Appendix H

Guidance on Structuring the Incidence Response Handling Team

Introduction

The context for this appendix comes from the discussion in Section 9.9 (Incident Handling: An Essential Component of Cybersecurity) in Chapter 9. This appendix should be used with cybersecurity incident management-related discussion throughout Chapter 9 (Section 9.2.1, Fig. 9.11, Table 9.2).

Computer Security Incident Response Teams (CSIRT) was mentioned in Chapter 9, and will be used in the appendix too. Incident classification has been explained in Chapter 9 and therefore that is not explained here. The need for having an incident response team is also explained in Section 9.9.2 in Chapter 9 and that is the background for the team structuring-related discussion in this appendix. Do also refer to Part II of Appendix F where "Incident management" was explained in the context of forensic readiness of an organization.

Putting Incident Response Team in Context

"Incident response" if often understood and treated as "incident response team" then it is not right. Although it may appear logical at the surface, however, using the two terms synonymously is often unrealistic. People who are not very knowledgeable about the process of incident response often get drawn in dealing with security-related incidents. Let us consider one example described below.

Suppose a worm infects many computer systems. Users might work together to analyze what went wrong and to battle the worm. However, even when users do that they cannot be called as an incident response team. This is because an "incident response team" is a "competence" that is required for dealing with potential or real information security incidents. An "incident response team" is characterized by "mission" in terms of job-related responsibilities, assigned to each. An incident response team is entrusted with the responsibility of dealing with incidents as part or the entire job descriptions of the individuals involved.

An often asked question is "how many individuals must be involved in an incident response effort to form a team together? When incident handling hard work is completed, the others involved in the incident are released from any responsibilities they handled while dealing with incident. However, the Incident Response Team has the ongoing, day-to-day responsibility of handling incidents and will have to deal with the next incident that occurs.

Decision Whether Team or No Team

Some of the advantages of forming a response team have been presented in Section 9.9. However, organizations still have the choice of not having a full-time/dedicated incident response team. Depending on organizations' business circumstances and operating scenario, it may not always be advantageous to create such a team. An option is to have individuals who are not full-time member of an incident response team but who are available (usually on the basis of an SLA, i.e., "service level agreement" between various business units of the organization) as and when incidents take place. It is worth noting that an SLA (mentioned above) constitutes specifying, at a minimum, how many hours in a given period (week, month or year) an individual from one organization is available for undertaking incident response activities. SLA arrangement provides an assurance that the individual devoted to the activities will be paid by the business unit utilizing his/her time and services for handling incidents along with timely response.

This approach would make sense for smaller organizations given that smaller organizations are not likely to have internal structure to support full-time/dedicated incident response teams, creating policy and procedures and related activities get treated as a non-priority matter while more immediately pressing issues (business survival) get priority attention. Therefore, for small organizations, forming an incident response team would be an overkill.

Shortage of resources, mainly human resources, is quoted as one of the major reasons for not forming an incident response team. From a security viewpoint, this is not a very good reason, lack of resources is indeed a problem for information security efforts more often than not.

There are organizations, where incident response may work better as a distributed effort. Different individuals from different divisions/groups/business units can be ushered whenever an incident of sizable magnitude or impact takes place. Under this type of arrangement those divisions/groups/business units may be comfortable because they may feel a sense of direct control over the incident response process. This is because some of their own staff members will be involved in handling their own incidents. In addition, a distributed effort model can help making sure that people involved in handling security incidents will be those who know and understand how individual units operate, how the systems and networks are configured and maintained, and how the applications work. Eventually, this can lead to better insight into what should and should not be done for resolution of each incident to an intended level of satisfaction.

Forming the Team

Having decided to have the team, forming an incident response team, in general, is not as easy as it may appear at the surface. The team members charged with this responsibility must handle many key issues such as the policy, whether or not a team is really required, defining and communicating with a community, defining functional requirements, defining the role of the incident response team, staffing the team properly, and creating and updating operational procedures. These issues are discussed now in this section. “Policy” is the most important issue in forming and managing an incident response team. An incident response team ought to always work within the policy constraints of the organization where it belongs or with a unit it serves.

