The critical first steps in a successful incident response program. (April 2006)

Stephanie D. Hight, *CCNA, RHCT*

Abstract— **Incidents cannot be defined if no policies have been violated. Defining an incident in an organization is one of the first considerations when creating an Incident Response Policy or it can also be referred to as computer security incident response capability (CSIRC). Defining steps, actions and communication plans shows that dealing with a security incident is not merely a technical issue. A Security Policy for Incident Response can be easily compared to a battle plan; for in effect the Incident Response Team is doing battle with the effects of the incident itself. Team members should be technically proficient including network administration, system administration, programming, and incident response. One essential part of an Incident Response Team is having a designated leader or manager of the team. An "Incident Manager" can not only provide meaningful input to the incident procedure but field the hierarchy issues that are part of the incident. Incidents should and can be managed without letting the incidents manage you.**

Index Terms—**Computer Security Incidents, Incident Response Teams, Incident Manager, Security Incident Response Capability, Security Education, Training and Awareness.**

I. Introduction

THE beginning of an incident can be as subtle as a user making a call to the help desk to report a "sluggishness" that cannot be explained on his or her computer or it can be as chaotic as every alarm and pager in the Information Technology department sounding at once. Whether it is noticed by a user or by a detection system, the steps that lead to a successful investigation, containment and resolution to an incident remain the same. The incidents themselves may be as versatile as missing files or a network coming to a crawling stop whether by a deliberate outside influence or a mistake made on the inside of the network. It is an all too common scenario that either has or will face all Information Technology (IT) departments; Incidents will happen, but it is the steps that are taken before an incident occurs that will determine whether a successful and quick resolution take place or a slow and costly battle. Although there is no set standard for incident response, there are a multitude of resources that one can pull from in order to get a general outline of how it should be handled. The best practices seem able to be broken down into 6 steps: Preparation, Identification, Containment, Eradication, Recovery and Follow-up [1]. It is the first step that this paper will deal with in detail, for without this first essential step of preparation the resulting steps themselves could turn chaotic and cause the resolution to be severely delayed. We will first start where all Information Security starts: the policy. The security policy of an organization will define exactly what role the Incident Response Team (IRT) can and will take as well as how they should go about identifying the incident and then from there carry out the steps that should be taken to contain and eradicate the problem. Secondly we will define and discuss the roles that an IRT plays within the organization and steps and actions that should be taken before an incident ever occurs. Lastly we will explore the proper chain of communication that should take place before, during and after an incident to keep all necessary parties informed and involved without causing widespread panic throughout the organization.

Manuscript received April 18, 2006

Stephanie Hight is a System Administrator with the City of Raleigh, Raleigh, NC 27601 (e-mail: Stephanie.Hight@ci.raleigh.nc.us).

II. Begin with a Policy

The phone rings in the Security Administrators office and a quiet voice on the other end timidly explains that a laptop has been stolen from the building. They go on to explain that this laptop happened to contain current databases of all employee information that contained personal information such as home addresses and most importantly Social Security Numbers. If in the right hands it could be deemed a gold-mine, information that could be sold or used to steal the identities of employees; definitely a worse case scenario for any Information Security (InfoSec) department as well as the organization itself. As the person on the other end of the phone finishes their explanation the inevitable question gets asked…now what?

Incidents cannot be defined if no policies have been violated [2]. So if there is no policy, officially there can be no incident. An incident can be defined as: any security event that directly relates to computers or networks that can also include, but is not limited to spontaneously crashing hard disks, computer viruses, and cracking computer systems [3]; it can also be defined as a violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices [4]. Defining an incident in an organization is one of the first considerations when creating

an Incident Response Policy or it can also be referred to as computer security incident response capability (CSIRC) [4]. Examples of security incidents are Denial of Service, Malicious Code, unauthorized access and inappropriate usage. The policy should address and define each of these threats as well have a specific course of action for each type of threat. Without a policy in place there are no guidelines or steps to be taken by the responding group. The group itself has no authority or leadership, because nothing has been established and approved by management.

