Creating and Managing an Incident Response Team for a Large Company

Timothy Proffitt
Creating and Managing an Incident Response Team for a Large Company

GCIH Gold Certification

Author: Timothy Proffitt, tim@timproffitt.com

Adviser: Pedro Bueno

Accepted:
Creating and Managing an Incident Response Team for a Large Company

Outline

1) Incident Response Team Basics ................................................................. 3
   a) Introduction ......................................................................................... 3
   b) CSIRT Services ................................................................................ 3
       i) Passive Services .......................................................................... 3
       ii) Active Services ........................................................................... 5
       iii) Management Services ............................................................... 7
   c) CSIRT Policies and Standards .............................................................. 8
       i) Incident Response Policy ............................................................. 8
       ii) Incident Response Standards and Procedures ............................. 9
       iii) Code of Conduct ....................................................................... 10
       iv) Disclosure Policy ....................................................................... 10
       v) Evidence Handling Procedures .................................................. 14
2) Primary Phases of the CSIRT ................................................................. 16
   a) Identification ..................................................................................... 16
       i) Triage Role .................................................................................... 17
       ii) Identification Tasks ..................................................................... 17
   b) Containment ..................................................................................... 19
   c) Eradication ...................................................................................... 20
   d) Recovery .......................................................................................... 21
   e) Lessons Learned .............................................................................. 21
3) CSIRT Membership............................................................................... 22
   a) CSIRT Staff .................................................................................... 22
   b) CSIRT Training .............................................................................. 24
   c) Extensions of the CSIRT ................................................................. 25
4) Conclusion ............................................................................................ 26
5) References ............................................................................................ 26
   Appendix A ......................................................................................... 28

Tim Proffitt
- 2 -
1) Incident Response Team Basics

a) Introduction

The computer security incident response team’s (C.S.I.R.T.) function is to react in a timely fashion, to intrusions, types of theft, denial of service attacks and many other events that have yet to be executed or considered against their company. The CSIRT will be responsible for investigating and reporting on malicious insider activity, internet spam, human resource violations and copyright infringements.

The CSIRT will typically be called into action by a notification or triggered event but can also be called into action by a discovery while performing one of many passive services. Call Centers, Help Desks, business unit liaisons, legal representatives, email notifications or anonymous forms from an Intranet will all be entry points into calling the CSIRT into action.

b) CSIRT Services

CSIRT serve several purposes. In addition to identifying, containing and eradicating a successful intrusion, the CSIRT will educate, communicate, execute vulnerability assessment, shape policy and more.

i) Passive Services
There are several passive services that the CSIRT will perform to provide the company aide protecting its information systems in anticipation of future malicious activity.

Vulnerability Assessment

The CISRT will perform vulnerability assessment against company assets. The CSIRT will verify reported vulnerabilities and how they can be exploited. The vulnerability assessment service can help the business to identify infrastructure that is a high risk and can also provide data on a system that has had incident response procedures executed against it. The vulnerability assessment service will help identify when the recovery phase of an incident response effort has mitigated the intrusion. Maintaining current vulnerability assessment data for the company’s high risk systems can better mitigate the security threats to the company.

Announcements and Information Disclosure

The announcement function is used to notify business units of potential threats to information systems, external virus outbreaks that can affect the infrastructure and new compliance objectives. The CSIRT will monitor technical developments and trends to help identify attack vectors. The announcement service will provide guidance to the business to aide in mitigating security threats before they happen.
In some cases, when investigating an intrusion, a disclosure of sensitive information will be uncovered. In the case of medical information (ePHI) or identity theft data loss, the CISRT will perform defined disclosure procedures. Depending on what data was exposed and which state the personally identifiable information owner resides in, the disclosure notification procedures will vary. Disclosure procedures will involve crafting notification letters, obtaining identity theft protection services for the effected parties, working with corporate communications to deal with the media, and potentially providing law enforcement evidence of the intrusion.

Intrusion Detection Service

The intrusion detection service is conducted by the monitoring efforts of the CSIRT. In some cases the security group and the CSIRT will be separate teams and monitoring of IDS and IPS technologies may be shared. In these cases, alerting on intrusion information will be passed up to the CSIRT for incident handling. The intrusion detection service typically monitors intrusion detection equipment, intrusion prevention equipment, security event manager logs and performs periodic intrusion discovery procedures. When an event of interest is identified, the CSIRT will move into its active services mode.

ii) Active Services
Creating and Managing an Incident Response Team for a Large Company

There are several services that the CSIRT will perform during an incident. The active services are typically what is expected of a CSIRT and are designed to contain, eradicate, recover, and report on an incident.

Incident Handling

Incident handling involves analyzing the incidents and events. Incident handling’s goal is to identify the scope of the incident, document the damage caused, and provide available response tactics. Incident handling typically involves incident analysis, evidence collection, tracking the origins of the intruder, response support for the victim(s) of the attack and coordination among other IRT, administrators and service providers.

Vulnerability Handling

Vulnerability handling involves gathering data around operating system and application vulnerabilities. The CSIRT will perform assessments against hardware and software to verify suspected vulnerabilities and help determine how the vulnerabilities can be exploited. The service will aide in determining the proper response to repair a vulnerability and can notify others about the mitigating strategy.

Evidence Handling

Evidence can be defined as any object found on an information system that could be involved in attacking the system or other systems around it. These can be computer viruses but also include exploit scripts, toolkits, log files, or even hardware devices such as physical key loggers.

Tim Proffitt
Creating and Managing an Incident Response Team for a Large Company

Lessons Learned Reporting

The reporting service primary goal is to document what happened and how the business can improve its’ defenses. The CSIRT will conduct a “lessons learned” or a post mortem meeting to discuss the incident and educate the management team. Incident Reporting is beginning to become an auditable event for external auditors to test against.

iii) Management Services

Awareness Training

Awareness training can be a service offered by the CSIRT. Since the CSIRT is typically conducting in depth investigations and vulnerability assessments against the businesses information assets, then next logical step is for the CSIRT to educate the technology teams about good security practices pertaining to the information systems that are being administered.

