CIRT, Through Conception Labor and Delivery

Peter Ridgley

CIRT, Through Conception Labor and Delivery

Peter Ridgley

GSEC Practical

Version 1.4b, Option 2

Submitted May 4, 2004

Abstract

The face of the Internet has changed drastically in recent years from a research network to an online transaction clearing house accessible to nearly every home in America. It is this transformation and accessibility that has given birth to a variety of conveniences as well as a new medium from malicious hackers to try out their techniques. The latter point is the one that many IT organizations are focused on defeating. The amount of malicious code available on the Internet and the relative ease with which one can access it and the systems connected to it has created a distributed model for exploitation of dizzying proportions. Dedicated corporate information security teams and a methodical process for dealing with events are one way to thwart the efforts of these evil doers.

The purpose of this case study is to show the efforts, successes and failures that a company, new to adopting a security posture, recently experienced. From the information provided here, it is my goal to provide you with an understanding of what you might face in conceiving and delivering a similar infrastructure in your environment. The focus of the study is around the creation, implementation and utilization of a Company Security Action Team (CSAT) and their direct experience with an event that called their Computer Incident Response Team (CIRT) into action. The study will show the lessons learned from this event so history does not repeat itself in your organization.

Details

Company ABC has about 5,000 employees and 6,500 computers. It has been traditionally termed a brick and mortar company with no more than a static web site presence. Today the company does host transactional services over the Internet via web portals, web services and customized web GUI front ends. The infrastructure is architected in a traditional DMZ configuration with internal, DMZ and external links protected by redundant firewalls. Rapid development of functionally rich application code, with little attention to security has set this company apart from its competitors and opened the door for exploits at the same time.

The company has recently fallen under the requirements of Sarbanes Oxley Act of 2002 (SOX), which applies "legislation affecting corporate governance, financial disclosure and public accounting practices" not seen "since the US securities laws of the early 1930s."[1] Section 404 of SOX is the section that IT organizations are most concerned with addressing. It

[1] PriceWaterhouseCoopers, "The Sarbanes Oxley Act of 2002", URL http://www.pwcglobal.com/Extweb/NewCoAtWork.nsf/docid/D0D7F79003C6D64485256CF30074D66C

states that internal controls need to be in place for all activities which occur within ones organization.

> 'The COSO Framework defined internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in three categories--effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. COSO further stated that internal control consists of: the control environment, risk assessment, control activities, information and communication, and monitoring. The scope of internal control therefore extends to policies, plans, procedures, processes, systems, activities, functions, projects, initiatives, and endeavors of all types at all levels of a company.'[2]

It is this requirement that has organized the creation of a formal security team, Company Security Action Team (CSAT). It is the responsibility of the team to ensure that policies, procedures and operational guidelines are set forth and followed in day to day business. CSAT is comprised of several technical engineers as well as members of the business, legal and corporate communications divisions.

One of the first initiatives tackled by this team was to set forth policies and procedures to mandate what is done on a daily basis and to determine how it will be completed. It was through this effort, in conjunction with the information guidelines provided in the GCC section 404 of the CoBIT framework, which initiated the need for a CIRT. Many of the members of the CIRT are also members of the security team. The CSAT charter, purpose, members and responsibilities are listed below.

Charter

> The Company Security Action Team (CSAT) is the group responsible for assessing, defining and implementing the enterprise-wide Information Security policies, procedures and guidelines for the Company. This group shall be comprised of representatives from the Information Technology and Security organizations, the business, legal counsel and corporate communications. It shall have as its executive sponsor the CIO of the Company.

Purpose

> CSAT shall be responsible for assessing the Company's Information Security posture as it relates to technology

---

[2] U.S. Securities and Exchange Commission, "Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports", URL http://www.sec.gov/rules/final/33-8238.htm#ii

applications, hardware systems, operational policies and personnel practices that are associated with the operation of the business.

