Sensitive information can be protected through a variety of means, including:

- Authentication mechanisms that verify the identify of a user, process, or device through the use of usernames and passwords, cryptographic keys, tokens, biometric characteristics, or other authenticators.

- Encryption capabilities that protect sensitive data (including authenticators) by converting the plaintext information into ciphertext using a cryptographic algorithm.

- Authorization controls that grant access privileges to an authenticated user, program or process.

- Sanitization actions that remove, replace, redact, encrypt, or mask specific data elements.

When sharing incident and indicator information with peer organizations, sharing partners, or the public, an organization may wish to anonymize the data to some extent, depending on the context and agreed-to sharing arrangements. For phishing and other attacks, it is natural to look for instances of the targets' names, email or account names, in the body as well as the subject and attachments of the message. Organizations may also not wish to share the fact that they have been attacked, so reports may employ pseudonyms such as "USBUS1". If this is the case, then any artifacts of the attack, such as packet captures or files should be examined for revealing target IP addresses, domains, and URLs.

If sharing is a regular practice, then a review/release process should be established according to agreed-upon guidelines to mitigate inadvertent identity disclosures. When incident data contains PII, consult the

1566 organization's privacy official to determine appropriate measures for redacting or anonymizing PII prior
1567 to sharing the information. Section 4.2.3 of NIST SP 800-122 provides guidance for anonymizing PII.[24]

4.2.2.2 Information Received from External Sources

1569 In addition to the protections specified by governing law and regulation pertaining to privacy and other
1570 protected classes of information, an information sharing community may impose more restrictive terms of
1571 use on information shared within the community. These restrictions will vary by community, some being
1572 relatively simple and low-cost such as a verbal agreement to limit distribution of the information to the
1573 incident response team personnel within your organization; other agreements may be more formal and
1574 contain clauses enumerating specific obligations such as permitted/prohibited uses; ownership of
1575 intellectual property and community-submitted content; use of linkages or references to information; and
1576 obligations to outside organizations such as law enforcement or regulatory agencies.
1577
1578 Formal sharing communities generally employ a framework agreement that specifies the responsibilities
1579 of participants in both legal and technical terms. Such a community may rely on federally managed
1580 administrative systems for establishing trust, such as the federal system for the protection of classified
1581 information and the clearance processes that support it. For example, one way to share information
1582 pertaining to the protection of unclassified systems is to exchange possibly sensitive vulnerability and
1583 protected information from those systems using a separate, classified, network. Such formalized sharing
1584 relationships can achieve high levels of trust since the community-specific restrictions can dictate that
1585 community information be viewed and processed only by cleared staff and only on highly-protected
1586 systems. Some communities may also impose need-to-know rules, and require that a participant's incident
1587 coordination staff be individually authorized to access community information.
1588
1589 A somewhat less formal approach is to require that participants sign an NDA and that participant incident
1590 coordination staff hold clearances. In this context, information exchanged should be labeled with handling
1591 guidance, e.g., that the information should remain in the community, be released openly, or shared
1592 without source attribution.
1593
1594 A less formal approach is to require all community members to sign a memorandum of understanding
1595 (MOU), so that all participants can be considered to be trusted to the extent that they have agreed to the
1596 terms of the MOU, and then to use access control lists (or equivalent group-oriented mechanisms) to
1597 specify which community members should have access to specific messages shared with the community.
1598
1599 Some communities may also adopt an information sensitivity marking convention such as the US-CERT
1600 Traffic Light Protocol (TLP)[25] depicted in Figure 4-2.
1601

---

[24] Another useful source for anonymization criteria can be found in the Health Insurance Portability and Accountability Act (HIPAA) regulations at §164.514(b). These criteria are only required under certain circumstances but are a useful set of criteria for other applications.

[25] Traffic Light Protocol, http://www.us-cert.gov/tlp
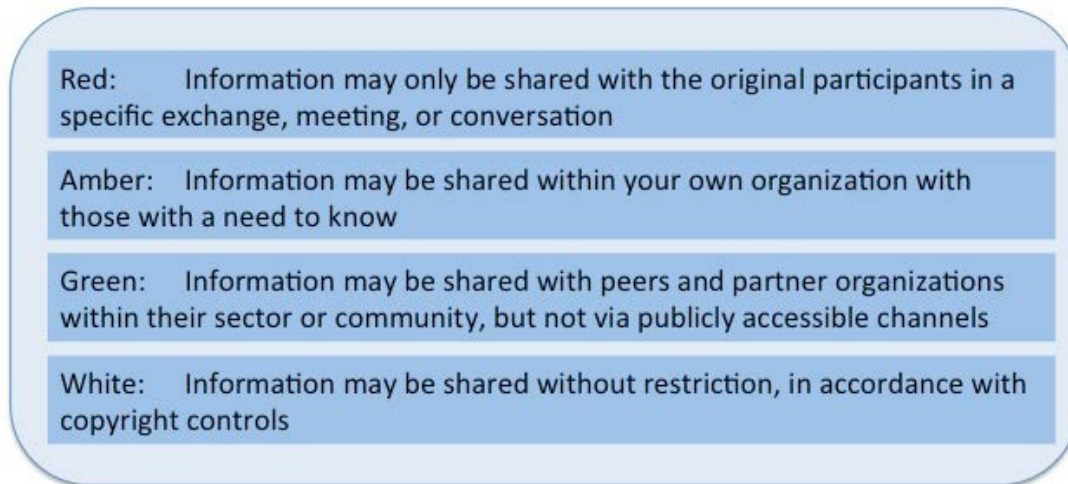
Figure 4-2: US-CERT Traffic Light Protocol

The TLP specifies a set of restrictions and a color code for indicating which restrictions apply to a particular record. In the TLP, red specifies the most restrictive rule, with information sharable only in a particular exchange or meeting, not even with a participant's own organization. The amber, green, and white color codes specify successively relaxed restrictions.

4.2.3   Storing and Protecting Evidence

As part of the information management, consideration should be given to how evidence is to be stored and protected. Basic questions to consider include:

- Is an appropriate backup policy in place and exercised?[26]

- Who is permitted access to the information?

- What qualifications will be required for system administrators that have access to the data? Background investigation? Citizenship?

- How long should the data be retained?[27]

Evidence should be collected and preserved using best practices for data preservation following chain of custody requirements, and other laws pertaining to the submission of evidence. A more detailed treatment of forensic techniques related to chain of custody and preserving information integrity are available in NIST SP 800-86 and section 3.3.2 of NIST SP 800-61, Revision 2.

Common security controls[28] should be employed where appropriate:

---

[26] NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* provides guidance regarding IDPS principles and technologies.
[27] For federal agencies, National Archives and Records Administration (NARA) General Records Schedule (24) Item 7, "Computer Security Incident Handling, Reporting and Follow-up Records" requires that these records be destroyed/deleted 3 years after all necessary follow-up actions have been completed. Research conducted by Mandiant indicates adversaries have maintained access to victim networks for close to five years. The complexity of evaluating incident data and potential difficulties at connecting a series of related incidents that initially appeared unrelated, coupled with the potentially lengthy timeframes on which adversaries may operate signal the need to re-evaluate the 3-year retention period for incident handling data.

1624   •   Data in transit should be protected by encryption.

1625   •   Physical media such as CD's and DVD's should also be encrypted if that is the mechanism for
1626   exchanging data.

1627   •   Strong, two-factor authentication should be employed for portal or server access to data.

1628   •   Web portals and file servers should employ strong cryptographic protocols to provide
1629   communications security.

1630   •   Access to data should be logged and audited regularly.

1631   •   Intrusion detection should be deployed.[29]

1632 Malware samples require special storage, access, and handling procedures. Malware samples are often
1633 preserved to support offline analysis and as evidence for an ongoing investigation or legal proceeding.
1634 Organizations often store not only the malware sample, but also accompanying metadata, artifacts, and
1635 analysis results. A malware sample that is not safely quarantined or sandboxed during unpacking and
1636 storage could propagate to enterprise networks and systems. Additionally, care must be taken to ensure
1637 that antivirus and anti-malware products do not inadvertently detect and remove an organization's
1638 malware collection. Common practice is to store malware samples in an isolated, protected file system or
1639 database as password-protected compressed files to avoid being inadvertently wiped by antivirus products
1640 during transit.

1641 In the case of commercial threat intelligence services, the provider usually retains the rights to the
1642 intelligence collected at each customer point-of-presence and can use that information to improve
1643 intelligence and defenses. A threat intelligence sharing community may find that some members may
1644 wish to make use of the community's data for research or even product development. Each community
1645 should consider these data use cases when drafting their membership charter.

