

CSIRT Management

M. E. Kabay, PhD, CISSP-ISSMP
Assoc Prof of Information Assurance
School of Business & Management
Norwich University

<http://www.mekabay.com/infosecmgmt/csirtm.pdf>

Table of Contents

1	Introduction.....	3
2	Creating the CSIRT	4
2.1	CSIRT Functions.....	4
2.2	Defining Service Levels.....	5
2.3	Establishing Policies and Procedures.....	6
2.4	Staffing.....	7
3	Responding to Computer Emergencies.....	9
3.1	Triage	9
3.2	Technical Expertise	10
3.3	Tracking Incidents.....	11
3.3.1	Will this Have to be Done Again?	11
3.3.2	Why document?	11
3.3.3	Keep electronic records.....	12
3.3.4	Advantages for Technical Support and CSIRTs	13
3.3.5	Requirements	13
3.3.6	Tools.....	14
3.4	Critical Distinctions	15
3.4.1	Get The Global Picture.....	15
3.4.2	Distinguish Observation From Assumption.....	15
3.4.3	Distinguish Observation From Hearsay	15
3.4.4	Distinguish Observation From Hypothesis	16
3.4.5	Challenge Your Hypothesis	16
3.5	The Telephone Hotline.....	17
4	Securing the CSIRT: Walk the Talk	18
5	Managing the CSIRT	19
5.1	Professionalism	19
5.2	Setting the Rules for Triage	20
5.3	Triage, Process and Social Engineering.....	22
5.4	Avoiding Burnout.....	23
5.5	Many Types of Productive Work.....	24
5.6	Setting an Example.....	24
5.7	Notes on Shiftwork.....	25
6	Learning From Emergencies.....	27
6.1	The Postmortem	27
6.2	Continuous Process Improvement: Sharing Knowledge Within the Organization.....	29
6.3	Sharing Knowledge with the Security Community.....	30

1 Introduction

In this overview,¹ I will summarize the key points in creating and managing a computer security incident response team (CSIRT), also sometimes known as a computer incident response team (CIRT) or a computer emergency response team (CERT).

No matter how good your security, at some point some security measure will fail. Knowing that helps you plan for security in depth, so that a single point of failure does not necessarily result in catastrophe. Furthermore, instead of trying to invent a response when every second counts, it makes sense to have a CSIRT in place, trained, and ready to act. As everyone should know, the value of time is not constant. Spending an hour or a day planning so that one's emergency response is shortened by a few seconds may save a life or prevent a business disaster.

The CSIRT should include members from every sector of the organization; key members include operations, facilities, legal staff, public relations, information technology, and at least one respected and experienced manager with a direct line to top management. The CSIRT should establish good relations with law-enforcement officials and should be prepared to gather forensic evidence. The organization should have a policy in place on how to decide whether to prosecute malefactors if they can be identified. The CSIRT should be prepared to respond not only to external attacks but also to criminal activities by insiders. Proper logging at the operating system level and from intrusion-detection systems can be useful to the CSIRT. The CSIRT plays an important role in disaster prevention, mitigation, and recovery planning.²

Organizing people to respond to computer security incidents is worth the effort not only when you actually have an incident but also because the analysis and interactions leading to establishment of the CSIRT bring benefits even without an emergency. A CSIRT can provide opportunities for improving institutional knowledge, contributing to continuous process improvement, and offering challenging and satisfying work assignments to technical and managerial staff, thus contributing to reduced turnover. A well-trained, professional, courteous CSIRT can improve relations between the entire technical support infrastructure and the user community.

¹ Much of this material originally appeared in a series of articles published in my *Network World Security Strategies Newsletter* beginning in 2004. Archives are available online at < <http://www.networkworld.com/newsletters/sec/> >. I updated some of the material and added new sections while I was creating the Computer Security Incident Team Management elective course for the Master of Science in Information Assurance program at Norwich University. I make no further specific references to any particular *Network World Security Strategies* newsletter from this point on.

²This introductory section includes material I published in the article "Securing your business in the age of the Internet" in the magazine *Business International* in 1999 (not available online).

2 Creating the CSIRT

Not every organization has a CSIRT already in place; not all CSIRTs are structured and managed in the most appropriate ways for a specific organization's needs. This section presents systematic approaches for rational design and implementation of a CSIRT.

2.1 CSIRT Functions

Shortly after the infamous Morris Worm incident of November 2, 1988 and several other attacks on the Internet of the day, security experts established the Computer Emergency Response Team Coordination Center (CERT-CC™) at the Software Engineering Institute of Carnegie Mellon University in Pittsburgh, PA.³ Since then, CERT-CC has provided invaluable services to the world community of Internet users and especially to system and security administrators. In addition to the archives of security alerts and incident analyses available online and via free e-mail subscriptions, CERT-CC provides free electronic textbooks of great quality. One of these is the famous *Handbook for Computer Security Incident Response Teams (CSIRTs)* edited by Moira J. West-Brown and colleagues and which is now in its second edition (April 2003).⁴ I strongly recommend this work to anyone concerned with establishing and managing a CSIRT.

West-Brown *et al.* describe the functions of the CSIRT as follows:

For a team to be considered a CSIRT, it must provide one or more of the incident handling services: incident analysis, incident response on site, incident response support, or incident response coordination.

They explain in detail all aspects of these functions and summarize their research on the range of services that CSIRTs actually provide, whether by themselves or in cooperation with other teams in the information technology sector, in a table [see page 25] which I have reformatted below:

- Reactive Services
 - Alerts and warnings
 - Incident handling
 - Incident analysis
 - Incident response on site
 - Incident response support
 - Incident response coordination
 - Vulnerability handling
 - Vulnerability analysis
 - Vulnerability response
 - Vulnerability response coordination

(Cont'd on next page)

³ < <http://www.cert.org> >

⁴ West-Brown, M. J., D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle, M. Zajicek (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd Edition*. Computer Emergency Response Team Coordination Center (CERT-CC™), Carnegie Mellon University Software Engineering Institute. HANDBOOK CMU/SEI-2003-HB-002. xvi + 201 pp. Available for free download from < <http://www.cert.org/archive/pdf/csirt-handbook.pdf> >

- Artifact handling
 - Artifact analysis
 - Artifact response
 - Artifact response coordination
- Proactive Services
 - Announcements
 - Technology watch
 - Security audits or assessments
 - Configuration & maintenance of security tools, applications and infrastructures
 - Development of security tools
 - Intrusion detection services
 - Security-related information dissemination
- Security Quality Management Services
 - Risk analysis
 - Business continuity and disaster recovery planning
 - Security consulting
 - Awareness building
 - Education / training
 - Product evaluation or certification

The only problematic term in this list is “artifact,” which the authors define as “any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.” [p. 28].

The specific combination of functions that your CSIRT will provide will be a function of personnel and budgetary resources and of the maturity of the team. It is wise to focus a completely new CSIRT on essential services such as incident handling and analysis as their first priority. With time and experience, the team can add functions such as coordinating with other security teams and with computer and network operations in the more proactive services and the security quality services that will lead to long-term reduction in security incidents and to lower damages and costs from such incidents.

2.2 Defining Service Levels

When you start working on a CSIRT, you must manage expectations carefully to avoid disappointment, frustration and hostility from users who may want more than you can reasonably provide. Managing expectations is a general principle applicable in a wide range of projects, not just CSIRT management; for example, in planning a large-scale transaction processing system where the contract stipulated a maximum response time per transaction of three seconds, I remember that the programming team built a timer into the system so that responses would take exactly three seconds even during the initial test phases. We knew that only a few data entry clerks would be working on the system to try it out for the first few weeks, and the last thing we wanted was to get them used to sub-second response times that would climb as the databases became increasingly loaded and when several hundred users finally began using the system. At first, the client thought that this strategy was odd, but after thinking about it, they realized that it made sense.

