Global Information Assurance Certification Paper

Building an Information Technology Incident Response Team: Issues that Need Special Attention

Tim Hicks

GSEC Version 1.4b Practical Paper
Submitted: April 17, 2003

Abstract

Most organizations have either addressed or are addressing the need for building Information Technology-based (IT) incident response teams and incident response plans. Many already have incident response programs to address physical emergencies and natural disasters, but they may not have designated trained personnel or equipped them to handle IT related incidents. Y2K[1], virus attacks, government regulations, and other current major national and worldwide events have demonstrated that the ability to respond to computer-related incidents has become critical and in some circumstances legally obligatory in many industries and government agencies. Although incident response activities could be outsourced to third parties, many more organizations have looked internally to build IT-based incident response teams. To help build these teams, many organizations and government agencies are sending their staff to training courses to learn how to create, staff, and implement an in-house IT incident response team.

Most of the training programs and courses available describe the "best practices" for building an IT incident response team with this information designed to assist the students when they return to their organization. Classes are available from *SANS Institute*[2]*, CERT Coordination Center* at *Carnegie Mellon*[3]*, Megamind*[4]*, and WhiteHat Inc.*[5]*,* to list just a few. These classes cover major topics and issues associated with creating an incident response team. Many of these issues are discussed in general terms but their relevance may not apparent to the student during the training. This paper describes those issues and others that have potential of creating significant problems and delays with the creation of an IT-based computer incident response team, program, and plans. From experience, these issues are usually not be given the emphasis and attention they require.

Issues with Building an IT-based Security Incident Response Team

Attending a training class is excellent exposure to the issues surrounding building an IT-based incident response team. Live experience however is still the best teacher. Certain issues create significant roadblocks in the team building process. Since many of these issues are multi-faceted, they have been categorized into six (6) groups.

1. Selection of Incident Response Team members and Team Organization
2. Management Understanding, Commitment, and Support
3. Enterprise-Level Policy, Standards, Guidelines, Practices
4. Compliance and Enforcement
5. Physical Requirements for an Incident Response Team
6. Team-Level Policy and Practices

Selection of Incident Response Team members and Team Organization

Many organizations have an incident response group or team that can respond to physical emergencies (fire, power outages, etc.) and natural disasters (hurricanes, flood, earthquake, etc.) Incident response teams that respond to computer-based incidents and potential cybercrimes are relatively new for most organizations. Selecting the right personnel, management and the team members, will be one of the first major issues encountered.

Management Lead and Support

With any endeavor, having qualified leadership is a key element to success. An IT-based incident response team must have a strong, management leader that understands both the need for such a team and the fundamental requirements for building and supporting the team. Finding such a leader can be a difficult task, but the lack of leadership or having a leader that does not understand the concepts of incident response can be disastrous and lengthen the timeframe to organize and institute the incident response team. First and second line management should be encouraged to attend training for their level management prior to implementing an incident response team. Classes for management are available. Hopefully, the team's management would also have a strong IT background.

Team Lead and Clearly Defined Roles

It is even more important to select qualified people and the right combination of people for the actual incident response team. As with management, selection of a strong team lead, appropriately trained, is vital. This should make common sense but the selection of the wrong team lead can quickly lead to discontent on the team and delay implementation. Along with a knowledgeable team lead, the team itself should be handpicked based on their skills, knowledge, and attitude.

There are three primary attributes that an IT incident response team member should have. One, they need to have an appropriate level of technical expertise. This does not however mean that the mostly highly skilled technicians will necessarily make good incident response team members. Two, they need to be able to work in an unorganized environment that can sometimes be viewed as chaotic especially during an acute emergency incident. They must to be able to keep calm and complete their respective duties. Three, they need to capable and willing to document, in detail. Surprisingly how many strong technical analysts cannot or will not document what they do and how they do it. This is extremely important since good documentation is key to incident response.

Once the team has been selected, it is important to very clearly define and document each team member's role, duties, and responsibilities. Sounds simple, but sometimes this step gets lost in the shuffle. Without clearly defined roles and responsibilities, the team may initially struggle at being effective.

Training and Expertise

Proper training is critical for any incident response team and the organization must be willing to make those expenditures appropriately. There are a myriad of training programs, both managerial and technical, covering most all the topics surrounding incident response. Certifications are also available. Training of often overlooked and under funded. When building the team, a clear training plan must be developed and approved before the team is implemented. Waiting for training until after the team is operational does not work well. Waiting for training may reduce the effectiveness of the team and planned expenditures could be redistributed elsewhere or eliminated if used. Training must be approved and supplied up-front.