CSIRT will also seek opportunities to build awareness of the user base through newsletters, announcements, lessons learned, marketing campaigns, and websites.

Risk Assessments

The CSIRT can have important insight into risk assessments. When the business conducts a risk assessment to bring on a new technology or application, a member of the CSIRT should be a participant in the effort. The experience of the CSIRT members will help identify risk points, potential vulnerabilities, and threats.

Tim Proffitt

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.
Compliancy Certifications

The CSIRT can also perform compliancy certifications. The team can conduct security evaluations on information systems or services to ensure the security or the pass / fail of a compliance regulation. The team can be used to provide guidance on best practices and recommendations for purchasing, installing or securing new systems.

c) CSIRT Policies and Standards

Policies are documented principles adopted by the management team. The policies of an organization should be clearly understood by the entire workforce and the knowledge of the incident response policy will allow the CSIRT to act on their responsibilities.

i) Incident Response Policy

Building an incident response policy involves several objectives.

First, an Incident Response Policy cannot be enforced unless it has management approval. Endorsement by management is critical. Without this approval the team will be destined to encounter business road blocks that will hinder a timely incident response. In some cases, it may not even be allowed.

Second, the policy must be clear. Any employee should be able to easily understand what the policy is about. If a non-technology oriented employee is confused by the policy, then the policy should be rewritten.
Third, the policy must be to the point. A long-winded policy will either be a bad policy or one that would include sections that should be in a procedure document instead.

Forth, the policy must be usable and implementable. Avoid statements that sound appropriate but will be open to interpretation. At the same time, the policy should not include objectives that the CSIRT will not be able to execute due to business processes or corporate culture.

Once the policy as been created, it is important to make regular checks against its effect on the workforce. When changes occur in the business direction or new technology systems are implemented, update the policy to match the new processes.

ii) Incident Response Standards and Procedures

A successful CSIRT is a team that has documented standards and procedures. Standards should be written from how the CSIRT will begin its investigations and report the findings to standards written for how the CSIRT will be trained and what authority the members will be granted.

A good standard will define when the CSIRT will contain and clean up incidents and when the team will watch and gather information for litigation.

Having good recovery procedures are essential. It is very rare to find a CSIRT member that has mastered every operating system and application in
Creating and Managing an Incident Response Team for a Large Company

your environment. Having procedures to follow on how to correctly down and restore a system can help prevent time consuming efforts and alleviate some of the stress of the incident.

These written procedures will aide the CSIRT in formalizing how investigations are carried out, how evidence is handled, what organizations are notified at what times, how post mortem reporting is conducted, how malicious software is to be eradicated and how to perform a recovery of a information system.

iii) Code of Conduct

The code of conduct policy for the CSIRT is a set of rules outlining how a team member will behave in a way that supports the goals of the incident response team and the mission statement of the company. The code of conduct will be used when no other policy or procedure applies. It should reflect the natural behavior of a professional incident handler. An example of a CSIRT code of conduct policy was written by the original manager of the CERT, Rich Pethia.

iv) Disclosure Policy

It is important to define the CSIRT disclosure policy. Without the policy, the team will have no guidance on who to disclose to, what to disclose and when to disclose the information. Traditionally, CSIRT staff treated all

1 CERT Coordination Center.

Tim Proffitt
- 10 -
information reported to them as confidential and information around security incidents were not distributed to other organizations. In some cases, law enforcement or other response teams were included when coordinating the response to the incident.

The policy should outline the information disclosure restrictions placed on the CSIRT staff. What will be reported to law enforcement? If the incident involved the disclosure of personally identifiable information, when do you disclose to the affected individuals? Personal information includes, but is not limited to, information regarding a person’s home or other personal address, driver’s license, marital status, financial information, credit card numbers, bank accounts, parental status, sex, race, religion, political affiliation, personal assets, home or other personal phone numbers, and so on. Did the incident involve the disclosure of electronically protected healthcare information as defined in HIPAA? Did the incident involve social security numbers? If the CSIRT is to engage law enforcement, can the business afford to have equipment confiscated?

The disclosure policy will specify (sometimes legal) limitations that outlines how or when law enforcement is notified, customers are notified, external CSIRTs and upper management.

There are very clear state laws in the United States that outline when companies must notify individuals that their personal information has been disclosed by unauthorized events. At least 35 states, as of Q1 2007, have

---

2 http://hipaa.yale.edu/guidance/index.html
Tim Proffitt
- 11 -
enacted legislation requiring companies and government agencies to disclose security breaches involving personal information\(^3\).

<table>
<thead>
<tr>
<th>State</th>
<th>Act</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arizona</td>
<td>Ariz. Rev. Stat. § 44-7501</td>
</tr>
<tr>
<td>Arkansas</td>
<td>Ark. Code § 4-110-101 et seq.</td>
</tr>
<tr>
<td>California</td>
<td>Cal. Civ. Code § 1798.82</td>
</tr>
<tr>
<td>Colorado</td>
<td>Col. Rev. Stat. § 6-1-716</td>
</tr>
<tr>
<td>Connecticut</td>
<td>Conn. Gen Stat. 36A-701(b)</td>
</tr>
<tr>
<td>Delaware</td>
<td>De. Code tit. 6, § 12B-101 et seq.</td>
</tr>
<tr>
<td>Florida</td>
<td>Fla. Stat. § 817.5681</td>
</tr>
<tr>
<td>Georgia</td>
<td>Ga. Code § 10-1-910 et seq.</td>
</tr>
<tr>
<td>Idaho</td>
<td>Id. Code §§ 28-51-104 to 28-51-107</td>
</tr>
<tr>
<td>Illinois</td>
<td>815 Ill. Comp. Stat. 530/1 et seq.</td>
</tr>
<tr>
<td>Indiana</td>
<td>Ind. Code § 24-4-9</td>
</tr>
<tr>
<td>Kansas</td>
<td>50-7a01, 50-7a02 2006 S.B. 196,</td>
</tr>
<tr>
<td>Michigan</td>
<td>2006 S.B. 309, Public Act 566</td>
</tr>
<tr>
<td>Minnesota</td>
<td>Minn. Stat. § 325E.61, § 609.891</td>
</tr>
<tr>
<td>Montana</td>
<td>Mont. Code § 30-14-1701 et seq.</td>
</tr>
<tr>
<td>Nebraska</td>
<td>Neb. Rev Stat 87-801 et seq.</td>
</tr>
<tr>
<td>New Hampshire</td>
<td>N.H. RS 359-C:19 et seq.</td>
</tr>
<tr>
<td>New Jersey</td>
<td>N.J. Stat. 56:8-163</td>
</tr>
<tr>
<td>New York</td>
<td>N.Y. Bus. Law § 899-aa</td>
</tr>
<tr>
<td>North Carolina</td>
<td>N.C. Gen. Stat § 75-65</td>
</tr>
<tr>
<td>North Dakota</td>
<td>N.D. Cent. Code § 51-30-01 et seq.</td>
</tr>
<tr>
<td>Ohio</td>
<td>Ohio Rev. Code § 1349.19, § 1347 et seq.</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>Okla. Stat. § 74-3113.1</td>
</tr>
<tr>
<td>Rhode Island</td>
<td>R.I. Gen. Laws § 11-49,2-1 et seq.</td>
</tr>
<tr>
<td>Tennessee</td>
<td>Tenn. Code § 47-18-2107</td>
</tr>
</tbody>
</table>