As you establish your CSIRT, you may want to start small, as I mentioned before. Perhaps you can limit the scope of the CSIRT to a few of the smaller production systems to avoid plunging into a

new area of expertise with enormous stakes riding on your success. You should decide whether to start with working-hours only, extended hours (e.g., early morning to late night) or 24-hour, seven-day operations. If software development is part of your environment and (as most people will recommend) is physically distinct from production systems, perhaps that could be a good start for the nascent CSIRT. Although many development staff may work long hours and on weekends, the effects of system emergencies may be less severe than attacks or breakdowns involving other systems such as, say, inventory, factory controls, customer service, sales and so on. When you are ready to tackle an even more significant production system, perhaps a system whose users tend to leave more-or-less at the end of the day might be a good candidate; e.g., the accounting system or support systems for any operation that does not run more than one shift per day.

In any case, be sure that you communicate your intentions for when your CSIRT services will be available to your customers (and yes, that's a deliberate use of the word).

The other aspect of service levels is how fast you can respond to emergencies. That's a much more complex issue and will be the subject of articles on triage and setting the rules for triage later in this series.

2.3 Establishing Policies and Procedures

As the US government Defense Information Systems Agency (DISA) training course on CD-ROM about CSIRTs succinctly puts it, "policies and procedures are not merely bureaucratic red tape."⁵ They are the scaffolding on which you can establish clear understanding and expectations for everyone involved in incident response. These living, evolving documents are tools that provide guidance on (quoting the CD-ROM)

- Roles and responsibilities
- Priorities
- Escalation criteria
- Response provided
- Orientation.

Policies are the statements of the desired goals; procedures are the methods for attaining those goals. Policies tend to be global and relatively stable; procedures can and should be relatively specific and can be adapted quickly to meet changing conditions and to integrate knowledge from experience. Policies cannot be promulgated without the approval and support of appropriate authorities in the organization, so one of the first steps is to identify those authorities. Another step is to gain their support for the policy project.

⁵ DISA (2001). Introduction to Computer Incident Response Team (CSIRT) Management, v 1.0. Originally available free from the Information Assurance Support Environment at < <http://iase.disa.mil/eta/index.html> >; now available for free authorized download from M. E. Kabay's Web site < http://www.mekabay.com/infosecmgmt/disa_cirtm_cdrom.zip >.

CSIRT Management

All policies and especially CSIRT policies should be framed in clear, simple language so that everyone can understand them and should be made available in electronic form. In other works, I have pointed out that hypertext can make policies more understandable by providing pop-up comments or explanations of difficult sections or technical terms.⁶

Similarly, procedures show how to implement the policies in real terms. For example, a policy might stipulate, “All relevant information about the time and details of a computer incident shall be recorded with regard for the requirements of later analysis and for possible use in a legal proceeding.” That policy might spawn a dozen procedures describing exactly how the information is to be recorded, named, stored, and maintained through a proper chain of custody. For example, one procedure might start, “Using the Incident-Report form in the CSIRT Database accessible to all CSIRT members, fill in every required field. Use the pull-down menus wherever possible in answering the questions.” Again, as the DISA CD-ROM points out, these procedures should minimize ambiguity and help members of the team to provide a consistent level of service to the organization. A glossary of local acronyms and technical terms can be helpful as part of these procedures.

Whenever policies and procedures are changed in a way that may affect users, it’s important to let people know about the changes so that their expectations can be adjusted. The DISA course recommends using several channels of communications to ensure that everyone gets the message; e.g., send e-mail, use phone and phone messages, send broadcast voicemail, announce the changes at staff meetings, and use posters and Web sites.

2.4 Staffing

The computer security incident response team may be a permanent, full-time assignment for a fixed group of experts or it may be a part time role assigned to dynamically as conditions require. In either case, or for any of the intermediate arrangements, certain fundamentals will dictate your choice of staff members for the CSIRT. Cowens and Miora write,

Maturity and the ability to work long hours under stress and intense pressure are crucial characteristics. Integrity in the response team members must be absolute, since these people will have access and authority exceeding that given them in normal operations.

Exceptional communications skills are required because, in an emergency, quick and accurate communications are needed. Inaccurate communications can cause the emergency to appear more serious than it is and therefore escalate a minor event into a crisis.⁷

⁶ Kabay, M. E. (2009). Security Policy Guidelines. Chapter 44 in Bosworth, S., M. E. Kabay & E. Whyne (2009), eds. *Computer Security Handbook, 5th Edition*. Wiley (New York). ISBN 978-0471716525. 2040 pp in 2 volumes. Index.

⁷ Miora, M., M. E. Kabay & B. Cowens (2009). Computer Security Incident Response Teams. Chapter 56 in Bosworth, S., M. E. Kabay & E. Whyne (2009), eds. *Computer Security Handbook, 5th Edition*. Wiley (New York). ISBN 978-0471716525. 2040 pp in 2 volumes. Index.

CSIRT Management

The DISA course on CSIRT Management addresses the question of the technical level required by CSIRT staff. The authors suggest,

Using a scale from 1 to 10 with 1 representing the novice or support staff, and 10 representing the technical wizard, . . .

To handle the initial Triage process, which involves separating service request into categories and directing them to the appropriate team member, individuals in the 1 to 3 technical range should be sufficient.

Information requests can be handled by team members in the 1 to 5 range. For example, a support staff person can send out publications, while someone with greater expertise would be required to address the question about identifying spoofed e-mail.

To handle incidents . . . team members in the 5 to 8 technical range are necessary. This response can involve technical analysis and communicating with compromise sites, law enforcement technical staff, and other CIRTs. In handling incidents that represent new attack types, you may need to call the wizards to help understand and analyze the activity.

Vulnerability handling requires your most proficient personnel, falling into the eight to 10 range. These individuals must be able to work with software vendors, CIRTs, and other experts to identify and resolve vulnerabilities. Many CIRTs don't have access to this level of technical expertise."⁵

I want to add to these excellent comments that in my experience, CSIRT staff with the psychological flexibility to allow them to adapt quickly to changing requirements will do better than people who resist change or resent ambiguity. Ideally, the team will include problem-solvers with an intuitive grasp of the differences between observation and assumption, hypothesis and deduction. As always, team-players committed to getting the problem solved will contribute more than people interested in acquiring personal credit for achievements. I also think that having at least one person on the team with a penchant for meticulous note-taking is a real benefit; more about recordkeeping in another segment in this series.

3 Responding to Computer Emergencies

I turn next to some of the immediate issues in responding to computer emergencies:

- Triage – deciding how to direct calls for help or reports of a computer security incident;
- Technical expertise – the different kinds of knowledge that support effective response;
- Tracking incidents – ensuring appropriate documentation to save time and reduce errors;
- Critical information – laying the ground rules for collecting the kinds of data needed for effective decisions;
- The telephone hotline – suggestions for real-time notification and response.

3.1 Triage

So let's start with triage. The word itself comes from a French root meaning to sort. In medicine, triage is "prioritization of patients for medical treatment: the process of prioritizing sick or injured people for treatment according to the seriousness of the condition or injury."⁸ Similarly, anyone receiving calls about computer security incidents must be able to classify the call right away so that the right resources can be called into play. As the DISA course on computer security incident response team management suggests, "The triage process recognizes and separates

- new incidents,
- new information for ongoing incidents,
- vulnerability reports, ...
- information requests, [and]
- other service requests."⁵

I have altered the order of the original list to reflect a decreasing rank of importance for these factors in communicating and acting upon calls.