Need for Subject Matter Experts

During an active incident and during follow-up investigations to determine root-causes, an incident response team must take advantage of subject matter experts, both technical and non-technical. The incident response team often does not have the expertise or staff to do everything that is needed during an incident and must rely on others for assistance. These "virtual" team members also require a minimum level of training to at least cover confidentiality/privacy policy and the proper way of handling potential evidence. This extended group may require a large number of people in some organizations. Their training and managing their time during incidents are often overlooked when initially planning for and building an IT incident response team. Subject matter experts must be accounted for in cost projections too.

Management Understanding, Commitment, and Support

Laws and regulations are forcing many companies to specifically address the monitoring and response to potential IT security vulnerabilities and threats. For example, with financial and insurance institutions, the Gramm-Leach-Bliley Act of 1999 states that institutions must "insure the safety and confidentiality of customer information, protect against any anticipated threats or hazards to security or integrity of such records, and protect against unauthorized access to or use of such records" [6]. Recent HIPAA[7] legislation specifies how personal medical history data must be secured and protected. Many states are adopted legislation that continue to place more emphasis on requiring organizations to have increased data protection and provide additional security due diligence. New legislation and regulations are making it increasingly necessary for organizations to create, maintain, and utilize on internal IT-based security incident response teams along with clearly defined and published incident response plans. "A new California law requiring companies to notify their customers of computer security breaches applies to any online business that counts Californians as customers, even if the company isn't based in the Golden State."[8]

All levels of management, in both business and government sectors, are beginning to understand that they could possibly be held liable for the lack of appropriate security measures. Upper levels of management are also beginning to understand the need

for IT incident response teams. For the team to be successful, it is extremely important to obtain that commitment and support, up-front, from all potential decision makers. Those higher-level decision makers may also need training. SANS Institute, Carnegie Mellon and others third parties offer mid to high-level management sessions and seminars on managing incident response. Building and implementing an IT incident response team and incident response plans will require approved expenditures, therefore management support at all levels is essential. Steps should be taken to involve upper-management early in the team development process.

Security Policy, Standards, Guidelines, Practices

The need for security-based policies within an organization cannot be emphasized enough. Many incident response team-building courses have discussions of policy, standards, and guidelines in their curriculum and most assume an organization has effective, published policies. The issue for the incident response team is what to do if polices are not in place.

Policies, regardless of type, are usually multi-faceted. Having effectively written and comprehensive policies published is step one. Awareness of policies and being able to distinguish between policies, standards, and guidelines is step two. Compliance and enforcement of policies is the required step three. Without a framework for the creation, review, approval, publishing, enforcement of, and amending of policies, especially IT security-related policies, an incident response team will be ineffective. Some organizations have very stringent and highly enforced policy. Others may have very "loose" policies that may, in reality, serve more as guidelines than enforceable policies. There are key policy-related issues that should be addressed in order for a team is to be effective and successful.

Lack of Determining the Assets Critical to the Organization

Trade Secret and highly confidential data or information would likely be considered critical to an organization. For some general businesses, critical assets could also be something physical such as their employees, customers, products, or inventory. Still for others, it could processes, formulas, or things less tangible like image to their consumers or their organizational trustworthiness. Like data, any aspect of the organization that is deemed critical should be designated and documented. This would allow the IT incident response team to set appropriate priorities when responding to incidents. During an emergency incident, time is usually the most critical factor. Triage often becomes a necessary part of incident response. Knowing what is critical to the organization beforehand can be the difference between an effective response and a failed response. If an organization has not addressed the issue of identifying what is critical to its operation for both short and long-term survival, their incident response team cannot effectively make the emergency decisions that may be needed.

Lack of Data/Information Classification

An organization that has not classified all its data based on some form of risk scale and documented those classifications may be flirting with potential disaster during an incident. The IT incident response team must understand the criticality of assets and the risk of potential loss or compromise on the organization. This way the response team can properly prioritize emergency activities even if assets, data or otherwise, are only classified as critical or non-critical, public or private, confidential or non-confidential. The incident response team must be able to quickly assess the level of response required. To do this, organizational assets, especially data, must be classified based on its criticality to the organization.

Lack of Security Policy

Security-based policies are key to the IT incident response team because it will be security policies most often compromised by incidents. Security policy defines all the IT processes and activities that are acceptable and unacceptable for an organization. There are still organizations that may have not documented their enforceable security policy. Even in organizations with well defined security policies, general awareness of those policies may be lacking, thus many potential violations may be totally unintentional rather that intentional. When creating an IT incident response team and incident response plans, strong security policies and standards are critical and should be addressed early in the team's development process. The SANS Security Policy Project[9] recently published a guide to assist organizations with development and implementation of information security policies.