1646 Organizations should determine the appropriate retention policies for information about attacks[30].
1647 Multiple types of information with varying policies may be involved. There are motivations to retain
1648 detailed information for an indefinite period of time, since this provides historical value as well as helps
1649 new members or sharing partners understand the persistence and evolution of different adversaries. Other
1650 considerations, such as financial, legal, contractual, or regulatory, may require one to limit data retention
1651 to a fixed period of months or years. The retention policy for shared repositories should be determined by
1652 its members, in consultation with the appropriate records management personnel and legal counsel for
1653 each organization, and made explicit in any information sharing agreements. Once the retention schedule
1654 is satisfied, organizations must either archive or destroy the incident data in accordance with the
1655 applicable policies.[31]

1656 For consortiums or organizations in specific industries or fields, there may be additional guidelines for
1657 storing and handling information. For example, organizations that are subject to HIPAA have

---

[28] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* provides a catalog of security and privacy controls and a process for selecting controls to protect organizational operations and assets from a diverse set of threats.

[29] NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)* provides guidance regarding IDPS principles and technologies.

[30] Federal agencies are subject to the National Archives and Records Administration (NARA) General Records Schedule as well as agency-specific retention policies.

[31] Draft NIST SP 800-88, *Guidelines for Media Sanitization*, provides guidance to assist organizations in making risk-based decisions regarding the sanitization and disposition of media and information.

1658 requirements for safeguarding protected health information (PHI). If there are any discrepancies between
1659 the organization's obligation to protect certain information types and how that information is handled
1660 during the incident data sharing process, the key stakeholders and information owners as well as the
1661 organization's counsel must work collaboratively to identify the appropriate course of action.

1662 An incident-coordinating or threat-sharing collaborative entity may well become a target of attack in and
1663 of itself. Therefore, measures should be taken to ensure that the infrastructure is adequately protected and
1664 monitored, that hosts and applications are maintained with current security patches and configurations,
1665 and that applications are free of common coding flaws[32].

4.2.3.1   Information Stored by a Community Portal

1667 Some communities provide a portal that maintains stored information for sharing. For these communities,
1668 it is necessary for participant organizations to access the portal to find, analyze, download, and upload
1669 shared information. Access to a shared portal may be triggered by significant events, such as alerts, may
1670 be periodic, or both. It is important for organizations to carefully manage and protect all credentials used
1671 to access the portal, to clearly understand the notification mechanisms used by a community, and to
1672 regularly visit the portal to contribute content, download new information, and to participate in
1673 coordination activities within the community. Organizations should understand that interaction with a
1674 shared portal requires a level of ongoing effort.
1675
1676 Each community portal may implement a specific set of data access and retention policies. In order for
1677 organizations to have confidence that shared information is available and appropriately preserved,
1678 organizations should understand the access control policy of a shared portal and its data retention policies.
1679 In order for participants to trust a portal's ongoing availability and performance, a community should
1680 have a written SLA for the portal which specifies expected availability, the security posture of the portal,
1681 expected outages, acceptable usage policies, and any remedies for failure to perform.
1682
4.2.3.2   Information Stored by an Organization

1684 If an organization stores shared information on its own computers and networks, the organization should
1685 institute practices that minimize the likelihood of data loss, protect the data from unauthorized access, and
1686 provide mechanisms for search and analysis. During an incident, it may be important to access shared
1687 information quickly; consequently, the information should be available and readily accessible to
1688 authorized incident handling personnel. An organization should ensure that shared information is
1689 ensconced on systems that are well protected and available during an incident.
1690
1691 It is important to understand that shared information may be voluminous and that a storage system is
1692 required that can scale and that also provides for the confidentiality, integrity, and availability of the
1693 information. An organization should formulate a data retention policy for shared data that balances cost
1694 with the need to retain historical information. One possibility is to deploy a database system, within an
1695 organization's network, that uses replication to preserve shared information in the event of hardware
1696 failures, and to compress or reduce older records on a schedule.
1697

---

[32] The NIST Software Assurance Metrics and Tool Evaluation (SAMATE) project seeks to develop standard evaluation measures and methods for software assurance. http://samate.nist.gov/index.php/SAMATE_Publications.html

1698   ### 4.2.4   Consuming and Responding to Alerts and Incident Reports

1699   An information sharing community may send out alerts or incident reports to its members. An alert
1700   generally provides technical information that receivers can use to understand their degree of exposure to a
1701   particular vulnerability, the potential impacts of a problem (e.g., application crashes, data exfiltration,
1702   hijacking), and recommended steps to effectively mitigate the problem. An incident report documents a
1703   problem in greater detail and categorizes an incident by type. It is important to understand that both alerts
1704   and incident reports may contain sensitive information and may, if publicly disclosed, reveal to
1705   adversaries some of the defensive capabilities of members if the information sharing community. Incident
1706   reports in particular may contain sensitive information that should be shared only with community
1707   members with which a high level of trust has been established. In either case, a participant in an
1708   information sharing community must appropriately protect the information in an alert or report and must
1709   independently decide how to respond.

Systems Affected	List of operating systems and/or applications affected.
Overview	Bumper sticker summary.
Description	Paragraph-level summary.
Impact	Estimate on what adversaries might be able to do
Solution	Steps that might mitigate the problem. Possibly detailed instructions.
References	Technical documents and bulletins.
Revision History	Dates for creation and updates.

Source: US CERT

1710
1711   **Figure 4-3: US CERT Alert**

1712   Figure 4-3 depicts an alert as documented by US CERT. This kind of alert identifies the types of systems
1713   that could be affected by a problem, provides a short overview of the nature of the problem, provides an
1714   estimate of the negative effects of the problem (e.g., system crash, data exfiltration, application
1715   hijacking),[33] possible steps to ameliorate the problem, and pointers to other sources of relevant
1716   information.
1717
1718   When an organization participating in an information sharing community receives an alert, the
1719   organization should evaluate how to respond based on the answers to six key questions.
1720
1721   1. *Does the alert apply to my organization's information technology assets?* An organization should
1722   compare the affected products identified in an alert with the information technology products
1723   deployed within their organization, preferably in an automated manner. If the organization does not
1724   use the products described in the alert, it may not be directly affected but it could still be impacted in
1725   unforeseen ways. If the alert applies to an organization's information technology assets, the remaining
1726   questions in this list should be considered.
1727
1728   2. *Are the suggested mitigations, if provided, both safe and effective?* An organization can approach this
1729   in two basic ways: (i) directly assess, analyze, and test the efficacy of the proposed mitigations, or (ii)
1730   if the source is deemed trustworthy and the suggested course of action seems viable, accept the
1731   mitigations as proposed. Organizations should consult multiple sources to arrive at an overall

---

[33] A more extensive list of potential effects is given in the MITRE Common Weaknesses and Vulnerabilities Types.

1732 judgment about the accuracy of an alert and the technical competency and the degree of diligence
1733 demonstrated by the submitter and base any mitigation decisions on information that is well-
1734 understood and comes from a trusted source. Organizations should seek out personal connections
1735 with competent technical personnel within the community. These connections can be developed
1736 through participation in community events formed around common technical or research interests, at
1737 information sharing conferences, or through collaborative incident response. A source's past and
1738 ongoing participation in an information sharing community can also be used to gauge their reputation:
1739 Have the source's recommendations in the past proven to be both safe and effective? Do the alerts
1740 issued by the source display a high degree of quality and technical knowledge? Some communities
1741 have rigorous membership processes that require prospective members to be sponsored by a current
1742 member and demonstrate a high degree of technical competency. In such cases, membership in the
1743 community itself attests to the trustworthiness of the source.

1744
1745 3. *Does my organization have access to the skills to implement the mitigation guidance?* Performing the
1746 mitigation steps may require specific, and sometimes scarce, technical skills. Mature organizations
1747 may already possess these skills, but less capable organizations may not have personnel with the
1748 requisite skills. Improving technical skills through training or bringing on contracted staff with the
1749 appropriate skills and experience is a time-consuming process, it is therefore important for an
1750 organization to establish (perhaps contractual) relationships with an appropriate consulting entity or
1751 service provider who can respond quickly if needed. In the longer term, it is important for an
1752 organization to understand the skill sets that are needed to respond to the alerts and incident reports
1753 flowing through a community, and to develop or hire staff with the skills to meet these needs.

1754
1755 4. *What would be the costs of mitigation?* Mitigation strategies vary in their costs and impacts on an
1756 organization's ability to execute its mission. Some mitigation techniques, like filtering traffic from a
1757 specific set of IP addresses, are relatively low-cost and low-risk, but others, such as retiring
1758 vulnerable software versions, may be disruptive to implement. An additional consideration is the level
1759 of confidence that an organization has regarding the mitigation's effectiveness and side effects. A
1760 configuration change to a firewall, for example, may have unanticipated side effects to the mission.
1761 An organization should scrutinize mitigation techniques carefully, organize them using a change
1762 tracking process, perform pre-deployment testing when time permits, and preserve the ability to
1763 reverse mitigation techniques that turn out to be too costly or ineffective.