Triage is common to ordinary help desks as well as to emergency hotlines. In general, there are two models for staffing the phones for such front-line functions: the "dispatch" model and the "resolve" model.⁹ The dispatcher has just enough technical knowledge to collect appropriate information about an incident and assignment to a team member for investigation; the alternative is to assign someone with more expertise to answer the phone so that response can be even faster. However, the resolve model risks wasting resources because the more experienced staff member may end up doing largely clerical work instead of focusing on applying his or her expertise to problem analysis and resolution.

⁸ Microsoft® Encarta® Reference Library 2009.

⁹ Czeglé, B. (1998). *Running an Effective Help Desk, Second Edition*. John Wiley & Sons (ISBN 0-471-24816-9).

CSIRT Management

To support triage, staff members need explicit training on data collection and priorities. They need to record who is calling, how to reach that person, what the caller thinks is happening, what the caller has observed, how serious the consequences are, how many people or systems are affected, whether the incident is in progress or is over as far as they know, and how the caller and others are responding. The CSIRT procedures should include guidance on assigning priorities to incidents; factors can include security classifications (e.g., SECRET or COMPANY CONFIDENTIAL data under attack), type of problem (e.g., breach of confidentiality, data corruption, loss of control, loss of authenticity, degradation of availability or utility), possible direct costs (e.g., personnel downtime, costs of recovery, loss of business), possible indirect costs (e.g., damage to business reputation, legal liability) and so on as appropriate for each organization.

Readers may find the work of John Howard relevant for such analysis; Dr Howard has established a useful taxonomy for discussing computer security incidents that can serve as a framework for establishing priorities.^{10,11}

I recommend an automated system for capturing information on all calls to the CSIRT. Using keywords “helpdesk software” and also “help desk software” brings up dozens of options for such programs. If you have modest skill in database design, you can also create your own using a program such as MS-Access. With appropriate locking strategies and automated reports, your CSIRT can know and control the priorities of all the open incidents under investigation at any time.

For more about triage, see §5.2, Setting the Rules for Triage.

3.2 Technical Expertise

We can start as the DISA CD-ROM course does by classifying technical expertise in approximate ranges:

- Low, suitable for the triage function which involves determining who should best handle a specific call;
- Medium, appropriate for answering requests for information;
- High, suitable for technical problem-solving;
- Expert, suitable for handling problems that others have been unable to resolve and especially for issues involving vulnerability analysis and real-time responds to attacks.⁵

As the DISA writers point out, “Vulnerability handling requires your most proficient personnel. . . . These individuals must be able to work with software vendors, CIRTs, and other experts to identify and resolve vulnerabilities. Many CIRTs don’t have access to this level of technical expertise.”

¹⁰ Howard, J. D. (1997). *An Analysis of Security Incidents on the Internet, 1989–1995*. PhD dissertation, Pittsburgh, PA: Department of Engineering and Public Policy, Carnegie Mellon University, April 1997.
< <http://www.cert.org/research/JHThesis/Start.html> >

¹¹ Howard, J. D. (2009). Using a Common Language for Computer Security Incident Information. Chapter 8 in Bosworth, S., M. E. Kabay & E. Whyne (2009), eds. *Computer Security Handbook, 5th Edition*. Wiley (New York). ISBN 978-0471716525. 2040 pp in 2 volumes. Index.

If you would like to download PowerPoint presentations that cover many aspects of technical support management, you are welcome to visit my Web site.¹²

3.3 Tracking Incidents

This section focuses on some of the advantages, requirements and tools for incident tracking. First I establish why I think documentation in general is so important.

3.3.1 Will this Have to be Done Again?

When I joined Hewlett-Packard (Canada) Ltd. in 1980, I arrived on the job armed with a small, green, hard covered book which I prominently entitled LOGBOOK in big black letters. From my first day as a member of the systems engineering organization, I wrote down what I learned; in a small Daytimer® book, I logged how I spent my time. When I met clients, I took notes. When I installed new versions of MPE, I kept a chronological record of everything I did—including mistakes. While I taught courses, I kept a list of questions I couldn't answer right away.

Pretty soon, people began asking me what I thought I was doing- writing a novel?

My colleagues may have been puzzled by what they perceived as a mania for record keeping, but I was equally astonished that record keeping was not a normal part of their way of doing work. The reason I automatically kept records was my years in scientific research, where logbooks with hard covers, numbered pages and even waterproof paper were just usual parts of doing serious work. The idea of doing anything of importance without keeping a concurrent record simply didn't occur to anyone. One could not reproduce an experiment without knowing exactly what sequence one had used in accomplishing the steps. Even adding salts to solutions had to be done in a particular order.

So I just kept on keeping my little green logbooks.

By the time I left Hewlett-Packard in 1984, I had trained a few of the younger support personnel to keep careful records, especially while solving problems. They had learned the advantages of documentation.

3.3.2 Why document?

Documentation, far from being a sterile exercise done to conform to arbitrary requirements of nameless, faceless superiors, should be a vital part of any intellectual exercise. Documentation is simply writing down what we learn: the crucial step in human history that changed traditional cultures into civilizations. By keeping a record independent of any specific individual, we liberate our colleagues and our successors from dependence on our physical availability. Documentation is our assurance that work will continue without us; a kind of immortality, if you will.

We document what we do as a part of systematic problem solving. Writing forces us to identify the problem in words, instead of being content to define it in vague, unclear ideas. Writing down each idea we are in the process of testing helps us notice the ideas we missed the first time we tackled the problem. Keeping notes helps us pay attention to what we're doing.

¹² Kabay, M. E. (1988-1996). The Art of Technical Support. Course delivered at John Abbott College.

< <http://www.mekabay.com/courses/academic/jac/TSP/index.htm> >

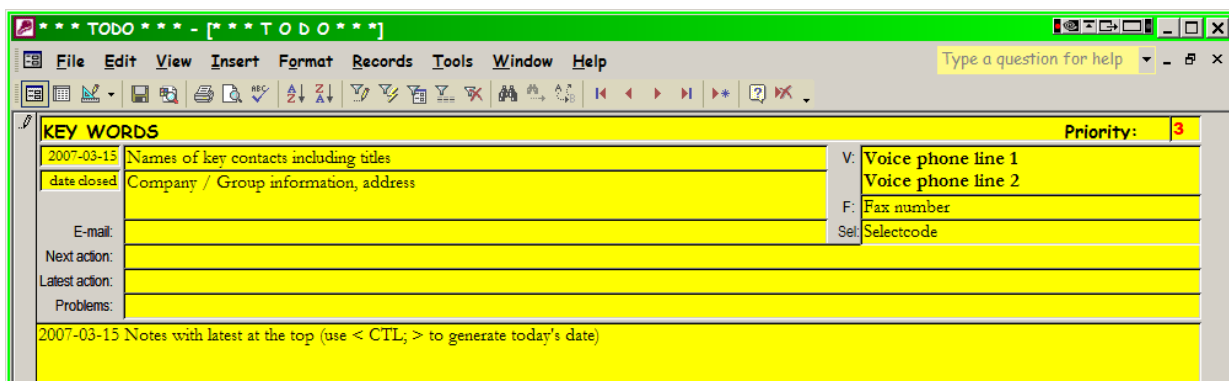
CSIRT Management

Documenting what we do also helps us during training—both our own and that of the people we are helping to learn technical skills. Trainees can review their own notes on how to do something instead of relying entirely on someone else’s description. If taking notes is viewed as a chance to engage one’s mind more thoroughly in what we’re learning, it can be fun. When I studied math, I had the habit of using a set of symbols entirely different from those the teacher used; it was harder than mere copying, but I sure learned what was going on.