Lack of Encryption Policy and Standard

Another issue arises when the organization has a lack of a data encryption policy or standard. An organization without a data encryption policy may be exposing critical data to unwanted risks. Encryption policy is predicated on the assumption that critical data has been identified and should be protected from unauthorized viewing. The actual technical encryption policy/standard should allow for the appropriate level of protection based on the data/information's classification, the technical "strength" of the encryption method being used and the way the information is transmitted. For instance, today, 128-bit encryption is considered strong while 40-bit encryption weak[10]. In transmission, information being sent via the Internet unencrypted is subject to being intercepted. Digital telephones are considered more secure than analog telephones. The basic issue is that the IT incident response team will continually be battling potential loss or unwanted exposure of information if an encryption standard or policy is not implemented, published, and enforced.

Lack of an Acceptable Use Policy

A topic that is covered in Carnegie Mellon courses and SANS Institute training is the need for all organizations to establish Acceptable Use Policies. Like data classification and encryption policy, an IT incident response team will not function effectively without them. Acceptable uses for any organizational asset or process

must be clearly defined, published and all users made aware. A recommended practice is for employees, staffs, and management to sign-off on Acceptable Use policies as part of an organizational awareness program. This awareness and sign-offs supply the basis for enforcement. Some of the more critical policies include:

Internet Usage
E-mail Usage (Spams, Chain Letters, Illegal, Offensive or Threatening Content)
Systems Access and Permissions
Copyright, trademark, patent, trade secret, intellectual property infringement

Acceptable Use policies may be covered in an organization's personnel code-of-conduct or similar documents. Acceptable Use policies can impact an incident response team in two ways. First, an experienced incident response team will spend considerable time responding to acceptable use violations of one kind or another. Second, the incident response team itself may require exceptions to those policies in order to actual perform their response activities. An example of this would be the need for the team to actually view potential inappropriate e-mail, such as pornography, during an incident. In the most literally sense, this could be considered a use policy violation also. It is extremely important to document all policy exceptions and any other circumstances unique to the incident response team. Special management approval/sign-off is imperative.

Many workable Acceptable Use Policy templates are available on the Internet and from various vendors and can be used as guides. It is important to recognize that Acceptable Use Policies are also critical to the creation and implementation of an IT incident response team and incident response planning.

Lack of Internet Usage Policy

One particular Acceptable Use Policy, an Internet Usage Policy, requires special attention since the use and misuse of the Internet will create many potential incidents the team must respond to. Organizations that utilized the Internet as part of the business or offer the Internet as a tool for their staff should have some form of Internet Usage Policy. What is not often addressed is the potential impact of allowing wide-open access with no compliance or enforcement. In these cases, unacceptable uses such as accessing inappropriate sites and downloading unsupported, illegal, or potentially harmful software can become violation nightmares for the incident response team. The lack of logging and tracking accesses can also create problems for the incident response team when determining what is actually occurring during an incident. Internet Security Policy should be reviewed at the time the response team is created.

Compliance and Enforcement

Even organizations, business and government, that have addressed their need for policies and standards and awareness still may not have an effective compliance program. Policies will become just guidelines at best without a defined, published,

and effective compliance program with published enforcement procedures. Again, this is not a new topic in classes but it is often not emphasized enough. Without a recognized compliance program with non-compliance ramifications, the incident response team will become frustrated with the outcome and resolutions of many incidents responded to.

There are many computer software vendors with products to assist an organization with identifying specific policy violation. Intrusion Detection products, in a broad sense, detect policy violations. Regardless of the tools being used, they are of little value if there are no ramifications for the specific violation detected. The response team would have no support for enforcement. It is very important to the people building an incident response team and program to assure that appropriate enterprise and security policies are in place, an awareness program is implemented, and there is a compliance program with consequences for non-compliance.

Physical Requirements for an Incident Response Team

For organizations beginning to build an IT-based team and program, there can be a reluctance to make the start-up expenditures beyond the personnel and initial training costs. Approval for any special physical environment and tools must sometimes wait until the incident response team proves its worthiness by responding to a number of incidents. A step-by-step strategy must be developed to recognize the team's requirements and then formulate the required justification for any physical environment changes, additional training, and equipment/tools to perform appropriate response activities.