- CSAT shall be responsible for creating Information Security standards, policies and procedures.
- CSAT shall be responsible for monitoring trends and developments within the world of Information Security and serve as the advisory body to the Company's senior management regarding Information Security risks, regulatory obligations and industry best practices.
- CSAT shall be responsible for assisting in accreditation efforts (Sarbanes / Trust Services)

CSAT Team Organizational Structure

Chief Security Officer

- Reports directly to the CIO and manages the overall security for the Company. This includes the physical security controls as well as the Information Security controls.

Information Security Technical Leader

- Team lead for the Information Security controls. This person manages the team of engineers responsible for the activities pertaining to the team.

Information Security Engineer

- IT Security member responsible for carrying out day to day firewall security changes or implementations.

Information Security Engineer

- Unix Systems Administrator responsible for expertise in the areas of host hardening, systems administration and forensics.

Information Security Engineer

- Windows Systems Administrator responsible for expertise in the areas of host hardening, systems administration and forensics.

Information Security Manager

- Manager of Enterprise Computing services responsible for the allocation of additional resources as needed.

Physical Security Manager

- Manager of physical controls for all assets within the corporation.

Business Liaison

- Business representative responsible for informing security team of upcoming changes or requests from the business. This person assists in putting projects on the table for action.

Project Manager

- Project Manager responsible for managing the team and its associated approved projects.

General Counsel

- Legal Counsel for all matters requiring legal consultation prior to disclosure.

Communications Manager

- Corporate Communications representative responsible for reviewing externally released documentation for completeness.

Compliance Manager

- Manager of internal audit and compliance.

After the creation of the CSAT team we needed to assess our role and define outstanding tasks to be resolved. After a meeting with our CIO the following priorities were identified.

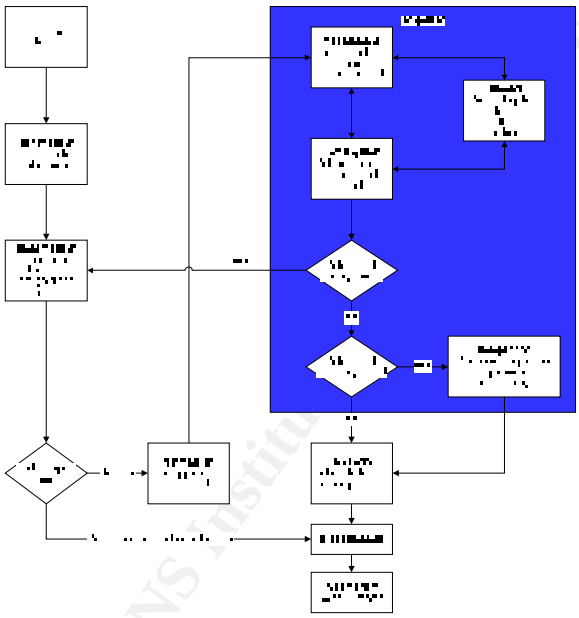
CSAT will work toward the following:

- Becoming Sarbanes Oxley accredited.
  - Review existing security policies.
  - Identifying missing / needed policies and work toward setting and implementing these.
  - Establishing a Security Awareness Program.
  - Creating a Computer Incident Response Team (CIRT).
- Defining a Communications Strategy to publicize our efforts.
- Beginning the process of Asset / Data Classification.
- Establishing guidelines for secure computing system builds.
- Evaluating current Network Infrastructure.
- Establishing centralized responses to customer audits and scans.
- Instituting a Threat Management Program

The above is an example of the first initiatives set forth for the team. The focus for this study is the formation and use of the team itself and the requirements for a CIRT. So now we have our big challenge. It is time to

build the documentation framework for a CIRT and sell this need to management. Luckily we have regulatory requirements like SOX section 404 requiring the need for this so the sale was easy. The hard part was creating the framework and trying to figure out what would work and what would not before and incident required us to learn the hard way. We knew that this team was going to have to be able to work with several other teams in order to get their job done right and efficiently. Resources would need to be pulled from other teams as event needs required. The team would need complete autonomy during an event in order to make critical decisions, potentially about business affecting systems. We wanted people with cool heads and clear thoughts that could be enabled to make decisions based on the facts before them and not the noise around them. With these basic premises we set out to create a team and the process for event handling and event escalation.