Finally, accurate records can be a boon in legal wrangles. In one case I experienced, upper management seriously considered legal procedures against a supplier for supposed breach of contract. Careful records of exactly when meetings were held and with whom permitted us to analyze the problem and resolve the issues by collaboration instead of by confrontation. Such records, if kept consistently, in good times and bad, can be accepted in a court of law as evidence—but only if everything points to a steady pattern of record-keeping as events unfold. Records made long after a problem occurs are worthless.

3.3.3 Keep electronic records

The best way of keeping records on specific problems is an easy-to-use database. Here is the layout of a simple file in I used for several years as director of technical support in a large corporate data center and ever since then to keep track of all my projects:



By the time I finished my task of setting up a self-sufficient technical support team in the data center, we had two thousand entries archived. We had a similar file reserved for system failures and another for summaries of articles from INTEREX proceedings volumes and various other publications. Every software product we requested information about was logged in the files as well, with a pointer to the folder in which specification sheets and correspondence were stored for the particular entry. These records were and are still in constant use to find experiences which may help in solving new problems as they arise.

With easily accessible records, it became possible to solve problems without me. Stored, sharable knowledge meant that it was no longer necessary for staff to depend on my physical presence. I was able to take month-long holidays without being called for help. Part of that involved intensive training of the staff, but a good deal was the direct result of proper documentation.

Liberate yourselves: share your knowledge.

3.3.4 Advantages for Technical Support and CSIRTs

Keeping track of all of technical support calls is essential for effective incident handling. Having details available to all members of the CSIRT in real-time and for research and analysis later serves many functions:

- Communication among team members: Having the details written down in one place means that team members can pass a case from one to another and share data efficiently.
- Better client service: Callers become frustrated when they have to repeat the same information to several people in a row; a good incident-tracking system reduces that kind of irritation.
- Documentation for effective problem-solving: A good base of documented experience can help find the right procedure and the right solution quickly.
- Institutional memory: When experience is written down and accessible, the organization's capacity to respond quickly and correctly to incidents improves over time.
- Follow-up with clients: Managers can use the incident database to prepare management reports and to follow-up with specific clients to understand and resolve difficulties or complaints.
- Forensic evidence: Detailed, accurate and correctly time-stamped notes can be a deciding element in successful prosecution of malefactors.

3.3.5 Requirements

Some of the more obvious requirements of any incident-handling system are listed below. Most are self-explanatory but I've added comments to a few of them:

- Unique identifier for case
- Dates and times for all events
- Who currently controls the case: It should be instantly obvious who is in charge of solving the problem.
- Keywords
- Contact information: Every person in the case should be listed with room for phone, e-mail and fax numbers.
- Handover of control: Whenever someone takes over control of the case, that handover should be noted in the record.
- Technical details including

- Diagnostics
- Tests of hypotheses
- Resolution: What was the outcome? When was the case closed?
- Search facilities: Full-text search capabilities.
- Knowledge base: Ability to integrate vendor-supplied entries to speed research.

In an online discussion by someone called “DonaldA-M” I noted two additional points I hadn’t thought of:

- Industry-standard database engine: Easy to learn, maintain and improve.
- Accept input from comma-separated value (CSV) files: Import data from other systems.

3.3.6 Tools

There’s a wide range of software available for tracking incidents. You can build your own, but then you’ll have to provide proper documentation and training materials because turnover is a constant problem for CSIRTs. In addition, unless your analysts have experience with the CSIRT function, they are likely to miss useful features that have accumulated over the years in products used by thousands of people.

I have provided a short list of proprietary (commercial) help desk products in the Readings section below. You will want to use the *Network World* search to see an extensive list of articles on this topic.¹³

There are also well-respected open-source tools listed below.

All such tools can be complex; since you don’t want people fumbling about in an emergency, be sure that you budget for adequate training for your staff as you implement the tool you select.

For Further Reading

- “DonaldA-M” (2003). Good, but there’s more... < <http://tinyurl.com/4bcve> >
- Cerberus Helpdesk < <http://cerberusweb.com/> >
- Help Desk Institute < <http://www.thinkhdi.com/> >
- HelpMaster Pro Suite < <http://www.prd-software.com.au/prd/help-desk-products/> >
- Open Source Ticket Request System (OTRS) < <http://otrs.org/> >
- Request Tracker (RT) < <http://www.bestpractical.com/rt/> >
- TrackIt! < <http://www.itsolutions.intuit.com/Track-It.asp> >

¹³ < <http://search.networkworld.com/query.html?qt=help+desk&> >

- Ward, J. (2003). Evaluate help desk call-tracking software with these criteria.
< <http://techrepublic.com.com/5100-6270-5030618.html?tag=series> >
- Ward, J. (2003). Product review: HEAT PowerDesk, call center tracking software.
< <http://techrepublic.com.com/5100-6270-5034947.html> >
- Ward, J. (2003). Product review: HelpMastercall, center tracking software.
< <http://techrepublic.com.com/5100-6270-5034721.html> >

3.4 Critical Distinctions

In this section, I'm focusing on critical distinctions that your CSIRT members should keep in mind in addition to the administrative details I summarized in the last section. From my experience running technical support and operations over the years, I believe that the same principles that underlie effective technical support equally inform effective CSIRT management.

3.4.1 Get The Global Picture

When gathering information about an incident, staff members should establish a clear picture of what people were doing when they realized that there was a problem. For example, it may be important to know that someone was accessing a rarely-used account and noticed that a file was not available because someone else had it open. Those details will help to characterize the attack and to provide clues that may lead to additional valuable data. However, my approach would include asking why my contact was accessing the rarely-used account; it takes only a minute, but getting a wider picture may give the analyst another perspective that can also lead to new clues. In the scenario I have sketched, one could imagine that a system administrator had become curious about some unexpected resource utilization in a supposedly dormant account. This simple fact might lead to additional exploration of system log files and questions about whether any other dormant accounts had sparked curiosity. So, in general, it is worth your while to explore the situation more broadly at first rather than driving down the very first avenue that presents itself in the initial questions.

3.4.2 Distinguish Observation From Assumption

As the CSIRT member listens to the observations of other staff members, it is critically important to distinguish facts – that is, personal observations – from assumptions. Assumptions are ideas taken for granted or statements that are accepted without proof. For example, imagine the serious consequences of hearing someone say, “And so then they exploited a flaw in the firewall and then they. . .” and simply writing that statement down as if it were a fact. Such an assumption could profoundly distort the investigation, putting people’s efforts into the wrong track and diverting their attention from a more fruitful line of inquiry. Hearing such a statement, I would write down, “And so perhaps they exploited a flaw in the firewall....”

3.4.3 Distinguish Observation From Hearsay

Everyone has played the child’s game of whispering a sentence to another person and then hearing the distorted version that come out the other end of a long chain of transmission without error correction. CSIRT staff must always distinguish between first-person observations (“I read the log file and found...”) and hearsay (“Shalama read the log file and she found...”). Don’t trust hearsay: check it out yourself by tracking down the source of the information.

3.4.4 Distinguish Observation From Hypothesis

Sometimes when people are careless or untrained, they don't distinguish between what they saw and an idea that might explain what they saw. In the previous example about a suppose that flaw in a firewall, the person speaking seemed to take the flaw for granted; that was an assumption. A similar problem can occur when someone thinks that *maybe* there's a flaw in the firewall and then proceeds as if that were true without testing their hypothesis. "And so maybe they exploited a flaw in the firewall, so we should patch all the holes right away." Putting aside for the moment the advisability of patching holes and firewalls, merely hypothesizing an exploit doesn't make it true. Maybe it's a good thing to patch the firewall, but it doesn't follow that it's the top priority right now simply from having thought of the idea. CSIRT staff should be careful to think about what they're hearing and note explicitly when people are proposing explanations rather than reporting facts.

