SECTION 4

The Security Incident Response Team Members

The knowledge and skill of the incident responder is paramount to the successful handling of any incident. The incident responder has to be able to demonstrate impartiality and to know the importance of identification, coupled with collecting and cataloging any evidentiary findings in context with surrounding factors.

- The incident responder needs to be *logical* in their approach to each and every situation. Each event and activity which is to be handled must be approached with an open mind and a sound methodology for investigation and containment.
- The incident responder has to be *thorough* in all actions that they take when responding, analyzing, evaluating and documenting the incident. The full scope of the incident must be accounted for during and after the actual handling activities occur so that nothing is missed and left to continue to create issues in the future.
- The incident responder is required to be as *objective* as possible during and after the response effort to ensure integrity and impartiality of their efforts. The actual data involved in the incident, along with the methods and techniques of exposure need to be identified, cataloged, and traced to ensure the full depth and breathe of the incident is investigated.
- The incident responder must be *observant* of all activities, events, and surrounding environment while responding to gather as much information about the situation as can be gleaned from the incident scene. All sources of data for the investigation must be included in the incident data collection efforts.
- *Resourcefulness* is the hallmark of an incident responder when checking, examining, and reviewing all of the parameters of any type of incident. Utilizing all possible sources of information about surrounding and concerning the hardware and software in relation to the data collected is needed to ensure the full scope of the investigation is covered.
- Above all other criteria, the incident responder must be *accurate* in his findings, results, and reports of the incident, the surroundings, and root cause for the incident. The final and ultimate criteria for the responder

Computer Incident Response and Forensics Team Management.
DOI: http://dx.doi.org/10.1016/B978-1-59749-996-5.00004-2

are the need for direct, distinct, and decisive in the examination and development of the results and report of the incident.

An incident responder's responsibilities before, during, and after the incident include the following:

1. Proper information gathering and collection techniques—techniques should be based on the best business practices as well as predefined corporate guidelines.
   The actual performance of data gathering, investigation, analysis, and examination needs to follow proper protocols and documented methods and techniques.
2. Proper documentation—full documentation should be developed as the incident transpires and is contained when possible and also includes the support manuals and vendor documentation. The one basic activity necessary during any event is to document everything that transpires during the event. All actions, activities, evaluations, supporting data collection, and any other relevant act must be fully documented by the responder during the response activity.
3. Proper performance—the obvious key to the whole process in containing and eradicating the incident root cause especially if the incident is caused by external factors. Complete and professional investigative and response performance is paramount for any incident responder.
4. Certification on response tools and techniques—industry certifications in Incident Handling go a long way to ensure the responders have the necessary background to properly respond no matter what the incident may be. Multiple professional certifications in incidence response, malware analysis, reverse engineering of software, penetration testing, and ethical hacking are all available and add to the expertise and standing of the assigned incident responders.
5. Proper methodologies—the proper way to handle an incident always depends on the type and timing of the incident. But, there are documented ways, such as found in Section 3.
6. Detailed, enhanced technical writing capabilities—I often talk about the first job of any security professional is to "secure the data" and the second job is to "report, report, and report." This area is critical to the successful improvement and enhancement of the organizational security posture after the incident is handled as well as the potential further investigative activities in the Forensics arena.

The selection criteria of the Security Incident Response Team (SIRT) members are usually based on two factors: who is available and what skills do they have? Additional factors can include the size and scope of the SIRT itself, what level of executive support is being provided to the SIRT, visibility of the SIRT

requirements and needs within the organization, and even possible recent events and incidents. The skills, abilities, and knowledge of the SIRT members are usually in two areas: technical and personal.

TYPES OF TECHNICAL SKILLS NEEDED

These skills, abilities, and knowledge are provided as a guide, not a full set of personnel requirements. Realistically, not many incident handlers will have all of these skills, but they should have a working knowledge of most of them.

- The basic security principles and engineering practices such as found in NIST SP 800-27 are as follows:
  - confidentiality
  - availability
  - authentication
  - integrity
  - access control
  - privacy
  - nonrepudiation.

  The SIRT member needs knowledge about basic security principles in order to understand potential problems that can arise if appropriate security measures have not been implemented correctly, as well as the potential impacts to the customer. SIRT members with this understanding are better prepared to determine their customer needs in securely configuring systems to prevent misuse or compromises and also be better prepared to provide appropriate technical assistance and guidance when breaches do occur.
- Ability to identify risks and threats to data, information, computers, and networks.

  The SIRT member needs to be able to recognize and categorize the most common types of system and network vulnerabilities and associated attacks, such as those that might involve:
  - malicious code (e.g., viruses, worms, Trojan horses),
  - protocol design flaws (e.g., man-in-the-middle attacks, spoofing),
  - implementation flaws (e.g., buffer overflow, timing windows/race conditions),
  - configuration weaknesses or incorrect settings,
  - user errors, omissions, or indifference,
  - physical security issues.
- Understanding the Internet (aspects ranging from architecture and history to future and philosophy)

  Each SIRT member should know about the history, philosophy, and structure of the Internet, and the various infrastructures that support it.