1764
1765 5. *Given my organization's mission and the possible infeasibility of mitigation strategies, should I*
1766 *perform mitigations at all?* When mitigation strategies cannot be realistically adopted because of cost
1767 or because the needed skills are not available, it may be necessary tolerate the additional risk posed
1768 by the problem described in an alert. An organization should consult the NIST Risk Management
1769 Framework (SP 800-37) for guidance on how to operate with known risks through maintaining a
1770 security plan and performing periodic security assessments to determine effectiveness of security
1771 controls. A supplementary strategy is to strategically reduce services where mitigation is difficult but
1772 where the mission can be achieved with reduced service levels.

1773
1774 6. *Is this alert associated with a campaign or wave of attacks?* An organization should evaluate the alert
1775 in the context of observed events, both current and historical. Through the analysis of information
1776 from local data sources and external sharing partners an organization may be able to correlate
1777 indicators; reveal meaningful patterns or sequences of indicators; or identify indicators that are
1778 common across multiple incidents. Organizations with advanced incident response capabilities may
1779 also be able to expose similarities in the adversary's TTPs; the specific types of organizations,
1780 systems, devices, or information targeted; or observe behaviors that are commonly exhibited by the
1781 adversary. When an analyst observes multiple incidents with the consistent appearance of specific
1782 indicators, TTPs, and behaviors within the attack lifecycle it is likely that the incidents are related and

1783   possibly part of a larger campaign by an adversary. By shifting the focus from tactical detection and
1784   remediation (i.e., single event-oriented) to the detection of campaigns, network defenders can devise
1785   courses of action that prevent, or at a minimum, make it harder for the adversary to achieve their
1786   goals. When an organization is able to enrich the information it receives from its sharing partners
1787   (e.g., by identifying additional related indicators or behaviors) or through its analysis has reason to
1788   believe that a campaign or wave of attacks is underway, it should share this information with its
1789   partners if possible and appropriate. By sharing this information, the knowledge maturation cycle can
1790   continue, improving the overall fidelity of detection methods and related mitigation strategies.
1791

1792 Figure 4-4 depicts an incident report as described by US CERT. An incident report presents a more
1793 complete view of a problem. As shown in the figure, an incident report will generally characterize an
1794 incident by type, give a range of dates when it was active, provide source information, describe functional
1795 impacts, describe vulnerable system types, and summarize the impacts and resolution strategies. Much of
1796 this information may be very sensitive, and information-sharing communities tend to distribute incident
1797 reports primarily in trusted venues.

Incident Type	One of: unauthorized-access, DoS, malicious-code, improper-usage, scans/probes/attempted-access
Incident date/time	Source IP, port, protocol
Operating System, version, patches	
System function (e.g., web server)	Location of systems involved
Anti-virus software configuration	Method used to detect the incident
Impact to agency Resolution	Source: US CERT
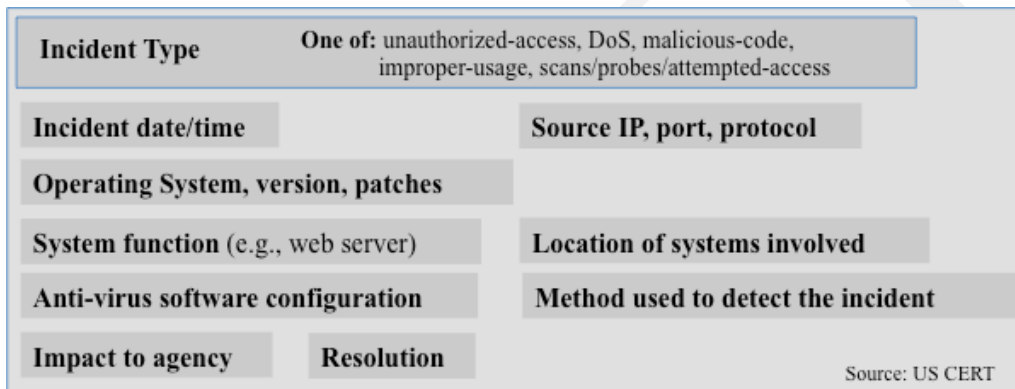
1798
1799 **Figure 4-4: US CERT Incident Report**

1800
1801 ### 4.2.5   Consuming and Analyzing Indicators

1802 A key aspect of consuming and analyzing indicators is that an organization must be able to monitor the
1803 same underlying observable events that are monitored and referenced in indicators by other participants in
1804 an information sharing community. If an information sharing community distributes an indicator about a
1805 particular set of observables, this will not help a receiving organization unless that organization can
1806 configure its systems to also monitor that set (or a significant subset) of observables. An organization
1807 should therefore, at a minimum, gain access to technical skills (either organization personnel or
1808 contractors) that are sufficient to configure event collection mechanisms as needed to monitor observables
1809 of interest to the community, and to perform a threat analysis of the observables to understand how they
1810 may relate to the organization's mission.

1811 When receiving indicator from external data sources a series of activities are generally performed to
1812 ensure that the information can be efficiently put into use by the receiving organization. These activities
1813 may include categorization, initial prioritization, decompression, decryption, validation, and content
1814 extraction. Categorization requires a review of the content metadata to determine the security designation
1815 and handling requirements for the content received. Sensitive information may require encrypted storage,
1816 more stringent access control, or limitations on distribution. Content like malware samples or artifacts
1817 may require special handling precautions to prevent their inadvertent introduction on production
1818 networks. Initial prioritization ensures that newly received information is processed in the most

1819 advantageous manner and may be based on the perceived value of the data source, the overall confidence
1820 level of the data, an operational requirement that specifies that data sources be processed in a particular
1821 order, the degree of preprocessing required to transform the data into actionable information, or other
1822 factors.

1823 Analysis of indicators includes a broad range of activities that are focused on the rapid identification of
1824 malicious actors and actions within an organization's systems and networks. By integrating and
1825 correlating data from internal sensors (e.g., antivirus, IDS/IPS, DLP) and network monitoring systems
1826 with data received from external sources an organization can expose and characterize relationships
1827 between indicators that allow cyber defenders to more effectively identify an adversary's activities and
1828 behaviors and rapidly apply effective mitigations. Analysis activities can also include identifying patterns
1829 of attack or misuse, contextual analysis that considers the conditions under which a pattern is observed,
1830 and incident timeline reconstruction. Indicator analysis processes should inform the selection of courses
1831 of action, defensive measures, and mitigation strategies.

1832 ### 4.2.6 Creating Written Records

1833 An organization should produce and maintain written records throughout the incident response lifecycle.
1834 The written record produced by an organization should be able to answer the following key questions:
1835
1836 • What happened? When did the incident occur?

1837 • How was it detected?

1838 • Who took part in the incident response? When were they notified?

1839 • What actions were taken in response to the incident? What was the rationale behind these actions?

1840 • What was the overall impact of the incident?

1841 By answering these questions, an organization will be better able to reconstruct the timeline and narrative
1842 of the response activity. This documentation is much easier to produce at the time of the incident, while
1843 the details of the incident are fresh in the minds of the participants; important details are often lost when
1844 events are documented ex post facto. It is important to capture information regarding indicators; the TTPs
1845 used by the adversary; the types of systems targeted/affected; and possible adversaries. When
1846 documenting decisions, describe the deliberations that led to the final decision. Document the amount of
1847 downtime suffered, the recovery/restoration process, and describe the mitigation strategies employed or
1848 other courses of action. Be sure to collect, preserve, and safeguard as much information as possible – this
1849 information may be necessary to support future legal action, for termination/disciplinary actions for
1850 insider threats, or to shape incident response policies and procedures. Any information that could be used
1851 to better protect the organization (and its sharing partners) in the future should be captured.
1852
1853 An organization should produce an after-action report that captures lessons learned for each phase of the
1854 response cycle (e.g., a particular indicator that, if observed, would have allowed the organization to act
1855 sooner and perhaps disrupt or stop the attack earlier in the cyber attack life cycle). Use the lessons learned
1856 to identify opportunities for improvement – focus on identifying and addressing weaknesses that were
1857 exposed in the response plan. The after-action report is an opportunity to formally document what went
1858 well during the incident response, and what did not. Based on the lessons learned, implement any changes
1859 to policy, management, and/or operational practices that are necessary. These changes could include
1860 identifying supplemental information; personnel training; or other protective or detective measures that
1861 would have allowed the incident to be prevented, responded to more rapidly, detected earlier, or