3.4.5 Challenge Your Hypothesis

I hope you will forgive me, Dear Reader, for a brief foray into the philosophy of science. I do have a reason to bringing it up.

In the 37 years (as of 2007) I have been teaching college courses, I've taught biology, genetics, biochemistry, embryology, physiology, applied statistics, programming, software engineering and information assurance. All of these subjects have involved a concept that some students have struggled to grasp: science depends on *disproof*, not proof. Empirical science (in contrast to logical systems such as mathematics) does not offer "proofs" in an absolute sense. Instead, a scientist formulates an hypothesis, defines a set of conditions and observations with predicted results and sees if there are grounds for rejecting randomness as a simple explanation of the deviation of the observations from the predictions. In many cases, scientists will assume the *absence* of a relationship or phenomenon (thus "null" hypothesis). Many experiments assume the absence of the interesting stuff and try to see if there are grounds for *rejecting* this simple explanation: "There's nothing there."

Science works by DISPROVING hypotheses. Explanations that cannot, by definition, be disproved are not part of a scientific effort.

Even more confusing for people who habitually think in terms of absolutes, even accepting the null hypothesis doesn't necessarily mean that there's nothing there. We may be measuring or counting too few occurrences to spot the cases that will challenge the non-existence of the phenomenon. There may also be confounding factors that obscure a real phenomenon.

But rejecting the null hypothesis does not, however, prove that any *specific* alternate hypothesis is necessarily correct. The evidence just restricts the *range* of reasonable hypotheses. We knock out explanation after explanation until what's left is a smaller set of explanations. In science, the best we hope for is not truth in an absolute sense but an operational equivalent to truth: useful enough to use for now.

OK, so now I want to bring this back to network management and the CSIRT. When your CSIRT members develop hypotheses, they have to try to shoot them down. Trying to show that an idea is *correct* is – ironically – the wrong approach to testing hypotheses. Just as in quality assurance, we have to come up with ways of showing that our explanation is wrong. If we fail enough times to disprove an hypothesis using genuine, thoughtful, intelligent tests of our ideas, maybe we've got something useful after all.

3.5 The Telephone Hotline

In this section, I propose simple guidelines for telephone hotline staff.

I want to add some additional requirements for the personnel involved in the CSIRT. Not only should managers look for and ensure adequate technical knowledge, they should select and enhance interpersonal skills and disciplined work habits.

CSIRT members inevitably work with some users who are stressed by the problems they are facing. It is no help to have a technical wizard who so offends the users that they stop cooperating with the problem-resolution team. Sometimes, CSIRT staff forget that their job includes not only resolving a technical issue but also keeping the clients as happy as possible under the circumstances – and the use of the word “clients” is deliberate here.

Here are some of the most irritating responses to users I have run across in my 30 years of technical support followed by my comments in square brackets:

- “No one has ever complained about this before.” [So what? If the problem is real, we should thank the user for reporting it, not make veiled criticisms that imply that the problem can’t be real.]
- “I don’t have time for this now.” [That’s a time management problem for the CSIRT, not for the client. Take responsibility for getting the right person to take charge of the problem in real-time.]
- “Why don’t you try calling . . . ?” [Same comment as just above.]
- “That’s not my problem.” [Just plain rude as well as irresponsible.]
- “Why don’t you reload the operating system and call me back if it happens again?” [Significant risk and time-cost for the client; often the first line suggestion of the terminally incompetent technician.]
- “Just format your hard disk and see if it happens again.” [Even worse than the previous suggestion if it is just a casual suggestion to get the client off phone for now.]
- “Don’t get mad at me – I just work here.” [A professional will understand that there’s a difference between criticism directed at the organization or its procedures versus a direct *ad hominem* attack. The former should be taken seriously and passed on to people who can evaluate the seriousness of the criticism; the latter can be unacceptable and should be passed on to a manager who can explain the need for civility even under stress.]

4 Securing the CSIRT: Walk the Talk

In this section, I want to expand on the importance of securing the CSIRT and more broadly, of using our own advice.

The course narrator in the DISA CD-ROM very properly notes, “Once the CIRT becomes known, it will be an attractive target for intruder attacks. A security breach at your CIRT site can be devastating to your reputation and have repercussions for the commands you support; in terms of security procedures, practice what you preach. You will need to provide solid physical, host, and network security in addition to appropriate staff training.”⁵

He continues,

“A compromise of any data related to incidents can have legal repercussions as well as financial and credibility consequences. What types of data need to be secured?

- Incident reports,
- electronic mail,
- vulnerability reports, and even
- briefing notes and slides.”

More generally, all security personnel should be scrupulous in respecting security regulations and best practices. Just before writing the original article on which this section is based, I was chatting with some security officers at a large corporation who were doing a due-diligence interview with me before approving enrollment for one of their employees in our graduate program. The questions centered around the confidentiality of company-specific information in the case study reports that the student would submit for grading during the 18-month program. I explained that no student is expected to reveal his or her employer’s name or even location; that students use an internal e-mail address defined by our teaching platform and used on our access-controlled extranet; and finally that all of our instructors are themselves security professionals. I said that it is a matter of course for security professionals to be under nondisclosure whether a contract is signed or not – at least, to maintain a professional reputation. We all agreed that working in security eventually affects our behavior in a reflex way; we laughed that it’s almost impossible not to look away when someone enters a password on a keyboard.

Another example of practicing what we preach is backups. For a security professional to lose data because of a lack of backups would be intensely embarrassing. I constantly urge my students to do backups of their school work so that they never have to repeat what they have already done in case of a disk failure or a human error. Personally, I can demonstrate that I do a daily differential backup every day, clone my main computer’s disk to my laptop at least once a week (actually daily when I’m teaching undergraduate courses) and create a full backup to DVDs once a month. I’ve only had a few occasions over these last decades when I needed those backups, but the minor effort involved was more than repaid by the ease of recovery and by the ability to look someone straight in the eye when telling them how to protect their data.

We have to walk what we talk.

5 Managing the CSIRT

All the work that goes into creating a CSIRT can be wasted if managers fail to lead. Sloppy management can result in degraded performance, alienation of the client base, staff frustration, sabotage and employee turnover.

5.1 Professionalism

The DISA course wisely emphasizes the importance of professional behavior by all members of the CSIRT. The authors write, “The survival of your CIRT may well depend upon using a Code of Conduct, which will earn the trust and respect of the commands you support. The conduct of any single team member reflects upon the entire CIRT organization. If the commands don’t trust your CIRT, they won’t report to you. It is important, therefore, not only to have a Code of Conduct, but to shake it out and dust it off every once in a while. Remind team members what it is and why it is important...and use it.”⁵

Here are some of the practical recommendations from that course (although I have put them in my own words for the most part):

- Write down the rules – a Code of Conduct – that represent your ideals of courteous, professional service to your clients.
- Train the team to understand and apply the Code.
- Review the Code periodically with the team.
- Speak clearly and avoid technobabble.
- Tell people exactly what you intend to do.
- Never hesitate to say, “I don’t know – but I’ll find out.”
- Don’t criticize other people in your interactions with clients.
- Respect the confidentiality of your clients.
- Be respectful of your callers: don’t belittle them or make them feel bad.