"Policies are the primary building blocks for every information security effort. In order to be successful with information security, every organization must have a set of policies which establishes both direction and management support [5]." They are the most effective way to clarify the specific roles of both the Information Security Specialists and other that may be involved with the responsibility of information security [5]. The policy itself can and should be very individualized for it reflects the view of security by management and management's commitment to uphold the policy. It also holds the scope of who it applies to and what circumstances the policy goes into effect. A key part of the policy is the severity ratings of incidents. This will help group procedures and documents that may only be needed in the event of a "high" level incident and also begin the outline of the standard operating procedures (SOP) for each level. Defining steps, actions and communication plans shows that dealing with a security incident is not merely a technical issue. It can pull in many non-IT resources and affect everyone in the organization.

Essentially the security policy is the plan or outline of what will happen as soon as an incident is discovered. A Security Policy for Incident Response can be easily compared to a battle plan; for in effect the IRT is doing battle with the effects of the incident itself. General George S. Patton is quoted as saying "I would rather have a good plan today than a perfect plan two weeks from now." It can and should be an ever evolving document that changes as new threats occur or as the outlook of management changes. But the most important thing is to have one, even if not complete or perfect, for without it there is no answer to the question, now what?

III. INCIDENT RESPONSE TEAMS

Incident Response Teams consist of individuals that are the first on the scene with the technical ability to respond rapidly and "stop the bleeding" [6]. An internal IRT can be defined as a group of individuals that an organization has given the task of incident handling, from beginning to end [3]. Globally there are Computer Emergency Response Teams (CERT) that can be called on to assist organizations that have an incident big enough that cannot be handled internally. When first starting the process of setting up an IRT an organization needs to make several initial decisions in how it will be modeled, what personnel will fill the positions as well as the services that the IRT will perform. In choosing the correct model the size of the organization can play a large role in deciding whether the IRT will be an in house solution, outsourced or a combination of the two. The latter is the most prevalent in the case of Managed Security Service Providers (MSSP) because they can offer 24x7 monitoring and identification of suspect activity that is far superior to an in-house solution. An MSSP analyzes and identifies each suspect activity and then passes the reports on to the internal IRT who then takes over the investigation [4]. This is a great benefit to organizations who can afford the service; it gives them the best of both worlds as they receive excellent monitoring and reporting from the MSSP which then gets taken over by the internal IRT who knows in detail all the workings of the system and can also keep the security and investigation all in-house. Additionally it needs to be decided what structure the team will have, will it be a central IRT that handles all incidents throughout the whole organization, which is the preferred model for small organizations or large companies that do not have remote satellite sites. There can also be a distributed model where there exists several incident response teams that are responsible for either physical locations or logical segments of the network. This model is most effective for larger organizations that have multiple satellite sites that cannot be managed from a central location. Team sharing is vital is this type of model since the different teams might be working on part of the same incident, or have seen such an event before and can lend advice on a quick resolution [4].

Staff expertise also plays a large part in the decision to outsource a large or small portion of Incident Response. Team members should be technically proficient including network administration, system administration, programming, and incident response. They should also have excellent problem solving skills with real world experiences. It is not necessary for all members to possess all of these attributes but rather have several people with areas of expertise [4]. Technical skill is not all that is needed in the personnel that fills the team; they also need interpersonal skills that will be needed in communicating with the users in the organization, which can include either management or everyday users. The IRT can also need to communicate and work with and support police and investigators if it leads to a penal, civil, administrative or disciplinary investigation [2]. Another possibility that should be addressed is a rotating incident response team. It is a 24x7 responsibility that can be very stressful and can cause difficulty in finding personnel willing to take on the on-call burden. Moral of employees can be severely diminished if only a few personnel are expected to handle the responsibility all the time without a rotation or break of some sort. Some organizations may even see fit to align the Disaster Recovery (DR) Team with the IRT. The DR team can provide expertise in keeping the operation up and running in the face of threats, something that the IRT may not have knowledge in. Integrating these two teams can provide the ability to deal with a larger range of events [7].