\(^3\) [http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm](http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm)

Tim Proffitt
Timing of a disclosure event is imperative. It is important to perform incident investigations and be as certain as possible about the disclosure events. At the same time the CSIRT should be notifying the victims as soon as possible. If the duration between the identification and the notification are too great, the company can face litigation and even greater loss of public opinion.\(^4\) It is imperative that the CSIRT utilize legal council when drafting a disclosure communication to anyone as this notification can have enormous consequences to the company’s reputation.

Disclosure Procedures to External CSIRT

There will be times where the company CSIRT will want to notify external CSIRT such as the CERT/CC, FIRST\(^5\), or private Managed Security Solutions Partners (MSSP). To be successful, it is important that coordination occurs among law enforcement, National CSIRTs and the research community who have experience in responding to security incidents. External CSIRTs can play an important role by helping their constituents protect their systems, detect, identify, and analyze compromises to the security of those systems and effectively coordinate the response to the attack. External CSIRT teams

---

\(^4\) [http://www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm)

\(^5\) [http://www.first.org/members/teams/](http://www.first.org/members/teams/)

Tim Proffitt
- 13 -
can also be evangelists in promoting and helping other organizations build effective incident management capabilities.

The details for sharing of information will change depending on the incident and how the external CSIRT will benefit from the information. Information is typically disclosed to:

- Inform other CSIRT of a large attack.
- Inform other teams about a new vulnerability or attack vector.
- Contact other sites that are the target of an incident to help coordinate the remediation.

Procedures should be clearly written for the internal CSIRT to follow when submitting an incident outside the organization. When reporting intruder activity, it is important to ensure that you provide enough information for the external CSIRT to be able to understand and respond to your report, but still filter any information that would be considered sensitive to the company.

v) Evidence Handling Procedures

During the CSIRT's active services, it is important to track information pertaining to the incident. This tracking of information should be at a level of detail that can be useful for recalling the event years later. Handling procedures should record information in logical organized methods to provide historical records and actions taken by the team. In many cases, this information can be used for statistical reporting purposes in management.
reports. For every incident, best practices capture and track, at a minimum, the following set of information:

- Local Tracking Number / External CSIRT Tracking Number
- Category of Incident
  - Disclosure, Hacking Attempt, Worm Outbreak, Malicious Insider, etc.
- Brief Description
- Contacts for all Parties Involved
- Subjective Priority
  - Critical, High, Medium, Low, Informational
- Evidence Gathered
  - who, what, where, why, how, when
- History of Actions
  - Record all actions by the team. This will be important if litigation is an optional outcome.
- Current Status of the Incident
  - Active, On Hold, Complete, etc.

CSIRT should utilize electronic collaboration tools such as a Microsoft SharePoint Server. Team members should have a single point to deposit, search, and update data on incident activities. Additionally, incidents should be archived for some predetermined period of time, using the collaboration tool. The SharePoint tool allows for a repository of electronic data, online workflow capabilities, versioning, automatic alerting and very flexible role
based access for team members and additional stake holders outside the team.

Physical evidence should be maintained in a designated “war room”. An empty office or conference room can be converted into a CSIRT war room with the understanding that the team will have sole access to a physically secured room. Locking cabinets for hard drives, tapes, and notes on tracking of the equipment are a must.

2) Primary Phases of the CSIRT

The functions that the CSIRT perform during active services are going to be considered the heart of the CSIRT mission. These primary functions are preparation, identification, containment, eradication, recovery, and lessons learned.

a) Identification

How does the company detect an event? What triggers the CSIRT into action? The answer for most is a mixed one.

- Technology departments deploy intrusion prevention sensors, monitor firewall logs, review honeypot activity, analyze antivirus alerts, review vulnerability assessment reports, examine authentication events, etc.

---

6 http://www.honeynet.org is a popular open source honeypot project

Tim Proffitt
- 16 -
Business units will typically educate and raise awareness about security risks to make the workforce use their eyes and ears to identify suspicious activity.

When either of these groups detects an event, the CSIRT should be notified.

i) Triage Role

The goal of the triage role is to ensure that information about an event is gathered from a single point of contact. The triage role is the primary contact for the CSIRT for the business. Contacted by email, fax, telephone, anonymous form, or hallway conversation, the triage role will kick off the incident procedures by calling into action the correct team members to start the investigation.

The company should be trained on how to report information to the CSIRT. The triage role should be clearly defined, contact methods should be easily accessible, simple and defined procedures for reporting and clear guidelines on types of events to be reported.

ii) Identification Tasks

The CSIRT should have a member of the management team as its sponsor. This is typically the CSO, CIO or VP over the technology department. Notify your sponsor that an investigation has started. If
additional resources are needed outside the CSIRT, the sponsor will help with obtaining what is needed.