I was a member and then team leader of the Phone-In Consulting Service (PICS) at Hewlett-Packard (Canada) Ltd in Montréal in the early 1980s and later was director of technical services at a big service bureau in that city in the mid-1980s. Those experiences support the correctness of DISA’s advice.

Notice how consistently DISA (and I) refer to clients; this usage emphasizes that both technical support teams and CSIRTs all perceive users as people to whom we owe service. There is no benefit to allowing an adversarial relationship between the technical support team or a CSIRT and the client base. Don’t allow a gulf to develop between the CSIRT and the client community; clamp down on

disparaging terms and derogatory comments about users. Ensure that team members understand why such language is harmful.

Identify CSIRT members with a chip on their shoulders: don't let them adopt defensive, arrogant or aggressive attitudes toward the users. If a computer-security incident can be traced to procedural errors (i.e., the procedures themselves rather than user error are causing problems), the person reporting the problem should be thanked for the information, not criticized for having experienced or identified the problem. And never let anyone say with a sneer, "Well, you're the first person to report that."

No one in a CSIRT has ever regretted being professional. Go out there and be NICE.

5.2 Setting the Rules for Triage

As I mentioned in §3.1, "Triage" in French (my native language) means "sorting." In emergency medicine, the term was applied to the process of prioritizing treatment for patients arriving at trauma hospitals near combat zones in World War I. The same concept has been applied to help desks. For example, the "Help desk triage policy" from Courtesy Computers illustrates how a help-desk team can categorize problems to ensure that important issues receive faster service than less important problems.¹⁴ Importance is defined in terms of the number of users affected, the effects on mission-critical functions, and the costs of downtime or of less-than-optimal functions. The five priority levels suggested in the document mentioned above are typical of the kind of triage categories established in many help-desk departments (adapted from a table in the Courtesy Computers document):

Priority 1

- Issue of the highest importance—mission-critical systems with a direct impact on the organization (Examples: widespread network outage, payroll system, sales system, telecom system, etc.)
- Contact: Immediate—5 minutes
- Resolution: 30 minutes

Priority 2

- Single user or group outage that is preventing the affected user(s) from working (Examples: failed hard drive, broken monitor, continuous OS lockups, etc.)
- Contact: 15 minutes
- Resolution: 1 hour

Priority 3

- Single user or group outage that can be permanently or temporarily solved with a workaround (Examples: malfunctioning printer, PDA synchronization problem, PC sound problem, etc.)

¹⁴ Help Desk Triage Policy. Courtesy Computers.

< <http://www.courtesycomputers.com/Best%20Practices/help%20desk%20triage.doc> >

CSIRT Management

- Contact: 30 minutes
- Resolution: Same Day

Priority 4

- Scheduled work (Examples: new workstation installation, new equipment/software order, new hardware/software installation)
- Contact: 1 hour
- Resolution: 1-4 days

Priority 5

- Nonessential scheduled work (Examples: office moves, telephone moves, equipment loaners, scheduled events)
- Contact: Same Day
- Resolution: 5 days.

In his helpful overview, “CIRT – Framework and Models,” Ajoy Kumar summarizes the functions of triage as follows: “Triage: The actions taken to categorize, prioritize, and assign incidents and events.¹⁵ It includes following sub-processes:

- Categorize events.
- Correlate various events. Personnel involved in such teams typically also belong to Forensic teams.
- Prioritize events.
- Assign events for handling and response.
- Communicate information to ‘Respond’ process for further handling.
- Re-assign (and close) events not belonging to CIRT.”

The DISA training materials suggest three broader categories of interactions with help desks and CSIRTs: “incidents, vulnerabilities, and information requests.”¹⁵ Incidents involve breaches of security; vulnerabilities include reports of security weaknesses (and may be reported as part of an incident); information requests – often managed using lists of frequently-asked questions (FAQs).

The DISA instructors go on to define factors which can help CSIRTs prioritize incidents as follows:

- “The sensitivity and/or criticality of the data affected
- The amount of data affected
- Which host machines are involved

¹⁵ Kumar, A. (2005). CIRT – Framework and Models.< <http://www.securitydocs.com/library/2964> >

- Where and under what conditions the incident occurred
- Effects of the incident on mission accomplishment
- Whether the incident is likely to result in media coverage
- Number of users affected
- Possible relationships to other incidents currently being investigated
- The nature of the attack
- Economic impact and time lost
- Number of times the problem has recurred; and even
- Who reports the incident.”

On this last point, the DISA writers point out that the organizational rank of someone calling in an incident may bear on its priority – but that it may be wise to cross-check the report with a security expert who can speak to whether the report is sound.

In summary, it is important to establish a sound basis for staff members of the CSIRT to carry out triage effectively. Once the rules for evaluating incidents have been clarified, staff members should practice analyzing a number of cases to train themselves in applying the rules consistently. Role-playing exercises based on historical records or on made-up examples can provide an excellent and enjoyable mechanism for staff members to establish a common standard for this difficult and sensitive task.

5.3 Triage, Process and Social Engineering

Sometimes staff (or even managers) question the value of strict adherence to policy. Policy is sometimes seen as the expression of unnecessary rigidity – an inability to respond quickly to changing or unexpected circumstances. However, in CSIRT management, knowing and adhering to well-thought-out policies and following a reliable process are particularly valuable not only for information gathering, data recording and analysis but also to maintain strict security.

One of the well-known tricks used by criminal hackers and spies is to simulate urgency that supports demands for violations of normal security restrictions. For example, criminals will call a relatively low-status employee such as a secretary and pressure him into violating standard protocols to obtain the password of his boss by claiming extreme circumstances of great urgency. The criminal may escalate the pressure to outright bullying by threatening the employee with punishment.

A criminal determined to penetrate security barriers can manufacture an incident that leads to involvement of the CSIRT. Allowing such a person to apply pressure for violations of protocol is an invitation to compromise. Worse, such deviations from well-trying and well-justified procedures can add to the embarrassment caused by the compromise: it's bad enough to have someone breaking through our security without having to admit that we helped her.

5.4 Avoiding Burnout

Much of the discussion below applies equally to CSIRTs and to help desks; in a sense, one can view the CSIRT as a specialized help desk. Many CSIRTs are specialized subsets of the help desk team.

Any organization, even one with a relatively small CSIRT or a small help desk, can suffer spikes in demand. Ordinary business cycles can influence network usage; for example, universities often see perfectly normal but large increases in call volumes at registration times as new students forget their passwords, try to connect unverified laptops to the university network, or get blocked for violating appropriate-use policies. At any site, a denial-of-service attack, a plague of computer virus infections, or an infestation of computer worms can cause a flood of calls ‘way above normal levels.

Another trend is the ironic observation that the better a CSIRT (or help-desk team, but I’ll continue by focusing on CSIRTs) becomes at handling problems, the more readily members of its community will turn to it to report problems or ask for help. Thus the better the CSIRT does its job, the heavier its workload can become, at least for a while. According to the DISA course, “As a new CSIRT grows and the workload increases, and especially on those teams that provide 24-hour emergency response, burnout becomes quite common. By studying the issue, one national CSIRT determined that a full-time team member could comfortably handle one new incident per day, with 20 incidents still open and actively being investigated.”

Staff members who face increasing workloads may become stressed. Working long periods of overtime, missing time with family and friends, perhaps even missing regular exercise and food – these factors may lead to increased errors and turnover if people are forced to accept increasingly demanding conditions for long periods.

One of the most valuable organizational approaches to preventing burnout is to rotate staff through the CSIRT function from your IT group on a predictable schedule. For example, you can assign people to the CSIRT for three- or six-month rotations.