We needed to define how to identify an event process in order to create a team that could respond to it. Since many before us have worked on this we took the model set forth by Price Waterhouse Coopers.[3]



From this process flow of Event Identification, Classification, Notification, Response, Recovery and Post Mortem we were able to define what was needed in the form of a team to instantiate each of the steps in this process.

[3] PriceWaterhouseCoopers, "Information Security, A Strategic Guide for Business", PriceWaterhouseCoopers Global Technology Centre, p179-180.

Here is what we came up with for the team structure as defined by PriceWaterhouseCoopers.

CIRT Leader

This person is responsible for:

- *Coordinating and delegating the incident response effort*
- *Acting as the central point of contact for the CIRT*
- *Coordinating the relationship between CIRT and management, legal and law enforcement*
- *Reporting incidents to the appropriate business manager, senior management and the human resources department for incidents involving employees*
- *Preparing for external participation in the incident response process*

Incident Documentation Specialist

The documentation specialist is responsible for recording, documenting and organizing all information from the incident, including all intrusion and response activity. Additional responsibilities include:

- *Coordinating documentation methods for all system administrators to ensure consistency*
- *Documenting time spent on intrusions and any monetary losses for all incidents. This would include the cost to remediate the incident.*
- *Coordinating collection of system logs and records with person responsible for securing evidence*
- *Maintaining summary reports of all incidents for historical documentation*

Technical Assessment Team

These team members, primarily technical personnel, will determine the root cause of the computer security incident, the extent of the damage and the effects on systems, data and operations. This team will preserve data in a way that facilitates its use in potential legal proceedings. Responsibilities for this team include:

- *Performing technical analysis and support*
- *Performing technical tasks including all analysis of logs and collection of technical information*

- *Interpreting the technical incident*
- *Gathering technical evidence*
- *Coordinating technical efforts with system administrators*
- *Coordinating recovery efforts*

Technical Support Team

The technical support teams work with the technical assessment team to assist investigation activities. Responsibilities for these individuals include:

- *Providing access to systems and networks*
- *Providing hardware, software and peripherals such as cables, switches, taps, sniffers etc.*

Legal Counsel

Legal counsel is used in the event guidance around regulatory requirements is needed. There are also times where they may be called upon to review a press release or more often to review a policy that was identified as missing during the post mortem event process. Responsibilities of these individuals include:

- *Understanding privacy related issues as they relate to e-commerce systems on the Internet*
- *Providing guidance in preparation of communication materials, internal or external.*

Corporate Communications

Corporate Communications is responsible for the preparation of internal and external corporate press releases. Responsibilities include:

- *Drafting the public response to an event*
- *Drafting the internal response to an event*
- *Being the single point of contact for all media related communications*

CIRT External Support

This group of outside resources can be called upon when the above internal groups cannot, for whatever reason,

satisfy the requirements of their responsibilities. An example would be when additional support is needed to forensically identify an event that the internal resources have limited knowledge or skill in addressing. These members might include:

- *Local and Federal law enforcement*
- *Vendors*
- *Security consultants* [4]

Soon after the creation of the CSAT and the subsequent establishment of the CIRT, the Company hired a third party vulnerability assessment team to come in and provide an overall risk profile of the computing infrastructure. This assessment initially consisted of a penetration test of the infrastructure to provide the results necessary for a baseline of our overall security posture. The penetration test modeled specific threat scenarios against our network and its supported services. The testing imitated a malicious attacker with a specific goal (e.g., to compromise a host in our DMZ, to access our corporate databases, or break into our custom applications).

The assessment included:

1. Reviewing technical architecture including technical specifications and high-level design documentation.
2. Performing reconnaissance to develop a picture of the network, including topology, devices and hosts, and services.
3. Testing identified components to gain access to network:
   a.) Devices such as firewalls, routers, and switches
   b.) Hosts such as web, FTP, database, application, and mail servers
4. Impersonating a customer with valid credentials to determine the ability to exploit customer data as well as Company internal networks.

