Global Information Assurance Certification Paper

Thomas A. Ambrosi
GSEC Practical Assignment V4.1b
"Lessons Learned during the Handling of the SQL Slammer Worm"
August 14, 2003

Abstract

While computer and network systems are becoming ever more complex and interconnected, security risks to these systems and the information they store, process and transmit have increased dramatically as well. Many systems still do not have adequate safeguards or security controls to protect against today's information security threats. As reported by the CERT Coordination Center® (CERT/CC) at Carnegie Mellon University, the number of reported computer and network security incidents has risen steadily since the CERT/CC was founded in 1988. The most dramatic increases have come in the last several years, when the number of reported incidents grew from 3,734 in 1998 to 82,094 in 2002 (4). If current trends continue, with 76,404 incidents reported for the 1st half of this year, 2003 will see nearly double the number of CERT/CC incidents reported in 2002. Because of the ever increasing threats associated with information technology infrastructures, organizations need a timely and effective approach to handling computer and network security incidents.

No matter how well an organization protects against information security related incidents, sooner or later that organization will find itself in the situation of needing to deal with one. This is particularly true of today's university computing and network environments. At many universities, system and network development and administration tend to be decentralized or even fragmented, and not all of those responsible for system and network administration are well trained for these job duties. Many people in system or network administrator roles are still taking on these roles as additional or part time duties. In this environment, they cannot devote the time and attention needed to properly administer the systems for which they are responsible, let alone take the time to obtain the appropriate training.

This paper presents some lessons learned from the handling of one particular incident (the SQL Slammer Worm) at a major university, from the initial indications that there was a problem, through problem resolution and documentation of lessons learned. These lessons, along with publicly available information on establishing and handling computer and network security incidents, are used to present some recommendations for improving plans and procedures for handling computer and network security related incidents. Establishing a program to appropriately respond to information security incidents and emergencies is extremely important for these issues to be efficiently and effectively resolved, if not prevented from happening in the first place.

Background

A major incident can cripple the information technology infrastructure of an organization as we have seen many times over the past two years. The year 2001 brought some of the nastiest worms that had been seen up until that time with the release of Code Red, Code Red II, and Nimda. In 2002 we saw the introduction of Klez, SQLSnake, and Slapper. In January of 2003, the SQL Slammer Worm spread voraciously across the Internet (16). To date, we have been relatively lucky in the sense that these worms could have inflicted much more damage than was actually caused. Although these worms have spread from system to system at an extremely rapid pace, they have by and large only consumed available bandwidth and processing cycles. Even so, the ability to respond appropriately when incidents such as these occur is critical, and even more so when incidents are of a more malicious nature.

Universities have some unique challenges in dealing with information security issues. Actions that would normally be taken to prevent or mitigate computer and network security threats are generally at odds with the traditional university philosophy of academic freedom and independence. In this environment, implementing any technology restrictions at all would be considered unacceptable by a significant portion of the university community. With an increased threat to information technology assets and also a myriad of federal and state laws, regulations, policies and standards to comply with, most universities have been scrambling to catch up.

In addition, universities are having to deal with increasing budget constraints, if not reductions. Technology must compete with academic programs and building projects for available funding. Technology generally does not get the same attention as these other programs, and information security is often down the priority list when it comes to dollars available for information technology projects. All these things taken as a whole make information security a very challenging endeavor in today's university environments. Approaches to dealing with these challenges will vary from one university to the next. This rest of this paper describes how one particular university is dealing with information security issues, and specifically, this University's handling of the SQL Slammer Worm.

In response to increasing computer and network security threats to University assets, a University-wide committee had been established to deal exclusively with computer and network security related issues. This committee is part of a larger organizational structure whose purpose is to discuss and deal with technology issues University-wide. Through this organizational structure, information security issues are discussed and dealt with on an ongoing basis. On a recommendation by this committee, the University decided to hire an Information Security Coordinator to form an Information Security Group and establish an Information Security Program. The Information Security Coordinator would have direct access to the Vice President of Information Systems, who would ultimately be responsible for information technology security issues.