Such rotations require especially good training programs and particularly good documentation to maintain efficiency as new people come on duty; in addition, the assignments must be staggered so that the CSIRT doesn’t have to cope with large numbers of newcomers all at once. Ideally, there wouldn’t be more than one switch of personnel a week.

How should existing assignments be transferred within the CSIRT? I recommend that *difficult* existing cases be transferred to staff members who have been on duty for a few weeks, not to the incoming staff member (even if she has experience on the CSIRT). The incoming CSIRT member should be given a chance to get into (or get back into) the rhythm of the job before being hit with the most intractable problem or the orneriest client.

Every incident must have a case coordinator – the person who monitors the problem, aggregates information from varied resources and serves as the voice of the CSIRT for that incident. When transferring responsibility for a case from one case coordinator to another, be sure to have the previous coordinator prepare the clients for the transition and introduce the new coordinator to the key client contacts to ensure a smooth transition of control. Clients often come to depend on the person they have been working with to resolve an incident; an unexpected change can be unsettling and even disturbing.

5.5 Many Types of Productive Work

The DISA course writers suggest, “Allow team members to allocate time away from high stress incident response assignments and pursue broader interests in areas such as tool development, public education and presentations, research, and other professional opportunities.” CSIRT members, by the nature of their work, will have a great deal to contribute to the awareness, training and education of their colleagues.

When I worked in technical support for Hewlett-Packard Canada in the 1980s, I was impressed by the care my managers exercised in preventing consistent overwork. Yes, in emergencies, we all pitched in – including managers – to resolve the problem for our clients; however, the policy on allocation of time was strictly enforced under normal circumstances. We kept careful records of our time – a habit I recommend for everyone – so that we could analyze where the burden of our work was distributed and to provide statistical information for load balancing and personnel planning. I remember distinctly how my excellent manager, Michel Amesse, spoke to me about a pattern of overwork I had demonstrated; he said that I was starting to violate the policy that no more than 70% of our time in the system engineering group should be spent on billable hours. I was astonished; why would HP want to *limit* the time spent on billing clients for our work? Michel explained that experience had shown HP upper management that it was *necessary* to maintain constant training and time for administration and just for thinking to ensure long-term productivity of their specialists.

5.6 Setting an Example

As I mentioned above, the behavior of managers can greatly influence morale, motivation and dedication among team members. Later in the 1980s, another superb manager, Pierre Labelle, Vice President of Operations at Mathema, Inc. in Montréal, taught me a lesson I have never forgotten about upper-management commitment to employee performance. We had an extended series of acceptance tests running from midnight to 06:00 for a week to see if we would approve installation of a new version of the HP3000 operating system on our production machines. To my surprise, I found Pierre staying late in his office while we began the tests. He was not directly involved in any of the quality assurance work, so I asked in puzzlement why he was there. He explained with a smile that if his team was going to work overtime and at odd hours on the project, the least he could do was to show his appreciation and support by being there. Indeed, Pierre – the VP, remember – actually went out and got us refreshments on several occasions during that week.

Making the CSIRT a stimulating and enjoyable duty that people *want* to be on is one of the best approaches to avoiding burnout and ensuring reliable response to computer-related problems.

5.7 Notes on Shiftwork

As discussed in §5.4, rotating assignments among CSIRT members can be an excellent idea. However, frequent changes in work schedules that involve changes in sleep cycles are *not* a good idea; for example, weekly changes in shift from day to night schedules can seriously disrupt the natural circadian wake/sleep cycle and have been shown to increase the rate of errors and accidents.¹⁶ One authoritative resource states that there are “adverse health and safety effects to working shifts.”

A shiftworker, particularly one who works nights, must function on a schedule that is not natural. Constantly changing schedules can:

- upset one's circadian rhythm (24-hour body cycle),
- cause sleep deprivation and disorders of the gastrointestinal and cardiovascular systems,
- make existing disorders worse, and
- disrupt family and social life.¹⁷

Scientific studies throughout the world have long shown that shiftwork, by its very nature, is a major factor in the health and safety of workers; LaDou (1982) writes in his abstract,

Daily physiologic variations termed circadian rhythms are interactive and require a high degree of phase relationship to produce subjective feelings of wellbeing. Disturbance of these activities, circadian desynchronization, whether from passage over time zones or from shift rotation, results in health effects such as disturbance of the quantity and quality of sleep, disturbance of gastrointestinal and other organ system activities, and aggravation of diseases such as diabetes mellitus, epilepsy and thyrotoxicosis.¹⁸

¹⁶ Dawson, T. & A. Aquirre (2005). *How Work Schedules Impact the Costs, Risks and Liabilities of Extended Hours Operations; Recommendations for Improvement*. Circadian Technologies Inc. White Paper. Available free (registration required) from < <http://www.circadian.com/contactforms/workfactorsform.php> >.

¹⁷ CCSOSH (1998). Rotational Shiftwork. Canadian Centre for Occupational Health and Safety. < http://www.ccohs.ca/oshanswers/work_schedules/shiftwrk.html >

¹⁸ LaDou, J. (1982). Health Effects of Shift Work. *West. J. Med* 137(6) (December 1928). < <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1274227> >

CSIRT Management

The US National Institute for Occupational Safety and Health has published a monograph about shiftwork that contains the following advice for improving shiftwork schedules:

- Avoid permanent (fixed or non-rotating) night shift.
- Keep consecutive night shifts to a minimum.
- Avoid quick shift changes.
- Plan some free weekends.
- Avoid several days of work followed by four- to seven-day “mini-vacations.”
- Keep long work shifts and overtime to a minimum.
- Consider different lengths for shifts.
- Examine start-end times.
- Keep the schedule regular and predictable.
- Examine rest breaks.¹⁹

¹⁹ Rosa, R. R. & M. J. Colligan (1997). Plain Language about Shiftwork. US Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health. < <http://www.cdc.gov/niosh/pdfs/97-145.pdf> >

6 Learning From Emergencies

One of the most important principles of management in general and operations management in particular is that fixing a problem has two aspects: the short term and the long term. One must be able to solve problems quickly enough to be effective; that is, the speed of solution must be appropriate to the consequential costs of delay. However, we should not figuratively wipe our hands in satisfaction and walk away from the problem resolution without thinking about why it happened, how we fixed it, and whether we can do better to avoid repeats and to improve our response.²⁰

6.1 The Postmortem

As a matter of standard operating procedure, every technical support and CSIRT must schedule time to analyze the underlying factors that led to the problem they have just resolved. This analysis will likely involve operational staff outside the CSIRT; these are the people with line expertise who will be able to contribute their intimate knowledge of technical details that contributed to this security breach. These discussions can often lead to practical recommendations for improvement of our security architecture such as topology or firewall placement, operational procedures such as monitoring standards or vulnerability patching, and technical details such as configurations or parameter settings.

Similarly, it is a commonplace in discussions of disaster recovery and business continuity planning that every practice run or real-life incident should be analyzed to see where we have made errors or achieve less than our goals in performance. Managers must ensure that these analyses are not perceived as (or worse, really) finger-pointing exercises for apportioning blame. In a column for *Network World*, I have explained the concepts of “egoless work;” the postmortem analysis of an incident must be ego-free.²¹ Managers can set the tone by responding positively to what might otherwise be perceived as criticism; “That’s a good point” and “Very good observation” are examples of positive, encouraging responses to observations such as “We were too slow in getting back to the initial caller given that she clearly stated that the entire department was off-line.” The meeting should focus on ways to improve the response given the insights resulting from detailed analysis of successes and failures during the recent incident.