It is in the identification function that a primary incident handler should be assigned. The responsibility of the primary handler is to ensure coordination, documentation, and communication with the CSIRT and any other departments or organizations directly involved. The primary handler will be responsible for the quality of the incident handling procedures for the assigned event.

The information gathered in this identification phase is critical. The first goal of the team is to determine whether the incident reported is actually an incident. The team will be asking assessment questions such as, what are the affected systems, if a vulnerability is present, the value of the system to the business (i.e. mission critical), can the vulnerability be exploited remotely, was this incident user error, was data exposed to unauthorized individuals, does this incident affect companies outside our own?

Be sure to establish good chain of custody scenarios. Document the “who, what, where, when”, whenever possible. Each piece of evidence must be under the control of a CSIRT member at all times and document the storage of evidence if it is secured. The chain of custody will be important for law enforcement if the evidence is going to be used in litigation.

---

7 See appendix for law enforcement contact information
Tim Proffitt
- 18 -
b) Containment

The containment function is designed to prevent the attack from affecting systems, people, or organizations any more than it has already. The CSIRT is now trying to keep the scenario from getting worse.

A decision must be made when entering the containment phase. If evidence collected is going to be used for litigation, care must be taken to keep the system(s) from becoming contaminated by the containment efforts. Drives should be imaged, back ups performed, original copies secured, etc. Always use a backup or a copy to perform the incident handling procedures.

The CISRT should perform multiple backups as soon as it is practical. The backups can be used for forensics or in the off chance that containment procedures render the system(s) inoperable. In most cases, original media will be cataloged and secured, while a backup copy will be used to restore the system for eradication and recovery.

The containment phase can involve many tasks: Patching systems, password changes, firewall rule changes, account management, stopping of services and RootKit / Antivirus system scans. On the employee side the CSIRT may place phone calls to halt a business process, obtain paper materials or printouts that contain false information or send a corporate wide communication to alert the workforce.
c) Eradication

The eradication phase involves the removal of any malicious activity or artifacts left by the intrusion. Typically eradication engages in removing virus infections, backdoor software, data left by the intruder and uninstalling attack tools. If the system was hit with any flavor of a rootkit, formatting hard drives, reloading the system, patching and restoration from backup is highly recommended.

Vulnerability assessment and analysis is typically performed during the eradication phase. Initiating system and network level vulnerability scans will help the team find open vulnerabilities. In many cases, attackers often use the same vulnerability across the entire network. A quality scanner such as Qualys\(^8\) or Foundscan can go a long way in providing your CSIRT will vulnerability data. The CSIRT should research the vulnerability against the known information repositories such as CERT or BugTraq to understand the impact of the exploit against the company.

Improving the defenses of the systems or business process affected is vital. New firewall rules, host based intrusion prevention technologies, upgrades to more secure applications and patching are good techniques for improving the defenses. If the vulnerability is not removed, the system can become compromised all over. Business process can be strengthened by objectives such as implementing least access principles, encryption mechanisms and social engineering awareness.

\(^8\) http://www.qualys.com/solutions/vulnerability_management/

Tim Proffitt  
- 20 -
d) Recovery

The recovery phase is used to bring the restored system(s) back into production. Recovery will typically take place, according to the system owner, after business unit testing has been conducted.

Monitoring is an important objective during this phase. When the incident system(s) are brought back into production use, monitoring must be conducted to validate the eradication was successful. Auditing the operating system logs, intrusion detection or prevention logs, checking for backdoor ports, reviewing firewall logs and searching for any new vulnerabilities are standard procedures.

e) Lessons Learned

The best way to improve on a company’s defense is to learn from the mistakes made. The goal of the lessons learned reporting is to finalize the CSIRT documentation, and create a post mortem report for review. In most cases, a meeting is scheduled within a week to review the report. The report should focus on events leading up to the incident, generally what occurred, what was done to contain and eradicate, and what can be done to mitigate the vulnerability in the future. The reporting phase is a good time to note organizational problems that conflicted with the CSIRT’s procedures and suggest improvements. Invite the correct management, stake holders and information technology individuals to better expose the CSIRT’s efforts. The
lessons learned meetings can be a good place to obtain approval to fix business processes, obtain newer technologies, update incident handling procedures and to educate the business.

It is important to have the CSIRT members involved in the incident complete the lessons learned documentation as close to completing the incident as possible. These post mortem reports should be short but professional and designed for executive consumption.

3) CSIRT Membership

Outsiders may view the CSIRT as a team of highly educated technologists. Although technical experience is a good prerequisite, there are several attributes that are needed for a successful incident team. It is important for the company’s management team to understand the needs of the CSIRT. Specific incident response training, paid time off, and membership buy in from across the company are several topics that will need to be agreed upon.

a) CSIRT Staff

One of the challenging facets of building a successful incident response team is to employ a multifaceted team. A typical team will have the following schema:

- Primary Members
Creating and Managing an Incident Response Team for a Large Company

- Technology Security Specialists
- System Administrators
- Network Engineers
- Desktop Support Specialists
- Disaster Recovery Coordinators

Secondary Members
- Inside Legal Council
- Corporate HR Specialist
- Corporate Communication Specialist
- Physical Security or Facilities Coordinator
- Management Team Sponsor

Geographically diverse companies will need to work out the combination of remote handlers with a centralized team. The primary members will be the core of the CSIRT and will work the majority of the smaller incidents. The secondary members will be expected to join the CSIRT when an event requires their expertise. A hoax email virus infection will not require the secondary members to be called into action, but payroll laptops going missing will no doubt call the entire team into action.

Interpersonal Skills

Having a wide range of skills is a high priority, but communication skills will greatly improve the reputation of the team. You may find expert security engineers that would seem to be a fit in the CSIRT except for a lack of interpersonal skills. The team members should have common sense, exhibit...
effective oral and written communication skills, show diplomacy when dealing with external groups, have the ability to follow standards and procedures, show integrity and have the willingness to continue their education.