As the newly hired Information Security Coordinator, I had been on the job less than one month when the SQL Slammer Worm was released. Although in the process of being established, there was not yet a University-wide Information Security Group, and there was no formalized incident response plan. There were, however established call lists and escalation procedures. There were also various network and system administrators throughout the University responsible for computer and network security of their own colleges or departments.

SQL Slammer was released Friday evening, January 24. By Saturday morning, the IT support staff was notified of a possible problem with the Internet Service Provider (ISP) providing Internet access for the University. It was also reported that the ISP was filtering SQL ports due to an SQL worm that was spreading over the Internet. Since there had been recent problems with ISP outages, it was initially assumed that this was why the network appeared to be down or sluggish.

It became apparent that there was a more serious problem when initial attempts by IT support staff to access University system and network devices were unsuccessful. When a member of the IT support staff was finally successful in connecting to the University network, it was noticed that there was a high rate of packet loss within the network itself. Upon taking a closer look at the problem and analyzing the traffic levels over the various University network segments, it was discovered that the high traffic levels were being generated locally on the internal network. It was decided to disable network feeds to various buildings that had been carrying enormous amounts of traffic. After disabling the major building feeds across the University, the network traffic levels appeared to be back down to more normal levels. Computers that seemed to be infected with the SQL Slammer Worm (i.e., those that were generating large amounts of traffic) were located and either shutdown or disconnected from the network. The eradication and recovery process for each of the infected machines took place over the next few days.

Analysis

There were certainly parts of the process that had taken place in the University's response to the SQL Slammer Worm that were handled well and those that could have been handled more effectively and efficiently. The rest of this paper will consider the steps in the incident handling process, present some of the issues and lessons learned during the University's handling of the SQL Slammer Worm, and provide recommendations for improving the incident response and handling procedures for future computer and network security related incidents.

One of the most definitive guides on computer security incident handling is the "Computer Security Incident Handling Step by Step" published by the SANS Institute (13). In this guide, the SANS Institute has outlined a six step process for handling computer security incidents: preparation, identification, containment, eradication, recovery, and follow-up. The process outlined by SANS has become the defacto

standard for handling computer and network security related incidents, and this paper will consider these six steps as a guide to walk through the incident handling process.

Step 1: Preparation

The first step, and arguably the most important, in this six step process is preparation. Obviously, the best way to prepare for any incident is to prevent it from happening in the first place. Up front preparation is critical to help prevent, reduce the number of, and limit the impact of cyber security related incidents or emergencies. Could the University have been better prepared when the SQL Slammer Worm was released? Certainly. If the University had practiced defense-in-depth strategies, and all systems were configured securely, were up-to-date with system patches, and were managed by well trained, skilled, and vigilant administrators, the impact on the University would not have been as great, and the University-wide network outage most likely would not have happened. But this is not likely to be the case in traditional university environments, where open systems and networks and limited resources are the norm, and there are generally not enough well trained system and network administrators to fully staff university requirements.

In this environment, how can a university implement an effective incident response plan? One answer is to prepare before an incident occurs. There is always going to be a reactive side to incident response, but one of the objectives should be to take a proactive approach. Incorporating a proactive capability to defend systems and networks into the incident response plan will ultimately reduce the number of incidents that will be encountered and therefore help reduce organizational risk. By taking a proactive stance and establishing formalized incident response plans and procedures, less time and resources will be required to respond to incidents, leaving more time that can be devoted to taking the necessary steps to protect system and network infrastructures.

The first issue that surfaced during the University's handling of the SQL Slammer incident was the fact that there was no formalized incident response plan in place, and existing call lists of system and network support personnel were not up-to-date. Developing and formalizing incident response plans and procedures should be one of the first items to accomplish. This would include clearly defining goals, capabilities, and the constituency that will be served. Successful handling of computer and network security related incidents requires an organizational approach and should reflect the business strategy of the university. The scope, depth, and breadth of the response should be considered (14). With limited resources, you will need to optimally deploy the resources under your control and leverage other resources where you can. Try not to take on more than you can handle with the resources you have available.