1862 recovered from faster. In the aftermath of an incident, the overriding objective is to prevent a similar
1863 incident from occurring in the future.
1864
1865
1866 **4.2.7   Performing Local Data Collection**

1867 Organizations that have the resources to monitor their systems and networks should identify and
1868 configure local data collection capabilities. Commonly available data sources include the log files and
1869 alerts generated by network devices, security appliances, operating systems, antivirus products,
1870 applications, and intrusion detection/protection systems. Local data collection entails more than just
1871 enabling logging on these various sources; logging parameters must be configured to capture those events
1872 and alerts that provide the most value to the incident responder.
1873
1874 When configuring log collection parameters, consideration should be given to the volume of data that a
1875 particular setting is likely to produce. Log configuration should be actively tuned to bring relevant events
1876 into sharper focus, remove "noise" (i.e., data with little or no practical value) from the channel, and
1877 ensure that the data collection strategy is not so aggressive that it creates a self-imposed denial of service.
1878 This tuning may include establishment of alerting thresholds; determining what actions/accesses will or
1879 will not be logged; and defining baselines for network activity, system configurations, and filesystem or
1880 registry objects. A significant consideration is also to ensure that logging errors are appropriately handled
1881 by defining how the logging system should respond when specific errors are encountered (e.g., can't
1882 complete a "write" operation because the disk is full or network connectivity has been lost).
1883
1884 Local logging and monitoring practices can be refined and improved upon based on input received from
1885 sharing partners, after-action reports, red team exercises, and by reviewing the alerts/events generated by
1886 an organization's own security scans. The frequency and/or scope of information collection may on
1887 occasion be temporarily increased (e.g., additional objects are monitored, more frequent measurement of
1888 network/CPU/disk utilization, both successful and failed object/service accesses are logged) in response
1889 to an active incident or to assist with fault detection, isolation, and correction during troubleshooting of
1890 networks and systems.
1891
1892 Threat sharing organizations collect threat intelligence from a variety of sources, including open source,
1893 internal malware repositories, and key external partners, easily collecting thousands of indicators in a
1894 short time. Inevitably, there is a need to store and organize this information into in some kind of
1895 structured knowledgebase. Free-form methods such as wikis can be quite flexible and suitable for
1896 developing working notes, while ticketing systems are good for tracking response activity. Some form of
1897 structured database is useful for organizing and tracking intelligence, and above all, querying and
1898 analyzing the collected threat information. An organization's collections or knowledgebase should pay
1899 particular attention to any TTPs regarding known adversaries that have been targeted by them.

1900 Organizations typically collect the following items in a knowledgebase:

1901 • Source of the indicator

1902 • Rules (e.g., NDAs) governing the use of or sharing of this indicator

1903 • When the indicator was collected by the organization

1904 • How long the indicator is valid

1905 • Groups or adversaries associated with the indicator

1906   •   Aliases of different adversaries or attack groups

1907   •   TTPs commonly used by the adversaries or attack groups

1908   •   Employees or types of employees targeted in the attacks

1909   •   Systems targeted in the attacks

1910
1911 It is often desirable to consolidate the log files from multiple sources to a centralized logging server or
1912 analytics platform such as a SIEM platform. Such aggregation, correlation, and analytics capabilities can
1913 be implemented using locally deployed hardware and software, or deployed in a cloud through various
1914 types of commercial service offerings. Section 3.4, presents specific considerations when evaluating and
1915 selecting commercial service offerings. The use of an analytics platform, depending on its feature set, can
1916 make it easier to correlate disparate data sources, perform offline analysis, support trending, and
1917 visualization. The ability to graphically depict data sets offers a unique perspective that may expose
1918 patterns of relationships among the data elements that might otherwise go unnoticed.

1919
1920 As part of the data collection process, an organization must also establish and implement a data handling
1921 and retention strategy. The data handling guidelines will specify the access control requirements for the
1922 log files; stipulate the rules governing data capture and acceptable use (e.g., avoid capturing sensitive data
1923 or PII); and protect log data at rest (e.g., both online and offline storage), in memory (i.e., by protecting
1924 the logging and analytics services), and in transit using end-to-end encryption where messages are
1925 encrypted by the sender and decrypted by the recipient with no third party involvement (e.g., PGP) or
1926 server-to-server encryption such as SMTP over Transport Layer Security (TLS) that uses Public Key
1927 Infrastructure (PKI) for encrypting messages between mail servers. The retention strategy will define the
1928 period of time the data will be retained, its storage method (e.g., online vs. offline), and how it will be
1929 safely and securely disposed of when it is no longer needed.

1930
1931 **4.2.8   Producing and Publishing Indicators**

1932 An organization's information technology systems produce numerous observables; these observables
1933 include indicators such as: malicious email messages; IP address, domain, and URL watch lists; and file
1934 hash codes. Security software often generates observables in the form of log files. For example, NIST SP
1935 800-92 "Guide to Computer Security Log Management" describes logs for intrusion detection and
1936 prevention systems, remote access software, web proxies, vulnerability management software,
1937 authentication servers, routers, and firewalls, as well as the use of non-security-specific log collection
1938 mechanisms, such as syslog, among others.

1939
1940 Indicators can be produced organically, thorough local data collection and analysis activities, or through
1941 maturation or enrichment of indicators received from sharing community partners. There are three basic
1942 types of indicators: atomic, computed, and behavioral.[34] Atomic indicators are simple data elements that
1943 cannot be further decomposed (e.g., IP address). Computed indicators are derived from other incident data
1944 (e.g., hash value). Behavioral are composite indicators, consisting of atomic and computed indicators
1945 joined through combinatorial logic and perhaps enhanced through the inclusion of contextual information.
1946 Organizations with basic network monitoring capabilities should be able to produce atomic indicators and
1947 perhaps simple computed indicators from existing data sources. The generation of sophisticated computed

---

[34] Amin, R., Cloppert, M., Hutchins, E. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin

1948 indicators or behavioral indicators often require more advanced tools and analytical processes, and greater
1949 technical expertise.
1950
1951 When producing and publishing indicators, it is important to include metadata that provides context for
1952 the indicator, describing how it is to be used and interpreted, how it was observed, how it relates to other
1953 indicators. Metadata may also include handling instructions, sensitivity designations, and provenance
1954 information (e.g., what tool was used to acquire the data, how the data was processed, who collected the
1955 data). Publishers of indicators should also consider assigning a confidence level to the information that it
1956 intends to share. The confidence level represents the degree of certainty that the publisher asserts for a
1957 specific data element, relationship, or data set. Users of the information may take this confidence level
1958 into consideration when using this information as basis for decisions. As indicators are created,
1959 aggregated, or enriched their sensitivity and classification should be reevaluated; in some cases it may be
1960 necessary to sanitize the data or place restrictions on its use or dissemination.
1961
1962 While there is a need to provide information to sharing partners in a timely manner, it is equally important
1963 to ensure that any content that is published is known to be of good quality prior to publication; inaccurate
1964 or imprecise indicators may result in high false positives/negatives rates, disrupting response activities
1965 and adversely affecting an organization's reputation within a sharing community. Incident data that is
1966 shared should be managed through a version control system, whereby new or updated content receives a
1967 unique release number that allows it to be efficiently identified and retrieved. Incident data often has a
1968 "shelf-life" that consists of the period of time from the initial creation of the data and when it is no longer
1969 considered useful or relevant. Organizations that publish incident data should implement data aging
1970 procedures and algorithms that ensure that the published data is topical, timely, and accurate.
1971
1972 At times some information may be shared with a community that turns out, on closer investigation, to be
1973 incorrect, perhaps due to a cut-and-paste error, or typo, or some information that is sensitive may be
1974 inadvertently shared. Therefore, some mechanism for retracting submissions should be included in the
1975 community knowledgebase. These can be simply a communication to the administrator for manual
1976 removal or perhaps a programmed feature. Automated submission mechanisms require hardening to
1977 ensure that the feature does not become an attack vector for the adversary that allows them to mask their
1978 presence by modifying or deleting information. Organizations that share indicators should provide a
1979 feedback mechanism that allows sharing partners to submit error reports; suggested improvements; or
1980 additional information about the indicators. This feedback plays in an important role in the enrichment,
1981 maturation, and quality of the indicators that are shared within a community.
1982
1983 Some information shared with a community may be marked as "currently under investigation" and
1984 requires that members not share beyond the collective, and do no active investigation (such as collecting
1985 malware samples from a suspect website, or even performing a DNS lookup on a suspect host-name) that
1986 might tip-off a potential adversary or otherwise compromise the investigative activities. At some point,
1987 such information may be downgraded, once an investigation is concluded, so it is useful to have some
1988 mechanism to change the marking or add a revised marking such as "downgraded to GREEN as of
1989 12/20/2015."
1990 The use of standard data formats for the exchange of incident data enables greater interoperability and
1991 speed when communicating with sharing partners. Information is commonly exchanged in unstructured
1992 formats (e.g., text documents, email) that require manual processing and interpretation. The use of
1993 structured data supports the exchange of data with minimal or no human intervention (i.e., automated or
1994 "machine-to-machine"). When evaluating standard data format, look to formats that are lightweight and
1995 easy to implement; formats that are very feature-rich can also be exceedingly complex and difficult to use
1996 in practice. Choose formats that are widely adopted, readily extensible (i.e., new data elements or features