The other aspect that sometimes gets lost in such postmortems is exploring the reasons for the problems. If we don’t pay attention to underlying causes, we may fix specific problems and we may improve particular procedures but we will likely encounter different consequences of the same fundamental errors that caused those particular problems. We must pursue the analysis and deeply in off to identify structural flaws in our processes so that we can correct those problems and thus reduce the likelihood of entire classes of problems. Readers interested in learning more about management style and small-group leadership tools may find some material of value in the Management Skills lectures and in the Leadership lectures on the MSIA section of my Web site.²²

²⁰ Kabay, M. E. (2004). On not knowing. < <http://www.mekabay.com/opinion/index.htm> >

²¹ Kabay, M. E. (2006). Egoless work: Take your ego out of the equation. *Network World Security Strategies Newsletter* (2006-02-02). < <http://www.networkworld.com/newsletters/sec/2006/0130sec2.html> >

²² MSIA public lectures < <http://www.mekabay.com/msia/public/index.htm> >

CSIRT Management

The US National Institute of Standards and Technology *Computer Security Incident Handling Guide* by Tim Grance, Karen Kent and Brian Kim specifically recommends a post-incident analysis in section 3.4. The authors' list of suggested questions is as follows (quoting exactly):

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?²³

The authors also recommend the following (paraphrasing and summarizing):

- Invite people to the postmortem with an eye to increasing cooperation throughout the organization;
- Plan the agenda by polling participants before the meeting;
- Use experienced moderators;
- Be sure the meeting rules are clear to everyone to avoid confusion and conflict;
- Keep a written record of the discussions, conclusions, and action items.

On this last point, I must add that all action items should indicate clearly who intends to deliver precisely what operational result to whom in which form by when.

²³ Grance, T., K. Kent & B. Kim (2004). *Computer Security Incident Handling Guide*. NIST Special Publication SP800-61. < <http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf> >

6.2 Continuous Process Improvement: Sharing Knowledge Within the Organization

On page 3-23 of the *Computer Security Incident Handling Guide*, the authors make a series of recommendations on how to capitalize on the knowledge gained through systematic analysis of incidents.²³ I am commenting briefly on each of their suggestions (shown in quotation marks).

- “Reports from these meetings are good material for training new team members by showing them how more experienced team members respond to incidents.” The incident reports that were used for discussion in the analytic meetings should be made available, perhaps as appendices, in a single report document so that all of the information about a specific incident or series of incidents can be accessed at one time. In what follows, such a dossier is referred to as the *follow-up report*.
- “Another important post-incident activity is creating a follow-up report for each incident, which can be quite valuable for future use.” The general principle is that without documentation, we lose the opportunity for increasing institutional knowledge. If we don’t record what we have learned, transmission depends on luck: the haphazard contacts of people who need to know something with those who can help. Without documentation and efficient indexing, information transferred becomes an inefficient, random process of querying and guesswork. Informal knowledge sometimes remains limited to a few people or even a single individual; without these key resources, the information is unavailable. If the holders of undocumented information leaves the organization their knowledge is usually lost to the group.
- “First, the report provides a reference that can be used to assist in handling similar incidents.” Why waste time reinventing solutions that have already been found? Why make the same errors and cause the same problems that have already been located and that could be avoided?
- “Creating a formal chronology of events (including time-stamped information such as log data from systems) is important for legal reasons, as is creating a monetary estimate of the amount of damage the incident caused in terms of any loss of software and files, hardware damage, and staffing costs (including restoring services).” One of the most kinds of information for managing security is cost estimates. Rational allocation of resources depends on knowing how often problems occur and how much they cost so that we can reasonably spend appropriate money in the form of equipment and the time of our employees or consultants to prevent such problems.
- “This estimate may become the basis for subsequent prosecution activity by entities such as the U.S. Attorney General’s office.” Estimates of monetary consequences are also essential for civil torts in the calculation of restitution.
- “Follow-up reports should be kept for a period of time as specified in record[-]retention policies.” As the authors discuss in another section and as I will discuss in the next section, historical records become increasingly useful as they provide a statistical base for analyzing and predicting phenomena. The costs of saving such data (which have relatively small volumes) have dropped to virtually nothing given the huge digital storage capacities of today’s archival media and their extremely low cost.

6.3 Sharing Knowledge with the Security Community

One of the most valuable contributions we can make to each other is information sharing. The Computer Emergency Response Team Coordination Center (CERT-CC) offers an overview of why and how to report security incidents in its “Incident Reporting Guidelines.”²⁴ The CSIRT experts summarize the types of activity on which they would appreciate receiving reports; reasons for reporting security incidents; the variety of people and agencies who can benefit from such reports; extensive guidelines on what to include in the reports; and how to reach the CERT-CC securely.

The section “Why should I report an incident?” has the following headers (and a paragraph or so of explanation of each point):

- You may receive technical assistance.
- We may be able to associate activity with other incidents.
- Your report will allow us to provide better incident statistics.
- Contacting others raises security awareness.
- Your report helps us to provide you with better documents.
- Your organization’s policies may require you to report the activity.
- Reporting incidents is part of being a responsible site on the Internet.

Another way of contributing to the field is to speak at conferences. For example, the Forum of Incident Response and Security Teams (FIRST) organizes conferences, technical colloquia and workshops.²⁵ The 19th Annual FIRST Conference on Computer Security Incident Handling will be in Seville, Spain on June 17-22, 2007²⁶. In 2007 the focus was “Private Lives and Corporate Risk: Digital Privacy – Hazards and Responsibilities” and included sessions on a wide range of topics suitable for technical, managerial, and legal staff at all levels. The conferences are open to all, not just members of FIRST, and organizers want participants to

- “Learn the latest security strategies in incident management
- Increase your knowledge and technical insight about security problems and their solutions
- Keep up-to-date with the latest incident response and prevention techniques
- Gain insight on analysing network vulnerabilities
- Hear how the industry experts manage their security issues
- Interact and network with colleagues from around the world to exchange ideas and advice on incident management best practices.”

²⁴ < http://www.cert.org/tech_tips/incident_reporting.html >

²⁵ < <http://www.first.org/> >

²⁶ < <http://www.first.org/conference/2007/> >

CSIRT Management

Readers should think about contributing papers to such conferences. Anyone who has spoken at technical conferences will confirm that there's no better way to solidify one's expertise than marshalling information into a clear presentation and speaking before one's peers. Feedback from interested participants can improve not only the current presentation but also the process being described. Intelligent, enthusiastic interchange among practitioners of good will with varied experiences and from different environments is not only productive of new ideas, it's immense fun!

The FIRST event includes "Lightning Talks" which are described as "short presentations or speeches by any attendee on any topic, which can be scheduled into conference proceedings with the approval of the organisers." Participants with hot news can thus present their findings or their ideas without necessarily having to prepare a long lecture or submitting their work many months in advance.

Another CSIRT conference organizer is ENISA, the European Network and Information Security Agency. ENISA has a calendar of conferences and workshops; at the time of writing, it seems to be a bit out of date (last entry from November 2006), but readers can get a good sense of the opportunities available for future conferences.²⁷

Other conferences such as those organized by the Computer Security Institute (CSI)²⁸, MIS Training Institute (MISTI)²⁹ and RSA Security³⁰ among many others offer opportunities for discussions of CSIRT management. Take advantage of these opportunities by registering for the calls for participation (CFPs) and responding to one or two a year if you can.

You will be contributing to the progress of knowledge and you'll have a blast.



²⁷ < http://www.enisa.eu.int/pages/04_01.htm >

²⁸ < <http://www.gocsi.com/netsec/> >

²⁹ < <http://www.misti.com/default.asp?Page=70> >

³⁰ < <http://www.rsaconference.com/2007/US/> >