Gaining support and cooperation of the entire organization, from executive level management all the way down to the constituency being served is critical. Universities are generally overseen by shared governing bodies and committee structures. Decision making processes are deliberate, and universities tend to be slow to adopt and

implement change. Nothing is changed in this environment without working within and gaining consensus through these organizational structures. There is a lot of coordination and communication that needs to take place, and without this support and cooperation, successful handling of computer and network security related incidents in a timely and effective manner will be extremely difficult, if not impossible.

A second issue that arose during the handling of the SQL Slammer incident was that there did not seem to be a single person in charge of handling the incident. One of the key steps in managing any crisis is to take charge quickly (8). As part of the incident response plan, a central point of contact should be identified to lead and coordinate future incident handling efforts. This person should be in charge of setting up a central command and communication center for coordination of the incident handling activities. Although SANS places the task of assigning a person to be responsible for the incident in the identification phase, I am also bringing it up here to make sure that a procedure for identifying the person who will be in charge of the incident is in place before the next incident occurs (13).

In addition to coordinating the technical tasks of the incident response activity (e.g., identification, containment, eradication, and recovery activities), this person would also coordinate the receipt and dissemination of information pertaining to the incident and communication with other organizations. Proper communication is important to ensure that the information made available to various groups remains up to date and consistent throughout the incident handling process. Information will need to be communicated to management, help desks, operations staff, system and network administrators, the constituency, the media, incident response team members, and possibly law enforcement. Different levels of information will need to be communicated to different groups of people. At most universities, the central command and communication center would most likely be the Network Operations Center (NOC), or equivalent group responsible for monitoring system and network activities. The NOC would be an ideal place to set up an incident command center. It is generally a 24x7 operation and would already have the necessary network and telecommunications connectivity in place.

A third issue in responding to SQL Slammer was the delay in notification of IT support staff. It was Saturday morning before anyone on the University IT call list was notified that there was a problem, even though the SQL Slammer activity had started Friday evening. Another important aspect of being prepared is timely detection and notification of potential problems. To be prepared to identify anomalies, you need to understand how your systems and networks behave under normal conditions. You need to know your system and network configurations, what processes are running on your systems, what normal system loads are like, what network connections typically exist, and what normal traffic volumes and patterns look like. Planning ahead by benchmarking usage patterns and establishing alert thresholds for out of bounds activities will enable potential problems to be detected and dealt with before they reach crisis mode.

A fourth issue that came up during the process of identifying and shutting down compromised University systems was locating and notifying the responsible

administrators. For some systems, there were no responsible administrators available. The responsible administrator was either on vacation with no backup, or in some cases, there was simply no responsible person designated to administer and maintain these systems. As part of the preparation and planning process, it is important to develop a comprehensive list of responsible system and network administrators. Make sure that every system under your purview is assigned a responsible administrator. This will not be an easy task. You will most likely be asking to place heavier workloads on resources that you do not directly control. In many cases, system and network staffing is one deep, with no provisions for a backup when administrators are out of the office or unavailable. Inter-departmental agreements or agreements between system administrators could be established to provide back up coverage in cases of emergencies. This information will need to be communicated to the operations staff or equivalent group responsible for incident notification. It is also important to make every attempt to inform the responsible administrators through established communication channels before service is cut off to a portion of their systems or network. Make sure to find ways to keep the constituency informed and up to date on the status of the situation. Have a plan for keeping help desks informed and trouble hotlines current.