1997 can be incorporated with minimal engineering and design effort), scalable, and provide the requisite
1998 security features to protect the data.
1999

4.2.9 Producing and Publishing Incident Reports

2001 Once an incident has been resolved, a final report should be produced that provides a summary of the
2002 incident, the ensuing investigation, the findings, and recommended improvements.[35] Incident reports help
2003 ensure that key decision makers are apprised of the incident and have the information necessary to make
2004 important operational decisions (i.e., those impacting the fundamental interests of the organization).
2005 Organizations should sanitize incident reports shared with an external partner by removing sensitive
2006 information or incident details that are not relevant to an external entity.
2007

4.3 Maintaining the Sharing Relationship

2009 Once sharing relationships are established, continued participation in the sharing community is essential
2010 for fostering stronger ties to other members and for the continuous improvement of incident response
2011 practices. Participating in community conference calls and face-to-face meetings increases an
2012 organizations ability to establish and cultivate trust with other members – a trust that may be a catalyst for
2013 a more free and open exchange of information, broader participation, and increased collaboration over
2014 time. Community-sponsored training events provide opportunities for less mature organizations to gain
2015 practical insights from seasoned incident response practitioners.

2016 Organizations are encouraged to conduct after-action (i.e., hotwash) discussions and evaluations after an
2017 incident. In particular, it is helpful for an organization to review the value of external information sharing
2018 and collaboration efforts, identify opportunities for improvement (e.g., address data quality or latency
2019 issues), and draw attention to tools, techniques, or internal or external information or threat intelligence
2020 sources that can be used to counter similar threats in the future. The amount of post-incident analysis
2021 needed may vary based on the size, complexity, and impact of the incident. Shortly after an incident, the
2022 participants in an incident should meet to discuss the following types of questions:

2023 • Did the organization gain any important threat intelligence and indicators (from external
2024   organizations) that assisted with the subsequent detection of the IT security incident?

2025 • Did threat intelligence and coordination information from the external organization provide any
2026   countermeasures that the organization used to minimize the damage of the incident?

2027 • Did threat intelligence received from the external organization result in the detection of false
2028   positives?

2029 • Were the countermeasures employed effective?

2030 • Were the countermeasures cost effective?

2031 • If the organization shared internal incident information with external information sharing
2032   communities, was that information useful to the community?

2033 • Did the organization sanitize the information that it provided to the external communities? Was the
2034   level of redaction performed appropriate? Was enough information released to be useful? Were
2035   organizational, legal, contractual, and ethical obligations regarding sharing met?

---

[35] Appendix B-Incident-Related Data Elements, of NISP SP 800-61 provides suggestions of what information to collect for incidents.

2036   •   If an incident caused damage internal to the organization, was that information shared with the
2037   external communities? If not, why not? How did the organization decide what damage information
2038   to share or not share?

2039   •   If the organization lacked threat intelligence and countermeasure information during the incident, are
2040   there external information sharing and collaboration communities that could have provided the
2041   information?

2042   •   Did the organization share technical information collected internally? If so, how much effort was
2043   expended to sanitizing the information?

2044 The hotwash findings can be used by the organization to improve security measures, update policies and
2045 procedures, identify training needs, and to improve the organizational incident handling processes. An
2046 organization may also choose to selectively share relevant hotwash findings with their sharing
2047 communities to help improve the overall effectiveness of the community's incident response practices.

2048 The ongoing maintenance of a sharing relationship requires that an organization's information sharing
2049 rules be reevaluated on a regular basis. Some of the events that can trigger the need to reexamine
2050 information sharing rules or practices include:

2051   •   Changes to regulatory or legal requirements

2052   •   Updates to organizational policy

2053   •   Introduction of new information sources

2054   •   Risk tolerance changes

2055   •   Information ownership

2056   •   Operating/threat environment

2057   •   Organizational mergers and acquisitions

2058   4.4   Recommendations

2059 The key recommendations presented in this section are summarized below:
2060

2061   •   Define the overall goals, objectives, and scope of the information sharing initiative

2062   •   Obtain formal approval from the management, privacy officials, and legal teams and the support of
2063   key organizational stakeholders before sharing information

2064   •   Perform an information inventory that identifies the primary types of information that an organization
2065   currently possesses, the information owner, the sensitivity of the information, the protection
2066   requirements for the information, and the location of the information

2067   •   Enumerate risks of sharing incident and threat-intelligence data and identify appropriate mitigation
2068   strategies for each phase of the information life cycle

2069   •   Develop a process for reviewing and protecting data types and content that is likely to contain
2070   sensitive information

- Document the circumstances and rules under which information sharing is permitted by evaluating the risks of disclosure, the urgency of sharing, the trustworthiness of the information sharing community, and the methods used by the community to safeguard shared information

- Develop a list of data types and content, such as adversary indicators, that can be shared quickly with relatively minor review

- Identify peers and other organizations with whom coordination and information sharing relationships would be beneficial

- Ensure that the resources required for ongoing participation in a sharing community are available (e.g., personnel, training, hardware, software, and other infrastructure needed to support ongoing data collection, storage, analysis, and dissemination)

- Establish points of contact and engage in on-going participation with the sharing community through established communication channels

- Procedures for markup and data handling should be documented and approved by management.

- Mark, store and track information regarding the sensitivity of data to be shared.

- Protect sensitive information through the implementation of security controls, access control measures, and through the enforcement of an organization's information sharing rules

- Provide role-specific training to personnel so they understand how to handle incident and threat intelligence data appropriately

- Store and protect evidence that may be needed in the future; to help diagnose a future attack, or perhaps to support legal proceedings

- Implement the organizational processes, procedures, and infrastructure necessary to consume, protect, and respond to alerts and incident reports received from external sources

- Prepare for incident and threat-intelligence activities as much as possible in advance of needing to share in response to an actual incident.

- Implement the organizational processes, procedures, and infrastructure necessary to consume and analyze indicators received from external sources

- Document and use standard data formats and protocols to facilitate the efficient capture and exchange of information

- Produce and maintain written records throughout the incident response lifecycle, allowing the organization to later reconstruct the timeline and narrative of the response activity

- Produce and publish indicators based on local data collection and analysis activities, or through maturation or enrichment of indicators received from sharing community partners

- Produce and publish incident reports to provide initial notification of an incident, interim progress reporting during an incident, and a final report after the incident has been resolved

- Track sources of data and with whom that data has been shared

2107 **5.   General Recommendations**

2108 The general recommendations presented in this document are summarized below:
2109

2110 • Establish and actively participate in information sharing relationships as part of a proactive, ongoing
2111   cyber incident response capability

2112 • Exchange threat information, tools, and techniques with sharing partners – in doing so, an
2113   organization benefits from the collective resources and knowledge of its sharing peers and is able to
2114   better defend its networks and share costs

2115 • Increase the organization's cybersecurity posture and maturity by enhancing or augmenting local data
2116   collection, analysis, and management functions. By implementing such capabilities, an organization
2117   gains a more complete understanding of its systems and networks, and is able to use a broader and
2118   richer set of information available through external sharing partners

2119 • Use a cyber attack life cycle, such as the Lockheed Martin kill chain to define a framework for active
2120   defense that makes effective use of information available through both internal and external sources

2121 • Share information about both attempted and successful intrusions. Often, information related to
2122   attempted intrusions is less sensitive and requires minimal sanitization and analysis; therefore it can
2123   be shared more quickly

2124 • Carefully evaluate potential sharing communities/partners and select an information sharing model
2125   and community that is best suited for an organization or industry sector

2126 • An organization should perform a self-assessment to determine if they have the capabilities to
2127   effectively engage in an information sharing community

2128 • Ensure that a basic, foundational computer network defensive capability is in place before engaging
2129   in information sharing and coordination activities

2130 • As a new entrant in an information sharing community, use information from external sources to
2131   enhance existing internal incident response capabilities

2132 • Mature organizations should expand internal data collection operations, perform analysis, and begin
2133   to develop and publish indicators and actionable threat intelligence