No sooner than 30 minutes after the commencement of the penetration test, one of the hosts on a DMZ was found to contain evidence of a previously successful exploit, granting unauthorized access to the system. Evidence of the compromise was obtained and confirmed through the vendor providing the assessment test. At this point we knew what we

[4] PriceWaterhouseCoopers, "Information Security, A Strategic Guide for Business", PriceWaterhouseCoopers Global Technology Centre, p182-183

needed to do and the CIRT documentation and related team was called into action. Here are the steps that were taken to respond to the event.

At 5:05 pm 3/25/04 the CIRT leader was notified that a system on our DMZ had been compromised. Since our team is not a full time team the CIRT leader identified a documentation specialist and then went through the process flow for incident response.

The event was identified as an unauthorized access attempt utilizing a known flaw in IIS configuration and documented as such.

The event was classified as a severity level two incident, indicating that we were incurring damage and unauthorized access to the environment was obtained.

Notification to the CIRT team members went out in the form of emails and telephone calls to cellular phones.

The response process began after all team members replied to the notification sent by the CIRT leader. Immediately we began combing the logs from the firewall and the host affected to determine the scope of the damage. We were looking to see if this host had initiated any connections either out to the Internet or inside our internal corporate network. We were not able to conclusively find any evidence that any connections were initiated from the affected host.

The total time passed at this point was over an hour. Clearly this was not going to be acceptable going forward. We were operating in a relatively disjointed manner that was indicative of panic. We needed to remember that this process was defined to eliminate the feelings of stress and panic we were all feeling.

Chain of custody was established as part of the response process by documenting the shutdown and removal of the affected system from the network and the rack that it was installed in. This was done so further forensic investigation could be accomplished on the hard drive to determine what level of access the malicious user obtained. It was decided at this time that a qualified entity should perform sector by sector disk duplication so we could perform forensics on the drives.

External support in the form of our trusted third party was called upon to perform the sector by sector disk copy so that we could do some forensics on the drives without affecting the “real” system.

The recovery process was fairly easy for this situation because the system that was compromised was a member of a cluster. We validated that the other members of the cluster were not compromised nor were they at risk of compromise and restored the system functionality.

The incident remains open while forensics is performed on the disks.

The Post Mortem for this event is where we really learned what went well and what went wrong in this process.

After the event recovery process we gathered all the resources involved in the event and took over a conference room for a period of one hour. During this time we reviewed the documentation taken from the documentation specialist. We then asked all involved for their input on the success of the process. We learned that too much time had passed from the initial notification to the commencement of the response part of the process. We attributed a large percentage of the reason for this to the simple fact that the process was still so new. Another major factor was that while the document had been handed out to all involved to read many months ago, there was no effort given around a compliance check to ensure that everyone read and understood it. The Post Mortem was showing us all the importance of continuous improvement with process feedback. It was also showing the importance of internal controls, the very reason we were creating this team in the first place! In addition to the process improvement within our own team, it was clear that internal training and awareness programs need to be made part of the curriculum for all employees. Education around patch management could have very easily eliminated this event from occurring. We decided to work with our training department to develop some online training in the form of PowerPoint presentations to start. A more formal training program is being developed and made part of the new hire program. An annual compliance check for new training sessions is being deployed to ensure that employees have read and understood the content. We would like to employ some sort of testing process to see how everyone rates on their knowledge of Security. This information will be useful in the future as we work to develop a more robust awareness program.

Another factor for the response delay is that many were slow to respond because we live in a very dynamic environment and far too often an emergency is called when there really isn't one. Our conditioned response to the page was, it was some sort of false alarm and, like the others before it, would go away given a few minutes. In order to combat this conditioned response, we assured all members that whenever they receive notification from the CSAT team there is in fact an incident and they are empowered to drop whatever they are doing to respond. We also made it known that a lack of response to an incident without good reason would reflect on

performance during employee evaluation periods. Senior management had already signed off on these points and it was now expected of them for being members of this team. To try and ward off the feelings of expectations that some were uncomfortable with we also made it known that responsibilities would be rotated on a quarterly basis to give all members a chance to see how all aspects of the team operated. This creates a well rounded team and serves to fill gaps when resources are out due to illness or vacation.