Technical Skills

Technical skills will be important for a successful CSIRT. The primary members of the team will need to have a good amount of experience in their individual fields to effectively handle a security incident. Senior network engineers, senior system administrators, and senior security specialists will be good candidates for membership. The technical understanding provided by the experienced primary members will be needed for the large variety of incident scenarios that will be investigated.

b) CSIRT Training

Training of the CSIRT is important. Training will increase the skills of the team as new technologies are available, keep the team practiced, and educate the newest members.

Training should focus not only on forensic analysis and eradication techniques, but other general skills in communication, project management, evidence handling, team building, intruder techniques, compliancy laws, privacy laws and ethics. The team should be periodically evaluated to determine ways to expand the skills that would increase the competency of the CSIRT.

Tim Proffitt
Technical skills such as, but not limited to, firewall technologies, router and switch infrastructures, TCP/IP, Operating system installation and hardening, security event manager concepts, intrusion prevention technologies, vulnerability assessment techniques, wireless infrastructures, secure programming concepts, etc. should always be kept current.

New team members can be overwhelmed with the standards and procedures that they will be introduced to as an incident handler. In most cases, new CSIRT members will be paired with an experienced handler as a mentor. As the new team member becomes familiar with the roles of an incident handler, they can be used to draft communications, compose lessons learned reports for review, aide in research or work with evidence documentation.

c) Extensions of the CSIRT

A CSIRT, on occasion, may find that it will be unable to staff full time members. In these cases the CSIRT will need to develop good relationships with the subject matter experts needed when an incident is being investigated. The CSIRT policy can outline how outside employees can be called into service of the incident team when a set of criteria is met. You will see this situation more often for the human resources, legal council and physical facilities members. The management team should be clear on when the CSIRT can utilize these head count and what priority can be used. This standard
should be well established in advance so that these extended staff can be called into action quickly.

4) Conclusion

Using good communication skills, clear policies, professional team members and utilizing training opportunities, a company can run a successful incident response team. CSIRTs will continue to serve as an important component in supporting the management of risk and security in the business. By utilizing these passive and active phases of a CSIRT, the business will improve its security efforts across the enterprise and protect confidentiality, integrity and availability of its information systems.

5) References

CERT. Handbook for Computer Security Incident Response Teams (CSIRTs)

CERT. Defining Incident Management Processes for CSIRTs: A Work in Progress

SANS. Incident Handling Step-by-Step and Computer Crime Investigation: Book 1

National Conference of State Legislatures.
http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

http://www.microsoft.com/technet/SolutionAccelerators

Federal Bureau of Investigation
http://www.fbi.gov/contact/fo/fo.htm
Appendix A

FBI & Secret Service FIELD OFFICES

ALABAMA

Birmingham
FBI 205.326.6166/205.715.0232
1211 8th Avenue N.
Birmingham, AL 35203-2396
(US) 205.731.1144/205.731.0007
Daniel Building
15 South 20th Street, Suite 1125
Birmingham, AL 35233

Mobile
FBI 334.438.3674/251.415.3235
One St. Louis Centre
1 St. Louis Street, 3rd Floor
Mobile, AL 36602-3930
US: 334.441.5851/334.441.5250
Parkview Office Building
182 St. Francis Street
Mobile, AL 36602

Montgomery
US: 334.223.7501/334.223.7523
Colonial Financial Center
1 Commerce Street, Suite 605
Montgomery, AL 36104

ALASKA

Anchorage
FBI 907.276.4441/907.265.9599
101 East Sixth Avenue
Anchorage, AK 99501-2524
US: 907.271.5148/907.271.3727
Federal Building & U.S. Courthouse
222 West 7th Avenue, Room 559
Anchorage, AK 99513

ARIZONA

Phoenix
FBI 602.279.5511/602.650.3024
201 East Indianola Avenue, Suite 400
Phoenix, AZ 85012-2080
US: 602.640.5580/602.640.5505
3200 North Central Avenue, Suite 1450
Phoenix, AZ 85012

Tucson
US: 520.677.4300/520.677.4826
300 West Congress Street, Room 4-V
Tucson, AZ 85701

ARKANSAS

Little Rock
FBI 501.221.9100/501.228.8509
24 Shackelford West Boulevard
Little Rock, AR 72211-3755
US: 501.324.6241/501.324.6997
111 Center Street, Suite 1700
Little Rock, AR 72201-4419

CALIFORNIA

Fresno
US: 209.487.5204/559.487.5013
5200 North Palm Avenue, Suite 207
Fresno, CA 93704

Los Angeles
FBI 310.477.6565/310.996.3359
Federal Office Building
1100 Wilshire Boulevard, Suite 1700
Los Angeles, CA 90024-3672
US: 213.894.4830 213.894.2948
Royal Federal Building
255 East Temple Street, 17th Floor
Los Angeles, CA 90012

Riverside
US: 909.276.6781/909.276.6637
4371 Latham Street, Suite 203
Riverside, CA 92501

Sacramento
FBI 916.481.9110/916.977.2300
4500 Orange Grove Avenue
Sacramento, CA 95841-4205
US: 916.930.2130/916.930.2140
501 I Street, Suite 9500
Sacramento, CA 95814-2322

San Francisco
FBI 415.481.9110/415.977.2300
4500 Orange Grove Avenue
Sacramento, CA 95841-4205
US: 916.930.2130/916.930.2140
501 I Street, Suite 9500
Sacramento, CA 95814-2322

COLORADO

Colorado Springs
US: 719.633.3252/719.632.3341
212 N. Wahsatch, Room 204
Colorado Springs, CO 80903

Denver
FBI 303.629.7171/303.628.3085
1961 Stout Street, 18th Floor
Denver, CO 80202-1823
US: 303.866.1010/303.866.1934
1600 Lincoln Street
Denver, CO 80264

CONNECTICUT

New Haven
FBI 203.777.6311/203.503.5998
600 State Street
New Haven, CT 06511-6505
US: 203.865.2449/203.865.2525
265 Church Street, Suite 1201
New Haven, CT 06510