Only experience will determine the physical needs for an incident response team and this will differ in organizations. One common attribute however, is the need to maintain confidentiality and relative privacy during incidents. This may require response team members to be physically located close to each other all the time. Incident response team activities during an incident should not be conducted in a general work area, if it can be avoided. Since there is a cost associated with the team's physical environment, acquiring a secured location for the entire IT incident response team to work from, may not be easily justified. An additional testing and research computer lab may need to be justified also. During incidents, conversations and interviews must be conducted in person or over the telephone. Documentation must be prepared. Response activities may also need to be conducted in multiple locations including general work areas. These activities will likely require a high level of confidentiality thus physically secured location for the team may be justifiable.

The same process should also hold true for incident response hardware or software tools. When there is a need for such tools and not having them available limits the team's response capabilities, a case should be made for acquiring them. There should always be core set of tools that each response team member is proficient with. The key is to show that response capabilities and management expectations may be negatively impacted without the proper physical environment, tools and training.

Team-Level Policy and Practices

Specific policies and exceptions to policies should be in place before the IT incident response team begins handling incidents. Most training courses like Carnegie Mellon's *Creating a Security Incident Response Team* course[11], references some of the following policies that can apply directly to individual incident response team member.

Code-of-Conduct
Security Policy
Information Categorization Policy
Internet Usage Policy
Compliance Policy
Information Disclosure Policy
Human Error Policy
Media Policy
Law Enforcement Contact Policy

Some of these policies have been discussed earlier. Media and Law Enforcement Contact policy are self-explanatory. It is important to note that the incident response team may need exceptions or exclusions to these policies and additional agreements. All exceptions and additions must be approved at appropriate levels of the organization. Human Resources and a Legal Department may also need to be involved. An example of a policy exception could be an Internet Usage policy and Code-of-Conduct exception because the team may be required to view inappropriate Internet sites or other offensive materials collecting evidence in an incident. The incident response team may also use computer software tools not approved for general use. The team may require special access privileges to both physical resources and IT-based resources. The team may require special privileges to access highly sensitive information while responding to an incident. Policy exceptions and others special rules may not be immediately apparent when first building a team.

The incident response team may require special levels of protection based on the types of activities they are asked to perform. An Information Disclosure Policy and a Human Error policy are two examples of added protection the team may require for their protection. As more federal and state laws and regulations are passed that require more stringent protection of data and requiring more "due diligence" with securing certain computer environments, incident response teams may require additional personal protections. In some organizations, team activities may be covered in already established policy and practices. In organizations where each employee must sign an employment contract or a separate Code-of-Conduct, exceptions for the may need to be documented in those documents. The appropriate level of IT management should approve all team exceptions. The incident response team and its management must continually monitor the policy needs for the team and its members.

Conclusions

It is difficult to prioritize what issues are the most important when first building an IT incident response team. The order in which they are presented here is a suggested priority sequence. If an organization chooses to develop a team in-house or contract the service with a third party, resolving these issues should not change significantly. The requirements for maintaining security, confidentiality, and privacy will only increase over time. One thing is certain. The role of the IT-based incident response team and incident response will be ever changing and team requirements will need constant reviewing and updating.

References

[1] - Reference to Year 2000 or any 1/1/2000 computer-related activities.

[2] – SANS Institute Training, Track 8: *Systems Forensics, Investigations and Response*
URL: http://www.sans.org/onsite/track8.php

[3] – Carnegie Mellon Software Engineering Institute Education and Training, *Creating Computer Security Incident Response Team*
URL: http://www.sei.cmu.edu/products/courses/cert/creating-csirt.html

[4] - Megamind, an Institute for Advanced Technology Training, *Incident Response*
URL: http://www.megamind.org/TRAIN/incident.html

[5] – WhiteHat, Inc., *Computer Incident Response*
URL: http://www.whitehatinc.com/education/course-incidentresponse.html

[6] - Public Law 106-102, 106th Congress, 1st Session: Gramm-Leach-Bliley Act of 1999 Title V Subtitle A: "Disclosure of Nonpublic Personal information" Section 6801. URL: http://www.ftc.gov/privacy/glbact/glbsub1.htm#6801

[7] - Public Law 104-191, AUG 21, 1996, Health Information Portability and Accountability Act of 1996 (HIPAA), Standards for Privacy of Individually Identifiable Health Information, Final Rule - 45 CFR Parts 160 and 164
URL: http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf

[8] – Poulsen, Kevin. "California Disclosure Law had National Reach (News and Commentary)", SecurityFocus Magazine, published January 6, 2003.
URL: http://www.securityfocus.com/news/1984
Related URL: http://www.privacy.ca.gov/califlegis.htm

[9] - URL: http://www.sans.org/resources/policies/ - intro

[10] - URL: http://www.rsasecurity.com/standards/ssl/basics.html

[11] - URL: http://www.sei.cmu.edu/products/courses/cert/creating-csirt.html

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event