After discussing the time delay to respond we moved into the actual response process. What we learned initially was that in combing through system logs and firewall logs, our archival process did not allow for sufficient backlog to review. Our logs were being rotated every 30 days. In examining these logs we did not see any evidence of the compromise. This is probably true because the system was compromised more than 30 days ago. This discovery gave way to a budgeted Event Correlation project that has the capacity to store, normalize and report on events for a period of 120 days from disparate systems. These systems include devices like switches and routers, hosts, firewalls and Intrusion Detection Systems (IDS).

Another very significant point that was discovered was the systems compromised were not synchronizing with a time server and actually had an incorrect time zone configured on the system clock. This made it virtually impossible to correlate any system logs with logs on other systems. We immediately opened a change control ticket for a firewall change that would allow certain systems to synchronize with external time servers. We then opened up another ticket to configure all the systems to pull time from the designated ntp servers.

We also learned that beyond combing through logs and looking for the obvious we lacked the internal expertise to perform some true forensic analysis. Training became a very hot topic during the Post Mortem exercise. We decided to raise this topic with senior management.
Several policy based ideas came to light out of the Post Mortem as well. We learned that it was imperative that we receive a signed declaration from the CIO granting us the ability to scan our environment for vulnerabilities. In addition to this policy we decided we needed to draft a similar policy which requires a system to be scanned for vulnerabilities prior to receiving an IP address anywhere on the Production network. Yet another policy spoke about mandating that DMZ servers be at a certain level of Operating System. In our example we stated that all Windows servers in the DMZ must be at Windows 2000 or above and patched with all available released patches from Microsoft. Another similar policy was drafted for the Linux Operating Systems.

In conjunction with the Operating System minimum level configuration, we appointed the CIRT leader as the central point of contact for all notifications of vulnerabilities from SANS, CERT, etc. It is the CIRT leader's responsibility to notify the appropriate resources of the vulnerability and to have a task entered into the task management system to ensure the completion of the remediation effort. In the event the resource can't be located, the Help Desk is notified and takes the call from there. The theme here is that we were not doing enough proactive maintenance and assessment of the network and its associated hosts to help ward off exploit attempts in our environment.

Conclusion

In summary, the bulk of what we've learned during the Post Mortem was, we were not doing enough proactive maintenance on the network and systems to help prevent an event from occurring. A formal vulnerability alert process needed to be defined and incorporated into a proper Patch Management Process. Proper training is lacking from our security diet as are the policies that enable us to perform the work necessary in order to secure our environment. Logs of historical information were not being retained for a long enough periods. There was no system in place for timely log review and alerting of anomalistic conditions. Time was not synchronized across the Enterprise devices and systems. All of these points were addressed either through immediate action or through raising the issues to senior management in a way they could understand, ROI: Risk of Incarceration!

Thanks in part to legal pressure in the form of SOX, as well as customer requirements for accreditation efforts like Trust Services, we now have an established and working security team. The team continues to focus on keeping things simple and methodical while maintaining an eye on proactive maintnenance. Focus on process improvement through continuous feedback is the only way we found to effectively manage our failures and turn them into future successes. Good luck and make sure to request the epidural. The labor will be long and painful, but the end result will make you proud and better able to deal with the pressures that arise as events mature.

References

PriceWaterhouseCoopers, “The Sarbanes Oxley Act of 2002”, URL http://www.pwcglobal.com/Extweb/NewCoAtWork.nsf/docid/D0D7F79003C6D64485256CF30074D66C

U.S. Securities and Exchange Commission, “Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports”, URL http://www.sec.gov/rules/final/33-8238.htm#ii

PriceWaterhouseCoopers, “Information Security, A Strategic Guide for Business”, PriceWaterhouseCoopers Global Technology Centre

Carnegie Mellon Software Engineering Institute, “Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)”, URL http://www.cert.org/csirts/csirt_faq.html

Carnegie Mellon software Engineering Institute, “Handbook for Computer Security Incident Response Teams (CSIRTs), URL http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.pdf

U.S. Department of Homeland Security, “Incident Handling Checklists”, URL http://www.fedcirc.gov/incidentResponse/IHchecklists.html