The fifth and last point I would like to mention is to know your critical assets and systems. In cases where there are multiple, simultaneous incidents, or a single incident spanning a large number of systems, priorities will need to be set for which systems to respond to and recover first. Although incident prioritization will actually be accomplished during the identification phase, it is also listed here because the criteria for determining the priority of an incident should be defined ahead of time. Factors such as legal issues, university image and perception, safety of university assets, and potential impact on the university should be considered (1).

There are certainly many more aspects to consider in the preparation phase, and there are many available sources providing this information, some of which are (6) (9) (13) (20) and (21). It is important to have established incident response plans and procedures in place, as well as properly trained personnel, so when incidents do occur, these procedures can be followed. In this way, incidents will not necessarily escalate into a crisis.

Step 2: Identification

The second step in the SANS six step process (13) is to determine if an incident has occurred, and if so, to identify and assess the incident. Not every system or network event or anomaly should be considered a security incident. During the preparation phase, what constitutes an incident should already have been defined. A possible definition of an incident might be behavior that is contrary to what is normally considered acceptable or behavior that is in violation of university IT security policies (5) (15). What might be a security incident for one organization might not be a security incident for another. Once it has been determined that an incident has indeed occurred, the incident should be accurately identified and assessed (e.g., source, target, severity,

and impact). Incident prioritization should be accomplished here according to the criteria defined in the preparation phase.

After the University network operations staff initially detected the incident, the first issue that was encountered during the identification phase was the delay in identifying what was generating all the network traffic. This failure happened for a number of reasons, one of which was that by the time the incident was detected, the University network was already saturated, and it was almost irrelevant why the traffic was being generated. What was important at this stage was locating where the traffic was coming from (e.g., from which systems, network segments, and buildings) and regaining control of the network. Network feeds to the University backbone network from various buildings began to be disabled. After disabling the major building feeds, network traffic levels were back down to more normal levels.

The delay in identifying this incident as the SQL Slammer Worm also resulted from a combination of not having a single person in charge of handling the incident and not having an Information Security Group as part of the process. The importance of identifying the person to be in charge was already discussed in the preparation phase. Because the University did not have a single person in charge with the authority to make decisions, this phase of the incident handling process did not proceed as efficiently as it could have. For example, many actions were taking place simultaneously, some of which conflicted with others. Additionally, there were substantial delays in incident identification and the actions taken to restore the network back to normal traffic levels. It is important that the person in charge of handling the incident have the authority to make the necessary decisions and take the appropriate actions to properly respond to the incident. And because there was not yet an established Information Security Group, existing IT staff who dealt with security issues were not involved in the process until it was too late. Some of the University systems infected with the SQL Slammer Worm could have been identified relatively quickly via existing University incident reporting mechanisms (e.g., abuse@institution.edu). As a result, the incident was not properly identified as the SQL Slammer Worm for several hours, but at that point, accurate identification was academic.

Earlier detection of the incident and notification of the proper personnel possibly could have led to a more timely and effective identification and assessment of the incident. This might have led to actions that could have lessened the impact of SQL Slammer on the University network. Because of recent problems with the University's ISP, it was assumed that the ISP was the cause of the network problems, even though there was information that the ISP was filtering SQL ports in response to a SQL worm. In order to aid in the incident identification process, the network operations staff could have made use of other sources. If internet connectivity is available, there are a number of public websites that could aid in incident verification, including various Computer Emergency Response Teams (2) (3), information on the latest viruses and worms (17) (19) (22), threat and vulnerability websites (10) (11), and a number of Federal Government websites. Calls to other nearby or regional organizations can be made to see if they are

experiencing similar problems. A 24-hour cable news service can also be installed in the NOC so current (or breaking news) is available to the network operations staff.

Step 3: Containment

The objective of the containment phase is to limit the scope and impact of the incident, whether you are limiting the damage on one system or stopping the damage from spreading to other systems or networks. It is important to have the necessary agreements and mechanisms in place prior to an incident occurring for communicating with system and network administrators, management, your Internet Service Provider, and other local or regional organizations. Criteria should be defined in advance for deciding when it is necessary to disconnect a system from the network and shut down a particular system, network segment, or port. In any case, in deciding on which action to take, the least disruptive action should be strongly considered.