DISTRICT OF COLUMBIA

Washington, D.C.
FBI (HDQRS.)
202.278.2000/202.278.2478
601 4th Street NW
Washington, D.C. 20535-0002
1100 L Street NW, Suite 6000
Washington, D.C. 20005
US: (HDQRS.)
950 H Street NW
Washington, D.C. 20223

DELAWARE

Wilmington
US: 302.573.6198/302.573.6190
One Rodney Square
920 King Street, Suite 414
Wilmington, DE 19801

Tim Proffitt
- 28 -
## Creating and Managing an Incident Response Team for a Large Company

**FLORIDA**

- **Jacksonville**
  - FBI 904.721.1211/904.727.6242
  - 7820 Arlington Expressway
  - Jacksonville, FL 32211-7499
  - USSS 904.296.0133/904.296.0188
  - 7800 Arlington Expressway, Suite 500
  - Jacksonville, FL 32211
- **Miami**
  - FBI 305.944.9101/305.787.6538
  - 16320 NW Second Avenue
  - North Miami Beach, FL 33169-6508
  - USSS 305.629.1800/305.629.1830
  - 8375 NW 53rd Street
  - Miami, FL 33166
- **Orlando**
  - USSS 407.648.6333/407.648.6606
  - 135 West Central Boulevard, Suite 670
  - Orlando, FL 32801
- **Tallahassee**
  - USSS 850.942.9502/850.942.9503
  - 325 John Knox Road
  - Tallahassee, FL 32303
- **Tampa**
  - FBI 813.273.4566/813.272.8019
  - Federal Office Building
  - 500 Zamp Street, Room 610
  - Tampa, FL 33602-3917
  - USSS 813.228.2636/813.228.2618
  - 501 East Folk Street, Room 1101
  - Tampa, FL 33602
- **West Palm Beach**
  - USSS 561.659.0184/561.655.8484
  - 505 South Flagler Drive
  - West Palm Beach, FL 33401

**GEORGIA**

- **Albany**
  - USSS 229.430.8442/229.430.8441
  - Albany Tower
  - 235 Roosevelt Avenue, Suite 221
  - Albany, GA 31702
- **Atlanta**
  - FBI 404.679.9000/404.679.6289
  - 2635 Century Parkway Northeast, Suite 400
  - Atlanta, GA 30345-3112
  - USSS 404.331.6111/404.331.5058
  - 401 West Peachtree Street, Suite 2906
  - Atlanta, GA 31702
- **Savannah**
  - USSS 912.652.4401/912.652.4062
  - 33 Bull Street
  - Savannah, GA 31401

**HAWAII**

- **Honolulu**
  - FBI 808.566.4300/808.566.4470
  - Kahananako Federal Office Building
  - 300 Ala Moana Boulevard, Room 4-230
  - Honolulu, HI 96850-0053
  - USSS 808.541.0192/808.545.4490
  - Kahananako Federal Office Building
  - 300 Ala Moana Boulevard, Room 6-210
  - Honolulu, HI 96850

**IDAHO**

- **Boise**
  - USSS 208.334.1403/208.334.1289
  - Federal Building - U.S. Courthouse
  - 550 West First Street, Room 730
  - Boise, ID 83724-0001

**ILLINOIS**

- **Chicago**
  - FBI 312.421.4310/312.786.2525
  - E.M. Dirksen Federal Office Building
  - 219 South Dearborn Street, Room 905
  - Chicago, IL 60604-1702
  - USSS 312.353.5431/312.353.1225
  - Gateway IV Building
  - 300 S. Riverside Plaza, Suite 1200
  - North Chicago, IL 60064
  - USSS 208.334.1403/208.334.1289
  - Federal Office Building
  - 550 West Monroe Street, Suite 700
  - Springfield, IL 62704

**INDIANA**

- **Evansville**
  - USSS 812.985.9502/812.985.9504
  - P.O. Box 530
  - Newburgh, IN 47630
- **Indianapolis**
  - FBI 317.639.3301/317.321.6193
  - Federal Office Building
  - 575 John Grimes Building
  - 401 West Washington Street, Suite 1502
  - Indianapolis, IN 46202-2231
  - USSS 317.226.6444/317.226.5494
  - Federal Office Building
  - 501 Magazine Street
  - New Orleans, LA 70126

**IOWA**

- **Des Moines**
  - USSS 515.284.4565/515.284.4566
  - 210 Walnut Street, Suite 637
  - Des Moines, IA 50309-2107

**KANSAS**

- **Wichita**
  - USSS 316.269.6694/316.269.6154
  - Epic Center
  - 301 N. Main Street, Suite 275
  - Wichita, KS 67202

**KENTUCKY**

- **Lexington**
  - USSS 859.223.2358/859.223.1819
  - 3141 Beaumont Centre Circle
  - Lexington, KY 40513

**LOUISIANA**

- **Baton Rouge**
  - USSS 225.389.0763/225.389.0325
  - One American Place, Suite 1502
  - Baton Rouge, LA 70825

- **New Orleans**
  - FBI 504.816.3000/504.816.3306
  - 2901 Leon C. Simon Drive
  - New Orleans, LA 70126
  - USSS 504.589.4041/504.589.6013
  - Hale Boggs Federal Building
  - 501 Magazine Street
  - New Orleans, LA 70130

- **Shreveport**
  - USSS 318.676.3500/318.676.3502
  - 401 Edwards Street
  - Shreveport, LA 71101

**MAINE**

- **Portland**
  - USSS 207.780.3493/207.780.3301
  - 100 Middle Street
  - West Tower, 2nd Floor
  - Portland, ME 04101
Creating and Managing an Incident Response Team for a Large Company

**MARYLAND**

Baltimore  
FBI 410.265.8080/410.281.0339  
7142 Ambassador Road  
Baltimore, MD 21244-2754  
USS 410.962.2200/410.962.0840  
100 S. Charles Street, 11th Floor  
Baltimore, MD 21201  

Eastern Shore  
USS 410.268.7286/410.268.7903  
U.S. Naval Academy  
Police Dept., Headquarters Building 251  
Annapolis, MD 21402  

