CERT | Software Engineering Institute
Carnegie Mellon University

FINANCIAL INSTITUTION CSIRT CASE STUDY

It is a simple fact that the number of computer and software vulnerabilities is growing and the sophistication of attacks is increasing. Organizations need to develop a comprehensive plan to secure sensitive information and ensure the survivability of their critical infrastructure.

The purpose of this document is to share lessons learned by a financial institution (referred to in this document as AFI) as it developed and implemented both a plan to address security concerns and a Computer Security Incident Response Team (CSIRT).

Background Environment

AFI is one of the largest banks in a country with a global network of affiliate organizations. Their products and services cover the entire financial range—from traditional consumer banking and investment services to insurance and corporate investment banking. While this set of services, products, and customers are diverse, AFI's approach to security must be carefully coordinated across all business units to provide a consistent, repeatable process.

A problem facing AFI was that each of its business units had its own vision of how security measures would be implemented to protect its resources. As AFI acquired more companies and increased the number of service offerings, it became more critical that a standard set of repeatable processes were in place to deal with security incidents.

Senior management within AFI recognized that, to be successful in the financial industry, they must have a clear understanding of its security risks and be able to identify solutions to eliminate, mitigate, or minimize any potential threats to it organization. In the fall of 2000, AFI published and distributed its security architecture plan for infrastructure security on its internal website. This activity helped AFI articulate a direction for its information security needs.

Grassroots Effort

A newly-hired Information Security Manager saw that security incidents were occurring, and although they were being addressed, they were being handled inconsistently across the AFI organization. He recognized that a consistent incident response system needed to be implemented. The manager sought out industry best practices for approaches to build an effective incident response capability that would meet the needs of AFI's widely distributed environment. He reviewed information, such as the Software Engineering Institute's *Handbook for Computer Security Incident Response Teams (CSIRTs)* and the SANS Computer Security Incident Handling: Step-by-Step guide for guidance on how to structure an incident response management plan. The goal was to build a repeatable process based on existing best practices used in the incident handling arena.

The Information Security Manager, with management backing, began building support with key functional areas and other stakeholders, such as Information Security, Audit, Public Relations, and Risk groups. Early on, these groups collectively recognized the critical importance and value of implementing a CSIRT within AFI. A CSIRT would provide services and support to prevent and respond to computer security incidents. It would also mitigate risk, and (at least indirectly) improve the brand image of AFI's name across all the business units by quickly detecting and responding to computer security events before they potentially became public knowledge and damaged AFI's reputation.

In addition to building support across different functional units, a core group of technical and managerial personnel attended CERT/CC courses at the Software Engineering Institute on creating and managing CSIRTs, as well as an introductory course on incident handling.

As stated earlier, security events can happen at any time. Some notable security events include: the Melissa virus, which took several days to spread; the "Love Letter" worm, which became rampant in just a day; and the Nimda worm, which wreaked havoc in just hours. These incidents show that little time is needed to infect systems around the world, and a company must therefore have the capability to respond quickly to prevent major losses and interruptions in service.

For regulated businesses such as banking and health care, governments are enacting laws that require businesses to provide mechanisms for protecting consumer data and privacy. A functional CSIRT is one component of a comprehensive security plan that will help organizations mitigate the risk of exposure due to a security event, thereby protecting consumer privacy and data.

In every incident, there will be a cost to the organization. The question is how much that cost will be. If caught early, the cost can be minimal. However, if an incident continues undetected for a long period of time, the cost can be extremely high. To identify the total cost of an incident, the manager has to not only calculate the direct costs of manpower, equipment, and lost production time, but also determine other indirect costs, such as the potential cost of lost business and damage to the company's reputation and brand image.

Armed with support from key stakeholders, knowledge of best practices currently being used in incident management, an understanding of the current and potential threats to AFI, and a vision and plan for implementing a CSIRT, it was time to make the business case to the Chief Technology Officer (CTO) to finalize plans for funding and staffing an operational CSIRT. The arguments included facts about security threats and events that had already occurred within AFI, pending government regulations, and the costs of attacks.

Planning and Designing the Implementation of a CSIRT

With a resource commitment from the CTO, AFI was ready to start the process of planning and designing their CSIRT. One of AFI's first actions was to hire a full-time CSIRT manager and assign him the responsibility and authority to further develop a CSIRT strategic plan. The CSIRT manager had several tasks ahead of him, beginning with documenting the mission, vision, and goals of the CSIRT. Some of the other tasks included

- determining and defining the CSIRT reporting structure, authority, and organizational model
- determining the range and levels of service the CSIRT would provide
- identifying and procuring personnel, equipment, and infrastructure requirements for the CSIRT
- identifying and utilizing existing information security technical staff and resources to support the CSIRT activities (when needed)
- developing the CSIRT policies and procedures (and ensuring they align with AFI's existing policies, procedures, and regulations)
- identifying CSIRT points of contacts within all of the AFI affiliate organizations

Organizationally, AFI's CSIRT staffing structure consists of a full-time CSIRT manager, core team members, several subject matter experts (extended team), and representatives from international affiliates (distributed teams). The manager and core team members are responsible for the day-to-day operation of the core team and for coordinating CSIRT efforts across all the business units and functional areas within AFI.