The information collected during the identification phase should be used to decide what actions to take next. This will depend on what the current circumstances are. The potential impact of these actions on other systems, users, customers, and help desks will need to be considered. If at all possible, notify system and network administrators and the portion of the constituency that are going to be affected before any action is taken. Local system and network administrators can help by notifying their users of the problems and the actions being taken. Notifying users ahead of time can also have the added benefit of reducing the number of incoming calls to the help desk and the NOC.

Shutting off network traffic to all major University buildings was a pretty drastic action to take, but because SQL Slammer was released over a weekend, it was an easier decision to make. What if SQL Slammer had been released during business hours when University classes were in session and critical University business functions were being conducted? Would it have been prudent to have made the same decision? One of the objectives during the containment phase is to prevent continued intruder access and regain control of the network. Could there have been a less disruptive action to take while still containing the incident? One possible action could have been to block the MS SQL ports (incoming and outgoing) at the perimeter of the network and at each of the backbone switches feeding the University buildings where systems were infected. In this way, the incident could have been contained, and University business critical functions (and access to those functions) would still be allowed to operate, as long as they did not require access to MS SQL services.

One of the most difficult tasks during the eradication phase was locating and disconnecting all the individual systems that were infected with the SQL Slammer Worm. If system administrators of affected systems are notified in a timely manner, they can help locate and disconnect infected systems from their respective areas of responsibility. In this way, expertise across the University can be leveraged to help resolve problems, and central IT personnel will not need to be dispatched to various University buildings trying to hunt down and disconnect infected systems or the network ports to which they are connected. Local system administrators are also more familiar

with their areas of responsibility and will be able to accomplish this in a more efficient manner. By having the central IT staff work together with system administrators of other University departments, problems can be contained in a more efficient and effective way, with less impact to the constituency being served.

Step 4: Eradication

The goal of the eradication phase is to determine how the attack was carried out and to eliminate (or at least mitigate) the vulnerability that allowed the incident to occur. In the case of SQL Slammer, it is relatively straight forward to understand how the attack was carried out and to identify the vulnerabilities that allowed SQL Slammer to infect University systems and networks (12).

One vulnerability that SQL Slammer exploited was the lack of filtering, or controlling access to SQL traffic, at the perimeter of the University network. Universities have traditionally been open environments with little or no filtering at the network perimeter. The first layer of defense (the network perimeter) was nonexistent, with virtually no security controls implemented at the network layer. Computer security controls had traditionally been concentrated on individual servers and workstations. If mechanisms for controlling access to SQL traffic had been implemented at the University network perimeter, the chances for being infected with SQL Slammer would have been greatly reduced. At the very least, if University systems were infected, the list of possible sources of the infection would have been a very small number, and the subsequent impact would not have been as great.

Another vulnerability exploited by SQL Slammer was the fact that many systems were not current with patches. New systems are added to the network on a regular basis, and systems that are current with patches today might not be up-to-date tomorrow. There were many Microsoft SQL servers in operation that were not up-to-date with patches, and many administrators whose systems were infected with SQL Slammer did not realize there were instances of SQL server installed on their systems (e.g., instances of MS SQL installed with MSDE). Also, not having a program in place to regularly scan for vulnerabilities on University systems helped contribute to the large number of systems that became infected with SQL Slammer. Systems and networks are dynamic entities, particularly in university environments, so it is important to regularly scan systems for vulnerabilities. Knowing what is installed on your systems and establishing a program of regular vulnerability scanning could help identify potentially vulnerable systems before they are compromised.

Step 5: Recovery

The goal of the recovery phase is a simple one: to recover systems to their fully operational state. Procedures for restoring systems and criteria for prioritizing which systems to restore and bring back online first already should have been defined in the preparation phase.