The services provided by the IRT should be carefully

planned out. They can provide not only a reactionary service in handling the incident, but can give invaluable services in proactive ways as well. In working proactively the team aims to reduce the number of overall incidents that will happen by anticipating intrusions as well as implementing countermeasures [8]. Security incidents come in a various amount of forms, some that could be prevented with educating the end-users in proper password selection and file encryption. In having the IRT involved in the Security Education, Training and Awareness (SETA) program they are able to educate the users in ways that would reduce the number of incidents as well as possibly make them more aware and report noticed oddities faster. Having them involved in a program of this sort also lets the users of the organization meet and get to know the members of the team. This helps when an incident occurs and the team has to interact with the users, they already know them and might work better with them to resolve the problem. An IRT can easily be seen as a "police force" if never seen by and interacted with end-users. They could only be seen as the bearer of bad news [9] if never given the chance to dispense their knowledge in a way that could prevent the need for their services so often. If responders are invisible beforehand and never appear until things go wrong, they can be perceived as adversarial. The better the relationship before a security event happens, the less disruptive the responders will seem while it is trying to be resolved [9]. In going back to our earlier example of the stolen laptop, education of proper physical and electronic security might have prevented the user from leaving the laptop in a vulnerable place with no physical restraints. The user would have also been advised on proper encryption methods and keeping sensitive data such as social security numbers encrypted if put on a laptop or other unsecured devices such as PDA's or flash drives.

The IRT can also provide security alerts to the IT staff with known vulnerabilities and attack methods to make the system and network administrators more aware of attacks and vulnerabilities in order to help them plan upgrades and re-configurations if necessary. Site security consulting is another proactive service that the IRT could contribute to the IT staff. Since they are aware of cracking methods they could help design and advise on the logical layout of a new site, thus assisting in making the system more secure from the beginning [10]. A "Technology Watch" can be performed by the IRT. They will have the ability to look at new trends in InfoSec threats and be better prepared for handling new type of attacks. Monitoring security-related mailing lists as well as setting up and watching a honeypot can alert them in what to expect in the future so preparations can be made now to avoid the things that can be fixed or improved before an incident happens [4].

IV. PREVENTING PANIC THROUGH COMMUNICATION

One essential part of an Incident Response Team is having a designated leader or manager of the team. This position is one that needs to have direct communication with upper management in the time of an incident. The IRT manager would not be a technical part of the IRT, but rather the one who can help coordinate and dispense critical information to not only upper management but middle as well. He or she should have a familiarity with computer security issues and the function of IT areas and staff as well as general practices of the organization [11]. They would have the ability to effectively communicate and cooperate with all other managers in order to make them aware of the occurrence of an incident and assist in the facilitation of decisions that need to be made by such management [1]. They could also be the Primary Point of Contact in which users and/or managers could communicate the discovery of an incident. Having this person on the team keeps the technical members able to keep working while the chain of communication is continuing. It could be a distraction for the members of the team to have to stop several times an hour and give an update to different managers to whom the incident is affecting. This can hinder the progress as well as frustrate the team members trying to identify and contain the event. Having a manager that would handle all the communication and relaying of critical information takes that unnecessary burden off the team members that are better suited in resolving the problem than in relaying to management what the problem is and what part of the network it is affecting. That is not to say that team members might not be called on to give a "technical briefing" if necessary and would add necessary input to decisions that need to be made by management, such as having to go to the press or board members to report the incident. An "Incident Manager" can not only provide meaningful input to the incident procedure but field the hierarchy issues that are part of the incident [12]. This person would be adept in communicating to management in clear and precise terms that are articulated in business risk details. The Incident Manager needs to relay to management how things are going and give updates to how well contained the incident is. A relationship between the incident manager and the legal department should be encouraged as they will become a necessary part of the procedure if the incident is large enough.

If management is not updated regularly and given the appropriate information, panic can ensue. In the absence of information, rumors may spread and unduly give the incident a worse reputation than is actually true. This can cause a great uneasiness in management and may cause them to doubt whether the IRT has the incident under control, or may jump the gun and go to the press too early in an incident that turns out to be a false alarm. The briefings to management should be handled in an established routine [12]. All briefing documents should live in the Incident Response Security Policy so that they are readily assessable when needed. They should be templates that can be filled out quickly for giving the necessary updates at different stages during the event. All language should be clear and not too technical as the audience will most likely not come from a technical background. These

forms can not only be used for incidents but can be used to brief them on successful security issues such as appropriate patches and upgrades that have been done to eliminate risk. Keeping these forms seen on a more or less regular basis lets management get to know and trust the forms, not seeing them as always a potential problem. This will psychologically lead them to trust in the information on the form, which is what really matters [12].