2134 • An organization may need to consider outsourcing incident response functions in cases where the
2135   personnel and skills necessary to perform a task are not readily available within the organization, or in
2136   cases where developing or maintaining a specific security capability in-house is not financial
2137   advantageous

2138 • Before implementing an information sharing program, define its overall goals, objectives, and scope;
2139   obtain formal approval from the management, privacy, and legal teams; and acquire the support of
2140   key organizational stakeholders

2141 • Perform an information inventory that identifies the types of information that the organization
2142   currently possesses, the information owner, the sensitivity of the information, the protection
2143   requirements for the information, and the location of the information

2144 • Document the circumstances and rules under which information sharing is permitted by evaluating
2145 the risks of disclosure, the urgency of sharing, the trustworthiness of the information sharing
2146 community, and the methods used by the community to safeguard shared information

2147 • Identify peers and other organizations with whom coordination and information sharing relationships
2148 would be beneficial

2149 • Ensure that the resources required for ongoing participation in a sharing community are available
2150 (e.g., personnel, training, hardware, software, and other infrastructure needed to support ongoing data
2151 collection, storage, analysis, and dissemination)

2152 • Establish points of contact and engage in on-going participation with the sharing community through
2153 established communication channels

2154 • Protect sensitive information through the implementation of security controls, access control
2155 measures, and through the enforcement of the organization's information sharing rules

2156 • Store and protect evidence that may be needed in the future; to help diagnose a future attack, or
2157 perhaps to support legal proceedings or disciplinary actions

2158 • Implement the organizational processes, procedures, and infrastructure necessary to consume, protect,
2159 analyze, and respond to indicators, alerts, and incident reports received from external sources

2160 • Produce and maintain written records throughout the incident response lifecycle, allowing the
2161 organization to later reconstruct the timeline and narrative of the response activity

2162 • Produce and publish indicators based on local data collection and analysis activities, or through
2163 maturation or enrichment of indicators received from sharing community partners

2164 • Produce and publish incident reports to provide initial notification of an incident, interim progress
2165 reporting during an incident, and a final report after the incident has been resolved

2166 • Enumerate risks of sharing incident and threat-intelligence data and identify appropriate mitigation
2167 strategies for each phase of the information life cycle

2168 • To the extent possible, prepare for incident and threat-intelligence sharing activities in advance of an
2169 actual incident

2170 • Develop a list of data types and content that can be shared quickly with minimal review

2171 • Develop a process for reviewing and protecting data types and content that is likely to contain
2172 sensitive information.

2173 • Employ standard data formats and transport protocols to facilitate the efficient and effective exchange
2174 of information.

2175 • Mark, store and track information regarding the sensitivity of data to be shared.

2176 • Provide role-specific training to personnel so they understand how to handle incident and threat
2177 intelligence data appropriately.

2178

2179 ## Appendix A—Incident Coordination Scenarios

2180 The scenarios presented in this appendix introduce real-world applications of threat intelligence sharing
2181 and coordinated incident response. These scenarios are meant to provide insights into how sharing and
2182 coordination can increase the efficiency and effectiveness of an organization's incident response
2183 capabilities. These scenarios seek to demonstrate that by leveraging the knowledge, experience, and
2184 capabilities of their partners, an organization is able to enhance its cybersecurity posture. These scenarios
2185 represent only a small number of possible applications of sharing and collaboration. The dynamic nature
2186 of the threat landscape means that as the tactics, techniques, and procedures of the adversary change
2187 organizations must adapt their protection, detection, and response strategies.

2188 ### Scenario 1: Nation State Malware Attacks Against a Specific Industry Sector
2189

2190 A nation-state regularly targets companies in a certain industry sector for several months. The attacks
2191 come in the form of targeted emails that carry weaponized attachments containing a software exploit that,
2192 upon opening, launches malware on the victim's system. Once compromised, these systems contact
2193 servers controlled by the adversary to receive further instructions and to exfiltrate data.

2194 The individual companies form a formal threat-sharing collective, where they establish a central forum to
2195 post information about different attacks. The posts describe details relevant to detecting and defending
2196 against the threat, such as the sender addresses of phishing emails, samples of malware collected from the
2197 attacks, analysis of exploit code used by the attackers, and IPs and URLs involved with the attacks.

2198 As soon as one company's security team identifies a new attack, they quickly share the information with
2199 their peers. One company has advanced malware analysis capabilities and is able to extract additional
2200 information about the adversary and the infrastructure used for command and control from a malware
2201 sample collected by another company, and shared via the forum. By sharing the malware sample, the
2202 community is able to benefit from the malware analysis capabilities of one of its peers and to quickly and
2203 efficiently detect attacks that individually they likely would not have been able to find until well after the
2204 adversaries had penetrated their enterprises. In this scenario, an attack faced by one company becomes
2205 another's defense.

2206 ### Scenario 2: Campaign Analysis
2207

2208 Cybersecurity analysts from companies in a business sector have been sharing indicators and malware
2209 samples in an online forum over the past few years. Each company performs independent analysis of the
2210 attacks and observes consistent patterns over time, with groups of events often having a number of
2211 commonalities, such as the type of malware used, the domains of command and control channels, and
2212 other technical indicators. These observations lead the analysts to suspect that the attacks are not fully
2213 random.

2214 The forum members hold a technical exchange meeting to share data, insights, and analyses of the
2215 different attacks. What emerges from the combined data sets and joint analyses is the identification of
2216 several distinct sets of activities that are likely attributable to common adversaries or attacker groups,
2217 each with their own TTPs, target sets, and time table.

2218 This scenario demonstrates how a broader set of data helps reveal collective action and campaigns by an
2219 adversary and the TTPs used by specific adversaries or campaigns.

2220 ### Scenario 3: Distributed Denial of Service Attack Against Industry Sector
2221

2222   A hacktivist group targets a select set of companies for a large-scale distributed denial of service (DDoS)
2223   attack. The group employs a distributed botnet, loosely coordinated and controlled by members of the
2224   group. By analyzing the traffic generated by the botnet, one company is able to determine that the
2225   attackers are using a variant of a popular DDoS tool.

2226   The targeted companies are members of an ISAC. Using the ISAC's discussion portal, the companies
2227   establish a working group to coordinate their efforts to end the attacks. The working group contacts the
2228   ISAC's law enforcement liaison, who coordinates with federal and international authorities to aid in the
2229   investigation and gain court orders to shut down attacker systems.

2230   The working group contacts various ISPs, and provides information to aid in identifying abnormal traffic
2231   to their network addresses. The ISPs identify the source networks for the bulk of the traffic and are able to
2232   place rate limits on these sources, mitigating the attack. Using network traffic collected by the ISPs,
2233   international law enforcement agencies are able to identify the command and control servers, seize these
2234   assets, and identify some members of the hacktivist group.

2235   After a technical exchange meeting among the targeted companies, several companies decide to enlist the
2236   aid of content distribution providers, to distribute their web-presence and make their business systems
2237   more resilient to future DDoS attacks.

2238   **Scenario 4: Financial Conference Phishing Attack**
2239
2240   A cyber crime group made use of a popular business practices conference's attendee list to select targets
2241   for a wave of phishing emails. The group was able to identify multiple members of the business offices
2242   and, in some circumstances, compromise those machines and authorize electronic payments to overseas
2243   businesses.

2244   One company identifies the attack against their business office employees and during their investigation
2245   realizes that the recipients of the attack email had all attended the same conference six months earlier. The
2246   company's CIRT contacts the conference organizers, as well as representatives from other organizations
2247   that attended the conference. A conference call is arranged to share information about the attack.
2248   Separately, two other businesses stop the attack, but are unable to identify the source. Three other
2249   businesses check their mail and network traffic logs and are able to identify potentially compromised
2250   hosts using the shared indicators.

2251   The companies agree to share information about future attacks via an informal email list.

2252   **Scenario 5: Business Partner Compromise**
2253
2254   "Company A" and "Company B" are business partners that have established network links between the
2255   organizations to facilitate the exchange of business information. A cyber crime organization compromises
2256   a server at Company B and uses their access as a stepping-stone to launch attacks against internal servers
2257   at Company A. A system administrator Company A notices the unusual activity and notifies their security
2258   team, who identifies the source of the activity as coming from a Company B system.

2259   Company A's security team, who had previously engaged in a joint incident response exercise with
2260   Company B, contacts Company B's incident response team and describes the activity they are seeing.
2261   Company B's team is able to isolate the compromised server and perform an investigation to identify the
2262   source of the breach and other possible compromises.

2263 The initial attackers had identified a weakness in a web-facing application and used it to take control of
2264 the server. Company B developers quickly fix the code to close the security hole and also enable
2265 additional logging and intrusion detection signatures to be ready for future attacks.