Once the SQL Slammer infected systems were located and disconnected from the network, the next step was making sure those systems were patched, clean, and secure before they were placed back on the network. In the case of SQL Slammer infected systems, what was required was application of the patch distributed by Microsoft and verification that the patch was installed correctly. After a patch has been correctly installed, it is still a good idea to scan the patched system for additional vulnerabilities, worms, viruses, and trojan horses.

One issue that arose during the recovery phase was the varied expertise of the system administrators across the University. The ability to verify that patches were installed correctly and to scan for existing vulnerabilities varied from administrator to administrator. Also, the available tools (and the expertise to use them) for system administrators to scan for existing vulnerabilities and other malicious code were inconsistent across the University. This can be addressed through training. CDs containing tools for forensics analysis, port scanners, and vulnerability scanners can be developed and distributed. There are times you will not be able to trust the output of the tools that are being used on live systems. A CD of known good binaries for basic system tools (e.g., who, lastcomm, netstat, nbtstat, ps, ls, vmstat, and iostat) should be developed (18). Training sessions can be held on the various tools and how to use them. Training can also be provided on how to validate restored systems and monitor systems for the occurrence (or reoccurrence) of vulnerabilities or malicious code. This will help to ensure that system administrators are well-prepared to clean and secure their systems before they are placed back on the network.

Step 6: Follow-Up

The goal of the follow-up phase is to learn from the incident, to identify what worked well and where improvements can be made. Ideally, you would like to learn from each incident (hopefully not the same lessons) and continually improve the incident handling process. Having a follow-up meeting regarding the incident soon after it has been resolved is important while the event is still fresh in people's minds. It is important to accurately document the process that did take place and the actions that were taken. If the incident was not documented earlier, this would be a good place to capture this information. Identify what worked well along with areas that could be improved upon.

The University did an excellent job of handling the follow-up phase. A meeting was called the week after the SQL Slammer incident. This meeting was well attended by University personnel from various levels of management to IT support staff. The goal of the meeting was to learn from the handling of the SQL Slammer incident and to identify areas of improvement so they could be applied during the handling of future incidents.

At this meeting, the agenda was to discuss the incident from the moment it was first detected to the time it was completely resolved. Though not as part of any existing procedure, a member of the IT staff had written down the chronology of events that were taken in response to the SQL Slammer Worm. And even though the incident was still fresh in everyone's minds, this chronology of events helped focus the discussions.

During the meeting, it was important not to place blame on any particular group or individual. A very open and honest discussion took place, and people were genuinely concerned about how to improve the incident handling process. There are certainly areas of the University's incident handling process that can be improved, and many good recommendations came out of the meeting. Some of these recommendations are presented in this paper.

After the follow-up meeting, a person should be assigned the task of following through with documenting and reviewing the meeting notes for accuracy. Lessons learned and recommendations for improving system and network defenses and for improving the incident handling process should be documented. These recommendations, the costs and impact of implementation (as well as for not implementing), should be presented to management. The lessons learned from the SQL Slammer incident helped initiate the development of University incident handling procedures and focus a discussion on better protecting University technology assets. With the organizational structure in place for dealing with information security issues, the University will be able to continue to improve its system and network defenses and incident handling capabilities.

Conclusion

When the SQL Slammer Worm was released, the University certainly could have benefited from having more robust incident handling policies and procedures as well as better system and network protection mechanisms in place. By taking the time to do the necessary follow-up and analyzing the process that had taken place, some of the lessons that were learned during the handling of SQL Slammer can be used as the impetus to establish more comprehensive incident response policies and procedures.

Having established policies and procedures for responding to information security related incidents is essential. It is also important to establish a proactive plan for improving system and network infrastructure defenses and providing security training for system and network administrators. When incidents do occur, established plans and procedures can be followed, mistakes can be minimized, and incidents won't necessarily escalate into a crisis.