The SIRT member needs to know this information in order to understand why and the way that the various protocols are designed and work across the Internet.

- Detailed knowledge of network protocols (IP, ICMP, TCP, UDP, FTP)
  The SIRT member needs to have a basic understanding of the common network protocols that are used in their operating environment. For each protocol, he/she should have a basic understanding of the protocol, its specification, and how it is used. In addition, the SIRT member should understand the common types of threats or attacks against the protocol, as well as strategies to mitigate or eliminate such attacks.
- In-depth understanding of network infrastructure elements (router, DNS, mail-server)
  The SIRT member needs to have a basic understanding of the concepts of network security and be able to recognize vulnerable points in network configurations. The SIRT member should understand the concepts and basic perimeter security of network firewalls (design, packet filtering, proxy systems, DMZ, bastion hosts, etc.), router security, potential for information disclosure of data traveling across the network (e.g., packet monitoring or "sniffers"), or threats relating to accepting untrustworthy information.
- How network applications, services, and related protocols (SMTP, HTTP, HTTPS, FTP, TELNET, SSH, IMAP, POP3) function and interact with each other.
  The SIRT members need a basic understanding of the common network applications and services that the team and the customer use (DNS, NFS, SSH, HTTP, etc.). For each application or service, the SIRT member should understand the purpose of the application or service, how it works, common usage, secure configurations, and the common types of threats or attacks against the application or service, as well as mitigation strategies.
- Current security vulnerabilities/weaknesses and related attack methodologies (IP spoofing, Internet sniffers, denial of service attacks, and computer viruses)
  The SIRT members need to understand the different types of malicious code attacks (system compromises, denial of service, loss of data integrity, etc.) that occur and how these can affect their customers. Malicious code can have different types of payloads that can cause a denial of service attack or web defacement, or the code can contain more "dynamic" payloads that can be configured to result in multifaceted attack vectors. The SIRT members should understand not only how malicious code is propagated through some of the obvious methods (disks, email, programs, etc.) but also how it can propagate through other means such as website deployments, PostScript, Word macros, MIME, peer-to-peer

file sharing, or boot-sector viruses that affect operating systems running on PC, UNIX, LINUX, or Macintosh platforms. The SIRT members must be aware of how such attacks occur and are propagated; the risks and damage associated with such attacks, prevention and mitigation strategies, detection and removal processes, and recovery techniques.
Team members with special skills in reverse engineering, malicious code review, or detailed code analysis can provide additional support and focused methods for response during incident handling activities.

- Ability to identify host system security issues, from both a user and system administration perspective (backups, patches)
  The SIRT members should have a variety of expertise and exposure to the various types of operating systems (UNIX, Windows, LINUX, MacOS, or any other operating systems used) deployed in their area of responsibility. The members need to have experience in the operating aspects of the operating system, how the operating system is managed, maintained, patched, and how the security parameters of the operating system are installed and monitored.
  Then, for each operating system, the SIRT members need to know how to:
  - configure (harden) the system securely,
  - review configuration files for security weaknesses,
  - manage system privileges,
  - identify common attack methods,
  - determine if a compromise attempt occurred,
  - determine if an attempted system compromise was successful,
  - analyze the results of attacks,
  - review log files for anomalies,
  - recover from a compromise,
  - secure network daemons for non-Windows servers.
- Ability to identify network security issues (firewalls and virtual private networks)
  The SIRT member should have the ability to anticipate, identify, isolate, and describe potential new vulnerabilities that could affect the area of responsibility as a result of changes in network design, hardware, or software. The SIRT member should be able to identify security weaknesses in current network configurations, deployments, and architectures. The SIRT member should be able to identify and develop tools or processes that would mitigate or resolve these potential security weaknesses.
- Which encryption technologies (Triple DES (3DES), AES, IDEA, Blowfish) are in use in the organization
  The SIRT member needs to have awareness and understanding of the basics for use and employment of encryption within the area of responsibility. He/she needs to be aware of both major methods of encryption, symmetric and asymmetric, and how each is used.

The SIRT member must be aware of the core encryption algorithms (AES, 3DES, IDEA, etc.) used in each method and how they function in order to properly identify encryption deficiencies, weaknesses, and attacks. He/she should be familiar with the customer's means of Key Management and Key Distribution in order to understand potential key issues as this is usually the primary area of man-in-the-middle attacks on key systems.