**MISSISSIPPI**

Jackson  
FBI 601.948.5000/601.360.7550  
Federal Building  
100 West Capitol Street  
Jackson, MS 30269-1601  
USS 601.965.4436/601.965.4012  
Federal Building  
100 West Capitol Street, Suite 840  
Jackson, MS 32929  

**MISSOURI**

Kansas City  
FBI 816.512.8200/816.512.8545  
1300 Summit  
Kansas City, MO 64105-1362  
USS 816.460.0600/816.283.0321  
1150 Grand Avenue, Suite 510  
Kansas City, MO 64106  

Springfield  
USS 417.866.8340/417.864.8676  
911 St. Louis Street, Suite 306  
Springfield, MO 65806  

St. Louis  
FBI 314.231.4324/314.589.2636  
222 Market Street  
St. Louis, MO 63103-2516  
USS 314.539.2238/314.539.2567  
Thomas F. Eagleton U.S. Courthouse  
111 S. 10th Street, Suite 31346  
St. Louis, MO 63102  

**MONTANA**

Great Falls  
USS 406.452.8515/406.761.2316  
11 Third Street North  
Great Falls, MT 59401  

**NEBRASKA**

Omaha  
FBI 402.493.8688/402.492.3799  
10755 Burt Street  
Omaha, NE 68114-2000  
USS 402.965.3670/402.445.9638  
2707 North 108 Street, Suite 301  
Omaha, NE 68164  

**NEVADA**

Las Vegas  
FBI 702.385.1281/702.385.1281  
John Lawrence Bailey Building  
700 East Charleston Boulevard  
Las Vegas, NV 89104-1545  
USS 702.388.6571/702.388.6668  
600 Las Vegas Boulevard South, Suite 600  
Las Vegas, NV 89101  

Reno  
USS 775.784.5354/775.784.5991  
100 West Liberty Street, Suite 500  
Reno, NV 89501  

**NEW HAMPSHIRE**

Manchester  
USS 603.626.5631/603.626.5653  
1750 Elm Street, Suite 802  
Manchester, NH 03104  

**NEW JERSEY**

Atlantic City  
USS 609.487.1300/609.487.1491  
Ventnor Professional Campus  
6601 Ventnor Avenue  
Ventnor City, NJ 08406  

Newark  
FBI 973.792.2000/973.792.3035  
1 Gateway Center, 22nd Floor  
Newark, NJ 07102-9899  
USS 973.656.4500/973.984.5822  
Headquarters Plaza, West Towers, Speedwell Avenue, Suite 700  
Morristown, NJ 07960  

Trenton  
USS 609.989.2008/609.989.2174  
402 East State Street, Suite 3000  
Trenton, NJ 08628  

**NEW MEXICO**

Albuquerque  
FBI 505.224.2000/505.224.2276  
415 Silver Avenue SW, Suite 300  
Albuquerque, NM 87102  
USS 505.248.5290/505.248.5296  
505 Marquette Street NW  
Albuquerque, NM 87102  

---

Tim Proffitt  
- 30 -

© SANS 2007  
As Part of the Information Security Reading Room  
Author retains full rights  

© SANS Institute 2007,  
As part of the Information Security Reading Room  
Author retains full rights.
# Creating and Managing an Incident Response Team for a Large Company

## NEW YORK

**Albany**  
FBI 518.465.7351/518.431.7463  
200 McCarty Avenue  
Albany, NY 12209  
USSS 518.436.9600/518.436.9635  
38 North Pearl Street, 2nd Floor  
Albany, NY 12207

**Buffalo**  
FBI 716.856.780/716.843.5288  
One FBI Plaza  
Buffalo, NY 14202-2698  
USSS 716.551.4401/716.551.5075  
610 Main Street, Suite 300  
Buffalo, NY 14202

**JFK**  
USSS 718.553.0911/718.553.7626  
John F. Kennedy Int’l. Airport  
Building 75, Room 246  
Jamaica, NY 11430

**Melville**  
USSS 631.249.0404/631.249.0991  
35 Pinelawn Road  
Melville, NY 11747

**New York**  
FBI 212.384.1000/212.384.2745  
or 2746  
26 Federal Plaza, 23rd Floor  
New York, NY 10278-0004  
USSS 212.637.4500/212.637.4687  
335 Adams Street, 32nd Floor  
Brooklyn, NY 11201

**Rochester**  
USSS 716.263.6830/716.454.2753  
Federal Building  
100 S. Clinton Street, Room 1371  
Rochester, NY 14615

**Syracuse**  
USSS 315.448.0304/315.448.0302  
James Hanley Federal Building  
100 S. Clinton Street, Room 1371  
Syracuse, NY 13201

**White Plains**  
USSS 914.682.6300/914.682.6182  
140 Grand Street, Suite 300  
White Plains, NY 10601

## NORTH CAROLINA

**Charlotte**  
FBI 704.377.9200/704.331.4595  
Wachovia Building  
400 South Tryon Street, Suite 900  
Charlotte, NC 28285-0001  
USSS 704.442.8370/704.442.8369  
One Fairview Center  
6302 Fairview Road  
Charlotte, NC 28210

**Greensboro**  
USSS 336.547.4180/336.547.4185  
4905 Koger Boulevard, Suite 220  
Greensboro, NC 27407

**Raleigh**  
USSS 919.790.2834/919.790.2832  
4407 Bland Road, Suite 210  
Raleigh, NC 27609

**Wilmington**  
USSS 910.815.4511/910.815.4521  
One Rodney Square  
920 King Street, Suite 414  
Wilmington, DE 19801

## NORTH DAKOTA

**Fargo**  
USSS 701.239.5070/701.239.5071  
657 2nd Avenue North, Suite 382A  
Fargo, ND 58102

## OKLAHOMA

**Oklahoma City**  
FBI 405.290.7770/405.290.3885  
3301 West Memorial Drive  
Oklahoma City, OK 73134  
USSS 405.810.3000/405.810.3098  
Lakepoint Towers  
4013 NW Expressway, Suite 650  
Oklahoma City, OK 73116