2266 Company B's security team also determines that some customer personal information was potentially
2267 exposed to the attackers, so those customers are contacted and informed of the event, and instructed to
2268 change their passwords.

2269 Because the security teams of the two companies had participated in a joint exercise, they had established
2270 contacts, built trust relationships, understood each other's networks and operations, and were able to
2271 quickly resolve the issue and prevent further damage from occurring.

Scenario 6: US-CERT Provides Indicators, Receives Feedback

2272
2273
2274 The US-CERT receives information from a variety of sources that a number of servers located in the U.S.
2275 are being used to carry out cyber attacks against other U.S. firms. A specific foreign actor controls the
2276 compromised servers. The US-CERT identifies the firms under attack and notes that they are
2277 predominantly in the aviation industry. The US-CERT contacts the security teams of these firms and
2278 shares initial information about the attacks, including URLs, malware, and the kinds of vulnerabilities
2279 being exploited.

2280 A number of the U.S. firms are able to identify and remediate attacks. These firms, during the course of
2281 their investigation, are also able to identify new indicators associated with the attackers that the US-CERT
2282 was unaware of. The US-CERT is able to share these new indicators with the rest of the firms,
2283 anonymizing the sources, leading to a more comprehensive response to the threat.

Scenario 7: A Retailer Fails to Share

2285 A large retailer is subject to a cyber attack by a criminal organization. Millions of credit card numbers and
2286 account information of users are stolen during a breach that goes undiscovered for several weeks. The
2287 retailer does not participate in sharing threat information, so the organization relies on its own security
2288 and detection capabilities. Their internal capabilities prove inadequate in the face of a sophisticated,
2289 targeted threat that uses custom malware.

2290 The breach is discovered by credit card companies investigating a rash of credit card fraud. The
2291 commonality in the credit card fraud was purchases made from this one retailer. The credit card
2292 companies notify law enforcement as well as the retailer, who begin an investigation.

2293 The damages are enormous. The company notifies their customers of the theft of personal information,
2294 but does not release details of how the attack was carried out. Consequently several other retailers are
2295 successfully attacked by the same methods in the weeks following the initial breach. The financial losses
2296 realized by the retailers, customer, and credit card issuers could have been avoided, at least in part, had
2297 these companies engaged in active sharing of threat information

2298 ## Appendix B—Glossary

2299 Selected terms used in the publication are defined below.

2300 **Alert:** Timely information about current security issues, vulnerabilities, and exploits. [SOURCE: US-
2301 CERT]

2302 **Computer Security Incident:** See "Incident".

2303 **Computer Security Incident Response Team (CSIRT):** A capability set up for the purpose of assisting
2304 in responding to computer security-related incidents; also called a Computer Incident Response Team
2305 (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

2306 **Cyber Threat Information:** Information (e.g., indications, tactics, techniques, procedures, behaviors,
2307 motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, their
2308 intentions, or actions against information technology or operational technology systems.

2309 **Event:** Any observable occurrence in a network or system.

2310 **False Negative:** An instance in which a security tool intended to detect a particular threat fails to do so.

2311 **False Positive**: An instance in which a security tool incorrectly classifies benign content as malicious.

2312 **Incident:** A violation or imminent threat of violation of computer security policies, acceptable use
2313 policies, or standard security practices.

2314 **Incident Handling:** The mitigation of violations of security policies and recommended practices.

2315 **Incident Report:** A written summary of an incident that describes the steps in the investigation of the
2316 event, the findings, and the resolution.

2317 **Incident Response:** See "Incident Handling".

2318 **Indicator:** An artifact or observable that suggests that an adversary is preparing to attack, that an attack
2319 is currently underway, or that a compromise may have already occurred.

2320 **Information Life Cycle:** The stages through which information passes, typically characterized as
2321 creation or collections, processing, dissemination, use, storage, and disposition. [SOURCE: OMB Circular
2322 A-130]

2323 **Information Sharing and Analysis Organization (ISAO):** An ISAO is any formal or information
2324 entity of collaboration created or employed by public or private sector organizations, for the purpose of—
2325 (A) gathering and analyzing critical infrastructure information in order to better understand security
2326 problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the
2327 availability, integrity, and reliability thereof; (B) communicating or disclosing critical infrastructure
2328 information to help prevent, detect, mitigate or recover from the effects of an interference, compromise,
2329 or incapacitation problem related to critical infrastructure of protected systems; and (C) voluntarily
2330 disseminating critical infrastructure information to its members, State, local, and Federal Governments, or
2331 any other entities that may be of assistance in carrying out the purposed specified in sub-paragraphs (A)
2332 and (B).

2333   **Malware:** A program that is covertly inserted into another program with the intent to destroy data, run
2334   destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of
2335   the victim's data, applications, or operating system. [SOURCE: NIST SP 800-83, Revision 1]

2336   **Precursor:** A sign that an attacker may be preparing to cause an incident.

2337   **Profiling:** Measuring the characteristics of expected activity so that changes to it can be more easily
2338   identified.

2339   **Signature:** A recognizable, distinguishing pattern associated with an attack, such as a binary string in a
2340   virus or a particular set of keystrokes used to gain unauthorized access to a system.

2341   **Social Engineering:** An attempt to trick someone into revealing information (e.g., a password) that can
2342   be used to attack systems or networks.

2343   **Threat:** Any circumstance or event with the potential to adversely impact organizational operations
2344   (including mission, functions, image, or reputation), organizational assets, individuals, other
2345   organizations, or the Nation through an information system via unauthorized access, destruction,
2346   disclosure, or modification of information, and/or denial of service. [SOURCE: NIST SP 800-30, Revision
2347   1]

2348   **Threat Source:** The intent and method targeted at the intentional exploitation of a vulnerability or a
2349   situation and method that may accidentally exploit a vulnerability. [SOURCE: NIST SP 800-30, Revision 1
2350   and CNSSI No. 4009]

2351   **Vulnerability:** A weakness in an information system, system security procedures, internal controls, or
2352   implementation that could be exploited by a threat source. [SOURCE: NIST SP 800-30, Revision 1]

2353

2354

2355 **Appendix C—Acronyms**

2356 Selected acronyms used in the publication are defined below.

2357	**ACSC**	Advanced Cyber Security Center
2358	**AI**	Asset Identification
2359	**AMC**	Army Materiel Command
2360	**APWG**	Anti-Phishing Working Group
2361	**ARF**	Asset Reporting Format
2362	**ASLR**	Address Space Layout Randomization
2363	**CAPEC**	Common Attack Pattern Enumeration and Classification
2364	**CCE**	Common Configuration Enumeration
2365	**CCIPS**	Computer Crime and Intellectual Property Section
2366	**CEE**	Common Event Expression
2367	**CERT®/CC**	CERT® Coordination Center
2368	**CFM**	Cyber Fed Model
2369	**CIO**	Chief Information Officer
2370	**CIRC**	Computer Incident Response Capability (Center)
2371	**CIRT**	Computer Incident Response Team
2372	**CISO**	Chief Information Security Officer
2373	**CPE**	Common Platform Enumeration
2374	**CSD**	Computer Security Division
2375	**CSIRC**	Computer Security Incident Response Capability
2376	**CSIRT**	Computer Security Incident Response Team
2377	**CSOC**	Cyber Security Operations Center
2378	**CVE**	Common Vulnerabilities and Exposures
2379	**CVSS**	Common Vulnerability Scoring System
2380	**CWE**	Common Weakness Enumeration
2381	**CybOX**	Cyber Observable Expression
2382	**DDoS**	Distributed Denial of Service
2383	**DEP**	Data Execution Prevention
2384	**DFIR**	Digital Forensics for Incident Response
2385	**DHS**	Department of Homeland Security
2386	**DIB**	Defense Industrial Base
2387	**DLP**	Data Loss Prevention
2388	**DNS**	Domain Name System
2389	**DOD**	Department of Defense
2390	**DOE**	Department of Energy
2391	**DoS**	Denial of Service
2392	**ENISA**	European Network and Information Security Agency
2393	**ES-ISAC**	Electrical Sector Information Sharing and Analysis Center
2394	**FIRST**	Forum of Incident Response and Security Teams
2395	**FISMA**	Federal Information Security Management Act
2396	**GAO**	General Accountability Office
2397	**GFIRST**	Government Forum of Incident Response and Security Teams
2398	**GLBA**	Gramm-Leach-Bliley Act
2399	**HIPAA**	Health Information Portability and Accountability Act
2400	**HTCIA**	High Technology Crime Investigation Association
2401	**HTTP**	HyperText Transfer Protocol
2402	**IC**	Intelligence Community
2403	**ICE**	Immigration and Customs Enforcement