- How digital signatures (RSA, DSA) are used and defined
  The SIRT member should be cognizant of the methods and means used by the customer of Digital Signature activities for verification and validation of message traffic and electronic contract actions. The basic core Digital Signature algorithms (RSA and DSA) and their usage under corporate and federal standards (FIPS-186) are areas of focus for the SIRT member.
- Where cryptographic hash algorithms (MD5, SHA-1) are utilized and under what conditions are they used
  Hashing is often used throughout an organization for multiple requirements, such as password control, digital signatures, software version integrity checking, and file system integrity reviews. The SIRT member should be aware of each version and type of hashing is used, what particular version and algorithm is utilized (MD5, SHA-1, etc.), and how the process is controlled in the particular instance or application where it is employed. The methods for hashing and which algorithm is relevant is often a critical skill and knowledge set for the SIRT member as hashing is used extensively in Incident Response and Forensics for integrity purposes by the investigators and analysts to control evidence and its validity. Therefore, this understanding is vital to the SIRT member and often is a core critical skill necessary for team membership.
- An understanding of public data networks (telephone, ISDN, X.25, PBX, ATM, frame relay)
  The SIRT member should be well versed in the organization's data source provider's services and the telephone service provider's delivery mechanisms. Understanding the delivery and services being provided gives the SIRT member some awareness of the types of security controls inherited by the organization from their service providers and allows the team member to use the "upstream" security to assist in response efforts if the suspicious incident is originating from outside the organization. So the SIRT member needs to know what type of telephone services are provided, what kind of data delivery is provided and through what technologies is the data service delivered to the organization, and what access is provided to the organization from the Internet Service Provider.
- Possibly even domain experts from the fields of:
  - applications,
  - system,

- security,
- network,
- mail,
- database.

TYPES OF PERSONAL SKILLS NEEDED

These skills can become paramount for each team member to have as incidents are investigated, events happen, and breaches are found and disclosed to management, customers, and clients.

- *Common sense* to make efficient and acceptable decisions whenever there is no clear ruling available and under stress or severe time constraints. This one skill can be the most important in a crisis situation—"clear-headed" thinking and even decisive decision-making. The SIRT member who is technically competent and has excellent communication skills can solidify the reputation of the team and strengthen the respect with which a team is held (both by the customer and by others with whom the team interacts). On the other hand, the interactions of a SIRT member who is a technical expert but who possesses poor communication skills or no "common sense" can result in miscommunications and/or actions that can severely damage a team's reputation and standing in the community, especially when those communications are misinterpreted or mishandled.
- Strong, effective oral and written *communication skills* (in native language and English) to interact with clients and other teams. All communications need to be conducted so that there is no misunderstanding or misinterpretation of the needs of the responders. The SIRT member needs to be effective in his/her communications to ensure that they obtain and supply the information necessary to be helpful. They need to be good listeners, understanding what is said (or *not* said) to enable them to gain details about an incident that is being reported. The SIRT member needs to remain in control of these communications to most effectively determine what is happening, what facts are important, and what assistance is necessary.
- *Diplomacy* when dealing with other parties, especially the media, the senior management, and customers. Each response effort will involve the outside response staff personnel and management. Each interchange with these personnel needs to be handled in a proper and secure manner. Diplomacy and tact are essential when dealing with outside parties. The SIRT member needs these skills to be able to anticipate potential points of contention, be able to respond appropriately, maintain good relations, and avoid offending others.

- The dedicated *ability to follow* policies and procedures. Every response team has corporate policies and procedures defined for their efforts, investigations, and reporting mechanisms. Each of these documents needs to be followed during the response effort. To ensure a consistent and reliable incident response service, the SIRT member must be prepared to accept and follow the rules and guidelines, even if these policies, procedures, guidelines, and rules are not fully documented and regardless of whether the team member personally agrees with them. On the other hand, if the SIRT member feels that change is required and if they want to approach management with suggested changes, they should be permitted to propose changes.
- Always willing to *continue education*—learn new ways to handle and contain incidents. One of the hallmarks of a good investigator is the willingness to learn new techniques, tactics, and investigative procedures. The incredible diverse ways of attack available today demand constant learning of response methods and attack mechanisms to stay current.
- Extremely strong *ability to cope with stress* and work under pressure. Any incident response has several focus points which require direct and immediate attention. The identification of the incident, the containment of the harm from the incident, and the quick removal or eradication of the cause of the incident all are "pressure-packed" actions to be accomplished by the response team and its members as expeditiously as possible. The SIRT member, particularly, needs the ability to remain calm in tense situations; ranging from an excessive workload to an aggressive caller to an incident where human life or a critical infrastructure component could be at risk. The SIRT's reputation, and the team member's personal reputation, will be enhanced or will suffer depending on how such situations are handled.
- Must be a *team player*—no "lone wolf" personnel. In a response setting, SIRT members don't usually have the time for individual actions. These efforts are conducted by a team of incident responders which have varying degrees of expertise in different areas, so no one responder needs or should have all of the knowledge needed to completely handle any single incident. The SIRT members need to be aware of their responsibilities, contribute to the goals of the team, and work together to share information, workload, and experiences. Each team member must be flexible and willing to adapt to change as well as having team skills for interacting with other parties, both internal to the team and external to the organization.
- *Integrity and trustworthiness* of the member to keep a team's reputation and standing, especially in the face of possible criticism. Full trust and understanding of the team member's capabilities and expertise must be had by the team leader to ensure the integrity and trust of the team is maintained. Often, in response efforts, data becomes available to the SIRT member which is newsworthy. In this case, the team member must