The CSIRT manager has agreements in place with the supervisors in the technology department that when there is an incident, they will temporarily assign the needed subject matter experts without question to the CSIRT. These agreements and commitments further demonstrate the importance that AFI has placed upon the CSIRT, and ensure that the impact of incidents on AFI can be minimized.

The security managers at the affiliate organizations are responsible for implementation issues at their locations. However, they are required to follow AFI's CSIRT policies and processes and to report incident activity to the core team at AFI's headquarters. AFI's core team monitors the activities at all of the affiliate sites. This enables them to identify potential problems at one site and disseminate information or guidance to all of the other security managers, so they can assess and address any real or potential threats that may arise proactively and quickly. Managing a decentralized process where the extended and distributed team members do not directly report to the CSIRT manager is a challenge that AFI recognized it would need to face. Conflicting priorities between the CSIRT manager and a direct supervisor would make it difficult to get tasks done in a timely manner. In order to resolve this and to provide senior managers with regular updates, AFI established an Information Security Committee comprised of senior managers from each affiliate organization.

This governing body is chartered to provide oversight, resolve conflicts, and ensure that necessary actions are completed in a timely manner. This committee meets on a regular basis.

In addition to developing the organizational structure of the CSIRT, the CSIRT team also developed a handbook that documented the basic requirements and processes they would follow when an incident occurred. The CSIRT handbook was based on industry best practices, tailored to meet the specific needs of AFI. The handbook also addresses issues such as incident response processes, data handling, incident reporting, skills and training requirements, and communication with other functional areas.

Going Operational

Getting a CSIRT ready to become operational requires a large amount of planning, coordination, and communication. To build consensus and understanding for their CSIRT operations early in the development process, all CSIRT team members received formal CSIRT management and/or technical training classes from the CERT/CC and SANS. Team members also held face-to-face brainstorming sessions, which were used to discuss differences in operating procedures and to walk through incident scenarios. The benefits of such discussions helped to identify processes and/or issues that needed to be addressed. For example, during one of these sessions, the team identified a process they originally thought was straightforward and easy to accomplish, but through these sessions, determined that the process would not work as planned. Recognizing and resolving such issues will improve the ability of the CSIRT to successfully complete its mission and goals for the constituency.

In addition to the brainstorming sessions, the CSIRT staff (both core and extended members) held teleconferences at least monthly to discuss progress and raise any other issues that needed to be addressed or resolved in planning and implementing the CSIRT. (Any issues that could not be resolved in these meetings were escalated to the Information Security Committee for guidance and assistance in resolving.)

As the official operational date for the CSIRT approached, it was critical that AFI's constituents understood the purpose and role of the CSIRT. In addition, AFI's constituency also needed to understand how to interact with the CSIRT. To ensure the widest possible coverage, AFI's Corporate Communications office assisted the CSIRT in publicizing the team to the constituency through a variety of methods: CSIRT activities were highlighted in several of the company-wide magazines, on their intranet, and through meeting forums with AFI business units. Additionally, all virus alerts and security patches are distributed under a CSIRT label to help make the team more visible to the constituents.

If I Knew Then What I Know Now...

The CSIRT is operational, and the constituents are starting to report incidents to them. That was the goal from the beginning. When asked, "What would you do differently if you had to do it all over again?" AFI's Security and CSIRT Manager identified a few key things they learned through this process.

- **Full-time vs. Part-time**: During the initial phases, there were only one or two people working part-time on the CSIRT development. AFI recognized that the development of a CSIRT needs full-time attention. When working on something like this part-time, it is too easy to be pulled away by other priorities. By dedicating someone to the task full-time, a company shows that it is committed to taking the concept of a corporate CSIRT and turning it into a reality.

- **Don't underestimate the task**: When first starting out, it is easy to underestimate the amount of time required to gather support, develop relationships, and create and implement the processes. If possible, partner with another organization that has developed a CSIRT before. Their advice and guidance can help to provide progress checks along the way.
- **Communication**: This may be the most critical factor in determining if the CSIRT is a success or not. Setting expectations up front and communicating progress with supervisors, team members, peers and constituents are of utmost importance. Supervisors need to understand the challenges and rewards so they can continue to justify the assigned resources. Team members can get discouraged if they don't feel like they are making progress. Peers need to understand the value of the service and what is expected from them. Constituents need to know what services are available, when they can expect to receive them, and for which situations they can receive services. From start to finish, it can easily take one-and-a-half to two years to develop and implement a successful CSIRT in a large international organization.
- **Develop Checklists**: In the early stages of planning, AFI developed their processes and handbook based on research they conducted about best practices used by other organizations, the CERT/CC "Handbook for Computer Security Incident Response Teams (CSIRTs)" and the SANS "Computer Security Incident Handling: Step-by-Step" guide. Even with all this research, it was still difficult at times to discern between what was required and what was optional. The CERT CSIRT Development Team developed a pilot set of basic requirements1 for a CSIRT and provided this to AFI. This guidance helped AFI to streamline their development efforts and focus on the required elements first and the optional elements as time allowed.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0004354