**Tulsa**  
USSS 918.581.7272  
Pratt Tower  
125 West 15th Street, Suite 400  
Tulsa, OK 74119

## OREGON

**Portland**  
FBI 503.224.4181/503.552.5400  
Crown Plaza Building  
1500 SW 1st Avenue, Suite 400  
Portland, OR 97201-5828  
USSS 503.326.2162/503.326.3258  
1001 SW 5th Avenue, Suite 1020  
Portland, OR 97204

## PENNSYLVANIA

**Philadelphia**  
FBI 215.418.4000/215.418.4232  
William J. Green Jr. Federal Office Building  
600 Arch Street, 8th Floor  
Philadelphia, PA 19106  
USSS 215.861.3300/215.861.3311  
7236 Federal Building  
600 Arch Street  
Philadelphia, PA 19106

**Pittsburgh**  
FBI 412.471.2000/412.432.4188  
U.S. Post Office Building  
700 Grant Street, Suite 300  
Pittsburgh, PA 15219-1906  
USSS 412.395.6484/412.395.6349  
1000 Liberty Avenue  
Pittsburgh, PA 15222

**Scranton**  
USSS 570.346.5781/570.346.3003  
235 N. Washington Avenue, Suite 247  
Scranton, PA 18501
## RHODE ISLAND

**Providence**  
USSS 401.331.6456/401.528.4394  
The Federal Center  
300 Westminster Street, Suite 343  
Providence, RI 02903

## SOUTH CAROLINA

**Charleston**  
USSS 843.747.7242/843.747.7787  
590 Core Avenue, Suite 500  
North Charleston, SC 29406

**Columbia**  
FBI 803.551.4200/803.551.4324  
151 Westpark Boulevard  
Columbia, SC 29210-3857

**Greenville**  
USSS 864.233.1490/864.235.6237  
7 Laurens Street, Suite 508  
Greenville, SC 29601

## SOUTH DAKOTA

**Sioux Falls**  
USSS 605.330.4565/605.330.4523  
230 South Phillips Avenue, Suite 405  
Sioux Falls, SD 57104

## TENNESSEE

**Chattanooga**  
USSS 423.752.5125/423.752.5130  
Post Office Building  
900 Georgia Avenue, Room 204  
Chattanooga, TN 37402

**Knoxville**  
FBI 865.546.0751/865.544.3590  
John J. Duncan Federal Office Building  
710 Locust Street, Suite 600  
Knoxville, TN 37902-2537

**Memphis**  
FBI 901.747.4300/901.747.9621  
Eagle Crest Building  
225 North Humphreys Boulevard, Suite 3000  
Memphis, TN 38120-2107

**Nashville**  
USSS 615.736.5841/615.736.5848  
458 U.S. Courthouse  
801 Broadway Street  
Nashville, TN 37203

## TEXAS

**Austin**  
USSS 512.916.5103/512.916.5365  
Federal Office Building  
300 E. 8th Street  
Austin, TX 78701

**Dallas**  
FBI 214.720.2200/214.922.7459  
1801 North Lamar, Suite 300  
Dallas, TX 75202-1795

**El Paso**  
FBI 915.832.5000/915.832.5259  
660 S. Mesa Hills Drive  
El Paso, TX 79912

**Houston**  
FBI 713.693.5000/713.693.3999  
2500 East TC Jester  
Houston, TX 77008-1300

**Lubbock**  
USSS 806.472.7347/806.472.7542  
1205 Texas Avenue, Room 613  
Lubbock, TX 79401

**McAllen**  
USSS 956.630.5811/956.630.5838  
200 S. 10th Street, Suite 1107  
McAllen, TX 75501

**San Antonio**  
FBI 210.225.6741/210.978.5380  
U.S. Post Office Building  
615 East Houston Street, Suite 200  
San Antonio, TX 78205-9998

**Tyler**  
USSS 903.534.2933  
903.581.9569  
6101 South Broadway, Suite 335  
Tyler, TX 75703

## UTAH

**Salt Lake City**  
FBI 801.579.1400/801.579.4500  
257 Towers Building  
257 East 200 South, Suite 1200  
Salt Lake City, UT 84111-2048

**VERMONT**  
FBI 518.465.7551/518.431.7463  
Contact field office located in  
Albany, NY  
617.565.5640/617.565.5659  
Contact field office located in  
Boston, MA

## VIRGINIA

**Norfolk**  
FBI 757.455.0100/757.455.2647  
150 Corporate Boulevard  
Norfolk, VA 23524-4999

**Richmond**  
FBI 804.261.1044/804.627.4494  
1970 East Parham Road  
Richmond, VA 23228

**Roanoke**  
USSS 540.345.4301/540.857.2151  
105 Franklin Road SW, Suite 2  
Roanoke, VA 24011

## WASHINGTON

**Seattle**  
FBI 206.622.0460/206.262.2587  
1110 Third Avenue  
Seattle, WA 98101

**Spokane**  
USSS 509.353.2246/509.353.2871  
601 W. Riverside Avenue, Suite 1340  
Spokane, WA 99201

## WEST VIRGINIA

**Charleston**  
USSS 304.347.5188/304.347.5187  
5900 Core Avenue, Suite 500  
North Charleston, SC 29406

## WISCONSIN

**Madison**  
USSS 608.264.5919/608.264.5592  
131 W. Wilson Street, Suite 303  
Madison, WI 53703

**Milwaukee**  
FBI 414.276.4684/414.276.6560  
330 East Kilbourn Avenue  
Milwaukee, WI 53202

**Richmond**  
FBI 804.261.1044/804.627.4494  
1970 East Parham Road  
Richmond, VA 23228

## WYOMING

**Cheyenne**  
USSS 307.772.2380/307.772.2387  
2120 Capitol Avenue, Suite 3026  
Cheyenne, WY 82001
Creating and Managing an Incident Response Team for a Large Company

Tim Proffitt
- 33 -
<table>
<thead>
<tr>
<th>SANS OnDemand</th>
<th>OnlineUS</th>
<th>Anytime</th>
<th>Self Paced</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>