be trustworthy, discrete, and able to handle information in confidence according to the SIRT rules and guidelines, any customer agreements or regulations, and/or any organizational policies and procedures. The SIRT member may find himself in a position where he knows about information and could comment on a topic, but doing so could acknowledge or disclose information that was provided in confidence or that could affect an ongoing investigation or response effort. So the SIRT member must remain aware of his responsibilities and not be caught "off guard" and make unauthorized disclosures of his own.

- A willingness to *admit to one's own mistakes* or knowledge limitations about a topic and then go out and research it. However difficult it may be to admit a limitation, the SIRT member must recognize his or her limitation and actively seek support from their team members, other experts, or SIRT management. Always learning, examining, growing in knowledge and understanding of techniques are areas for each team member to actively pursue and update throughout their career.
- *Problem-solving skills* to address new situations and efficiently handle incidents as they happen. New techniques for attacks, new methods for response, new technologies are always arriving within the organization and need to be added to the repertoire of the team members' skills. SIRT members can become overwhelmed with the volumes of data related to incidents and other tasks that need to be handled if they don't have good problem-solving skills. Problem-solving skills also include an ability for the SIRT members to "think outside the box" or look at issues from multiple perspectives to identify relevant information or data.
- *Time management* skills and abilities, in order to concentrate on priority work. Focusing on the task at hand during the response and subsequent investigation is vitally important to the proper and quick resolution for any incident. Effective time management is important for the SIRT member because they will often be confronted with a multitude of tasks ranging from analyzing, coordinating, and responding to incidents to performing duties such as prioritizing their workload, attending, and/or preparing for meetings, completing time sheets, collecting statistics, conducting research, giving briefings and presentations, traveling to conferences, and possibly providing onsite technical support.
- Ability to consistently *deliver briefings* and possibly even court testimony. Expert witness testimony is always possible in any incident resolution effort, so each team member must have skills in properly explaining their efforts, and making it straightforward for potential external parties, such as court officers, lawyers, and juries. The SIRT member needs skills to present a technical briefing, management, or sponsor presentations, a panel discussion at a conference or seminar, or some other form of public-speaking engagement as required by the SIRT or management.

The SIRT member presentation skills probably will include providing expert testimony in legal or other proceedings on behalf of the SIRT or a customer.

All of these skills, abilities, and knowledge areas are found best when the team members are blended together to form a cohesive unit for incident response. Not many people are going to have all of these at one time, but the team concept comes into play here with certain skills and expertise on the team, rather than in people. Our response efforts are too varied to try to gather all these skill-sets into one or two individuals.

SP 800-61, the NIST Guide for Incident Response, also provides some guidance on ensuring team members stay active and engaged while participating in team activities and events as follows:

"It is important to counteract staff burnout by providing opportunities for learning and growth. Suggestions for building and maintaining skills are as follows:

- Budget enough funding to maintain, enhance, and expand proficiency in technical areas and security disciplines, as well as less technical topics such as the legal aspects of incident response. Consider sending each full-time team member to at least two technical conferences per year and each part-time team member to at least one.
- Ensure the availability of books, magazines, and other technical references that promote deeper technical knowledge.
- Give team members opportunities to perform other tasks, such as creating educational materials, conducting security awareness workshops, writing software tools to assist system administrators in detecting incidents, and conducting research.
- Consider rotating staff members in and out of the incident response team.
- Maintain sufficient staffing so that team members can have uninterrupted time off work (e.g., vacations).
- Create a mentoring program to enable senior technical staff to help less experienced staff learn incident handling.
- Participate in exchanges in which team members temporarily trade places with others (e.g., network administrators) to gain new technical skills.
- Occasionally bring in outside experts (e.g., contractors) with deep technical knowledge in needed areas, as funding permits.
- Develop incident handling scenarios and have the team members discuss how they would handle them.
- Conduct simulated incident handling exercises for the team. Exercises are particularly important because they not only improve the performance of the incident handlers, but also identify issues with policies and procedures, and with communication."[1]

[1] SP 800-61, Guide to Computer Incident Response, 2007.