2404	**ICS-CERT**	Industrial Control Systems Cyber Emergency Response Team
2405	**IDMEF**	Intrusion Detection Message Exchange Format
2406	**IDPS**	Intrusion Detection and Prevention System
2407	**IDS**	Intrusion Detection System
2408	**IETF**	Internet Engineering Task Force
2409	**IODEF**	Incident Object Description Exchange Format
2410	**IR**	Interagency Report
2411	**IRC**	Internet Relay Chat
2412	**ISAC**	Information Sharing and Analysis Center
2413	**ISAO**	Information Sharing and Analysis Organization
2414	**ISC**	Internet Storm Center
2415	**ISP**	Internet Service Provider
2416	**IT**	Information Technology
2417	**ITL**	Information Technology Laboratory
2418	**MAEC**	Malware Attribute Enumeration and Characterization
2419	**MOU**	Memorandum of Understanding
2420	**MSSP**	Managed Security Services Provider
2421	**NASA**	National Aeronautics and Space Administration
2422	**NCCIC**	National Cybersecurity and Communications Integration Center
2423	**NDA**	Non-Disclosure Agreement
2424	**NERC**	North American Electric Reliability Corporation
2425	**NIST**	National Institute of Standards and Technology
2426	**NTP**	Network Time Protocol
2427	**OCIL**	Open Checklist Interactive Language
2428	**OMB**	Office of Management and Budget
2429	**OpenIOC**	Open Indicators of Compromise
2430	**OVAL**	Open Vulnerability and Assessment Language
2431	**PCI DSS**	Payment Card Industry Data Security Standard
2432	**PHI**	Protected Health Information
2433	**PII**	Personally Identifiable Information
2434	**PKI**	Public Key Infrastructure
2435	**POC**	Point of Contact
2436	**RCERT**	Regional Computer Emergency Response Team
2437	**RFC**	Request for Comment
2438	**RID**	Real-time Inter-network Defense
2439	**SCAP**	Security Content Automation Protocol
2440	**SOX**	Sarbanes-Oxley Act
2441	**SIEM**	Security Information and Event Management
2442	**SLA**	Service Level Agreement
2443	**SMTP**	Simple Mail Transfer Protocol
2444	**SOP**	Standard Operating Procedure
2445	**SP**	Special Publication
2446	**STIX**	Structured Threat Information Expression
2447	**TAXII**	Trusted Automated Exchange of Indicator Information
2448	**TLP**	Traffic Light Protocol
2449	**TLS**	Transport Layer Security
2450	**TSA**	Transportation Security Administration
2451	**TTP**	Tactics, Techniques, and Procedures
2452	**URL**	Uniform Resource Locator
2453	**US-CERT**	United States Computer Emergency Readiness Team
2454	**USACE**	United States Army Corps of Engineers

2455   **USCYBERCOM**   United States Cyber Command
2456   **VERIS**   Vocabulary for Event Recording and Incident Sharing
2457   **XCCDF**   Extensible Configuration Checklist Description Format
2458

2459

Appendix D—Resources

2461 The lists below provide examples of resources that may be helpful in establishing and maintaining an
2462 incident response capability.

2463 **Incident Response Organizations**

Organization	URL
Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice	http://www.cybercrime.gov/
CERT® Coordination Center, Carnegie Mellon University (CERT®/CC)	http://www.cert.org/
Cyber Fed Model (CFM)	http://web.anl.gov/it/cfm/index.html
European Network and Information Security Agency (ENISA)	http://www.enisa.europa.eu/activities/cert
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/
Government Forum of Incident Response and Security Teams (GFIRST)	http://www.us-cert.gov/federal/gfirst.html
High Technology Crime Investigation Association (HTCIA)	http://www.htcia.org/
InfraGard	http://www.infragard.net/
Internet Storm Center (ISC)	http://isc.sans.edu/
National Council of ISACs	http://www.isaccouncil.org/
United States Computer Emergency Readiness Team (US-CERT)	http://www.us-cert.gov/
Defense Industrial Base (DIB) Cyber Security / Information Assurance (IA) Program	http://dibnet.dod.mil
Advanced Cyber Security Center (ACSC)	http://www.acscenter.org

2464

2465 **NIST Publications**

Resource Name	URL
NIST SP 800-30, *Guide for Conducting Risk Assessments*	http://csrc.nist.gov/publications/PubsSPs.html#800-30
NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*	http://csrc.nist.gov/publications/PubsSPs.html#800-34
NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*	http://csrc.nist.gov/publications/PubsSPs.html#800-37
NIST SP 800-39 Revision 1, *Managing Information Security Risk; Organization, Mission, and Information System View*	http://csrc.nist.gov/publications/PubsSPs.html#800-39
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	http://csrc.nist.gov/publications/PubsSPs.html#800-53
NIST SP 800-61 Revision 2, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/PubsSPs.html#800-61
NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*	http://csrc.nist.gov/publications/PubsSPs.html#800-83
NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*	http://csrc.nist.gov/publications/PubsSPs.html#800-84

Resource Name	URL
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	http://csrc.nist.gov/publications/PubsSPs.html#800-86
NIST SP 800-88 DRAFT, *Guidelines for Media Sanitization*	http://csrc.nist.gov/publications/PubsSPs.html#800-88
NIST SP 800-92, *Guide to Computer Security Log Management*	http://csrc.nist.gov/publications/PubsSPs.html#800-92
NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*	http://csrc.nist.gov/publications/PubsSPs.html#800-94
NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*	http://csrc.nist.gov/publications/PubsSPs.html#800-115
NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*	http://csrc.nist.gov/publications/PubsSPs.html#800-122
NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*	http://csrc.nist.gov/publications/PubsSPs.html#800-128
NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*	http://csrc.nist.gov/publications/PubsSPs.html#800-137

2466

Other Publications

2467

Resource Name	URL
6 U.S.C., Sec. 131, Definitions	http://www.gpo.gov/fdsys/granule/USCODE-2010-title6/USCODE-2010-title6-chap1-subchapII-partB-sec131/content-detail.html

2468

Data Exchange Specifications Applicable to Incident Handling

2469

Title	Description	Additional Information
AI	Asset Identification	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7693
ARF	Asset Reporting Format	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7694
CAPEC	Common Attack Pattern Enumeration and Classification	http://capec.mitre.org/
CCE	Common Configuration Enumeration	http://cce.mitre.org/
CEE	Common Event Expression	http://cee.mitre.org/
CPE	Common Platform Enumeration	http://cpe.mitre.org/
CVE	Common Vulnerabilities and Exposures	http://cve.mitre.org/
CVSS	Common Vulnerability Scoring System	http://www.first.org/cvss/cvss-guide
CWE	Common Weakness Enumeration	http://cwe.mitre.org/
CybOX	Cyber Observable eXpression	http://cybox.mitre.org/
MAEC	Malware Attribute Enumeration and Characterization	http://maec.mitre.org/
MARF	Message Abuse Reporting Format	http://datatracker.ietf.org/wg/marf/documents/
MMDEF	Malware Metadata Exchange Format	http://standards.ieee.org/develop/indconn/icsg/mmdef.html
OCIL	Open Checklist Interactive Language	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-

Title	Description	Additional Information
		IR-7692
OpenIOC	Open Indicators of Compromise	http://www.openioc.org/
OVAL	Open Vulnerability Assessment Language	http://oval.mitre.org/
RFC 4765	Intrusion Detection Message Exchange Format (IDMEF)	http://www.ietf.org/rfc/rfc4765.txt
RFC 5070	Incident Object Description Exchange Format (IODEF)	http://www.ietf.org/rfc/rfc5070.txt
RFC 5901	Extensions to the IODEF for Reporting Phishing	http://www.ietf.org/rfc/rfc5901.txt
RFC 5941	Sharing Transaction Fraud Data	http://www.ietf.org/rfc/rfc5941.txt
RFC 6545	Real-time Inter-network Defense (RID)	http://www.ietf.org/rfc/rfc6545.txt
RFC 6546	Transport of Real-time Inter-network Defense (RID) Messages over HTTP/TLS	http://www.ietf.org/rfc/rfc6546.txt
SCAP	Security Content Automation Protocol	http://csrc.nist.gov/publications/PubsSPs.html #SP-800-126-Rev.%202
STIX	Structured Threat Information Expression	http://stix.mitre.org/
TAXII	Trusted Automated Exchange of Indicator Information	http://taxii.mitre.org/
VERIS	Vocabulary for Event Recording and Incident Sharing	http://www.veriscommunity.net/
x-arf	Network Abuse Reporting	http://www.x-arf.org/
XCCDF	Extensible Configuration Checklist Description Format	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7275-r4

2470

Appendix E—Change Log