Strong communication channels between staff and management should be established [7]. This can be accomplished by having test runs of an actual incidents and practicing the chain of communication that needs to take place as well as test out the forms and work out any problems that arise during these tests before an actual incident happens. This can help to eliminate the administrative problems that might arise and hinder the decisions that need to be made by management to continue the incident response process. This also serves to familiarize management with the Incident Manager and how things should be handled, it lets them know what to expect as well as calm any doubts that can arise during the procedure.

V. Conclusion

Security incidents are something that are not wanted, but should be expected by all parts of the organization. Some can be avoided with proper training and education of users, and some can only be dealt with after they have happened. Having a well prepared plan can indeed be half the battle. It takes all the panic away from not only the technicians having to deal with incident in that it gives them a plan of action that can be put into play in a moments notice. It also takes the panic caused by lack of communication out of management when someone is available to give them much needed updates. Incident response can be a well planned out program of the Information Security Department of any organization if only they put in the necessary time to prepare for the events before they happen. In our story of the stolen laptop told earlier the chain of communication would have to go all the way to top management and then be communicated effectively to all users that were affected by the stolen information. This can seem like a daunting task if there is no incident manager or they do not have a well formed relationship with top management and the legal department. As with all programs in Information Security it all begins with a well defined policy, one that is living and always adapting to changes in the organization as well as changes in the electronic world in which organizations do business. Incidents should and can be managed without letting the incidents manage you.

References

[1] * Sarandis Mitropoulos, Dimitrios Patsos, and Chistos Douligeris "On Incident Handling and Response: A state-of-the-art approach," *Computers & Security*, 2005.

[2] * Dario Forte, "Assembling an incident response team in small-to-medium organizations," *Computer Fraud and Security,* vol. 2004, Issue 2, February 2004, pp. 9-10.

[3] * Joao Nuno Ferreira, Alf Hansen, Tomaz Klobucar, Klaus-Peter Kossakowski, Manuel Medina, Damir Rajnovic, Olaf Schjelderup, and Don Stikvoort, "CERTs In Europe," *Computer Networks and ISDN Systems*, vol. 28, Issue 14, November 1996, pp. 1947-1952.

[4] Tim Grance, Karen Kent, and Brian Kim (2004). Computer Security Incident Handling Guide (Special Publication 800-61). National Institute of Standards and Technology.

[5] * Charles Cresson Wood, "The Charles Cresson Wood File," *Information Management & Computer Secuirty,* vol. 3, Issue 4, October 1995, pp. 23-26.

[6] * Peter Stephenson, "Managing digital incidents- a background," *Computer Fraud and Security,,* vol. 2004, Issue 12, December 2004, pp. 17-19.

[7] * DrE. Eugene Schultz, "Aligning disaster recovery and security incident response," *Computers and Security,* vol. 24, Issue 7, October 2005, pp. 505-506.

[8] J. Hamdi Krichene and N. M. Boudriga, "Collective computer incident response using cognitive maps," *IEEE International Conference on Systems, Man and Cybertronics*, vol. 1, pp. 1080-1085, October 2004.

[9] * Eve Edelson, "Incident Response: Breaking it Gently," *Computer Fraud and Security,* vol. 2003, Issue 9, September 2003, pp. 6-8.

[10] N. Brownlee and E. Guttman (1998), "RFC2350: Expectations for Computer Security Incident Response," *Internet RFCs,* published 1998.

[11] Richard L. Rollason-Reese, "Incident Handling: an orderly response to unexpected events," *ACM SIGUCCS 31st Annual Conference,* 2003, pp. 97-102.

[12] * Matthew Pemble, "P-P-preventing the P-P-panic during incident response," *Computer Fraud and Security,* vol. 2003, Issue 12, December 2003, pp. 14-16.