There are many aspects of the incident handling process that are not touched on in this paper. Other sources provide a more comprehensive overview of the entire incident handling process; some of them are listed in the references section of this paper. It was the intent of this paper to document and present some of the lessons learned from the handling of the SQL Slammer Worm at a major university. What we have learned will help the University develop more robust incident response procedures and better system and network defenses, thus enabling it to be better prepared for the next information security incident. With continued improvement in incident handling and the protection of University systems and networks, the goal of affording more time to plan and prepare and less time reacting to emergencies may be soon be attainable.

References

1. Andersson, Niklas. “Deploying a Network Abuse Team – Case Study.” 11 Nov 2002. URL: http://www.giac.org/practical/niklas_andersson_gsec.doc (10 Aug 2003).

2. Australian Computer Emergency Response Team Home Page. URL: http://www.auscert.org.au/ (10 Aug 2003).

3. CERT Coordination Center® Home Page. URL: http://www.cert.org/ (10 Aug 2003).

4. CERT Coordination Center®. “CERT/CC Statistics 1998-2002.” 15 Jul 2003. URL: http://www.cert.org/stats/cert_stats.html (10 Aug 2003).

5. CERT Coordination Center®. “Incident Reporting Guidelines.” 11 May 1998. URL: http://www.cert.org/tech_tips/incident_reporting.html (10 Aug 2003).

6. Computer Systems Laboratory Bulletin. “Establishing a Computer Security Incident Response Capability.” Feb 1992. URL: http://csrc.nist.gov/publications/nistbul/csl92-02.txt (10 Aug 2003).

7. Davis, Steve. “Developing Continuity in Government Planning.” Disaster Recovery Journal. Volume 16, Number 2 (2003): 16-20.

8. Devlin, Ed. “The Role of Executives in Managing a Crisis.” Disaster Recovery Journal. Volume 16, Number 2 (2003): 14.

9. Fitton, Aaron. “Incident Handling Policies and Procedures: Prepare Now!” URL: http://www.giac.org/practical/GSEC/Aaron_Fitton_GSEC.pdf (10 Aug 2003).

10. Internet Security Systems’ X-Force® Home Page. URL: http://xforce.iss.net/ (10 Aug 2003).

11. Internet Storm Center Home Page. URL: http://isc.incidents.org/ (10 Aug 2003).

12. “Microsoft PSS Security Response Team Alert – New Worm: W32.Slammer." 30 Jan 2003. URL: http://www.microsoft.com/technet/security/virus/alerts/slammer.asp (10 Aug 2003).

13. Northcutt, Stephen. Computer Security Incident Handling Step By Step. The SANS Institute, Oct 2001.

14. Osborne, Terry. “Building an Incident Response Program to Suit Your Business.” 3 Jul 2001. URL: http://www.sans.org/rr/incident/program.php (10 Aug 2003).

15. Pham, Charles. “From Events to Incidents.” 29 Nov 2001. URL: http://www.sans.org/rr/paper.php?id=646 (10 Aug 2003).

16. Skoudis, Ed. “The Coming Super Worms.” National Information Assurance Leadership Conference. 6 Mar 2003 (2003).

17. Sophos Plc. Home Page. URL: http://www.sophos.com/ (10 Aug 2003).

18. Sorenson, Holt. “Incident Response Tools For Unix, Part One: System Tools.” 27 Mar 2003. URL: http://www.securityfocus.com/infocus/1679 (10 Aug 2003).

19. Symantec Security Response. URL: http://securityresponse.symantec.com/ (10 Aug 2003).

20. Wack, John P. “Establishing a Computer Security Incident Response Capability (CSIRC).” NIST Special Publication 800-3. Nov 1991.

21. Wood, Bradley J. and Bouchard, Julie F. “Improving Government-Wide Emergency Response to Cyber Incidents.” Proceedings of the 2001 IEEE Workshop on Information Assurance and Security. 5-6 Jun 2001 (2001): 195-198.

22. WormWatch.org Home Page. URL: http://www.wormwatch.org/ (10 Aug 2003).