Let us consider a couple of scenarios: Suppose an organization mandates that employees shall not interact with media/publicity/press unless that person obtains written approval from the head of the public relations department. There could be a policy provision in yet another organization stating that a computer system/network system/application under attack must be disconnected from the network if it holds extremely valuable resources (such as proprietary data, proprietary source code, etc.). Over and above this, an incident response team might enforce its own policy provisions for its own operations. As per this kind of policy provision it might be that a team member shall not publish information about any incident outside of the immediate team without the direct permission of the team leader. Failure to conform to existing policy could result in a disciplinary action against an incident response team; penalty could range from embarrassment to termination of employment or even to dissolution of the team itself.

Skill Sets to Look for: Incident Response Team

“Skills” and “competencies” are very important for the success of an incident response team; they are summarized in Table H.1.

Table H.1 Skills and competencies of incident response team

Skills/Ability/Competence	***Why it is Important***
Coordination skills	Coordinating the efforts of individuals, who are on an incident response team, are easy generally because they by and large report to the team leader, who can direct them to take charge of one particular activity or another.
Expertise in handling complex situations	Information security incidents were mentioned in Chapter 9 – they are becoming increasingly

	complex. Therefore, having *incident handling experts* becomes even more necessary. Although "Technical Gurus" can contribute greatly when incidents occur, pure technical expertise in itself is not adequate when it comes to many incidents. Experience with past incidents, knowing what policies to consider and procedures to follow, and so forth are just as critical, if not more critical, than pure technical skills. Serving on a dedicated incident response function is one of the best ways to build expertise.
Work efficiency	In today's world, given the complexity of business and obsolescence of technology, "collaborative wisdom" and "collective intelligence" are more important than individual knowledge and skills. A team builds a collective knowledge that often leads to achieve higher efficiency (see Ref. # 4 in Books, Further Reading). On the other hand, a lone worker, that is, an isolated individual has the risk of going off course in dealing with an incident. Collective wisdom developed within a team can help to keep the incident response efforts on track. Also, a team (as opposed to any individual or a few independent individuals) is more likely to develop and follow procedures for incident response, something that is very important for "process-centric" organizations for demonstrating repeatable results expected by maturity models.
Ability to work proactively	Being proactive means taking up actions that address incident response needs before incidents actually occur. Being proactive is one of the key success factors for incident response effort. Getting users and system administrators trained to recognize the symptoms of incidents and what to do (as well as what not to do) is a good example of a proactive effort.
Ability to meet multiple stakeholder requirements	Another benefit of having an incident response team is that a team is usually better suited for meeting agency or corporate requirements.

	The main reason is that a team has individuals who are geared toward the same assignment. Note that some government agencies and organizations go one step ahead in that they require (through a management directive or a policy statement) an incident response team be formed.
Smooth liaising ability	Response teams are more suitable in serving a liaison function than individuals because outside entities are not likely to learn and/or be motivated to deal with individuals. Having a team identity provides additional external visibility as well as reliability, both of which are more suited to the liaison function. A “team,” in many respects, mandates a certain degree of authenticity within internal and external organizations.
Ability to overcome organizational barriers	Organizational politics does affect the effort that occurs within an organization. Incident response teams, however, provide at least some degree of protection from politics that provide barriers to incident response efforts. The major reason is that these teams are likely to have more authority to take action. For example, closing systems that have been compromised at the super user level than individuals. Additionally, teams often engage individuals from a cross-section of organizations and groups, making them more politically pleasant within a range of an organization’s divisions and groups.

Challenges in Forming a Response Team

When organizations respond to the need for getting ready to address and avoid computer security incidents, the need for “Computer Security Incident Response Teams (CSIRTs)” arises. Computer security has been surviving to be accepted as a vital component of computer science. There is a need for CSIRTs to be accepted within the security domain. As new teams get formed, they are confronted with the hurdles of having to justify their very existence. CSIRT has just started to get support and understanding of the problems that they are trying to address. Even if they manage to surmount those challenges, they still have an additional challenge to face: The lack of documented information on how to effectively form and operate a CSIRT and gain respect for it.

Whenever a serious decision is based on a contact, using the wrong contact may result in leakage or revelation of vital information to unsuitable parties or (usually worse) to outsiders. It also shows a missing control and attention to detail within the CSIRT, which is bad for its reputation. Finding the right contacts for organizations is not always a simple task. For non-critical contacts, one can use publicly available resources, such as telephone directories or similar services available on CD-ROM or through a search on the Internet.

Considerations for Forming a Successful Incident Response Team

We end this appendix with key success factors (KSF) for a successful incident response team; the KSFs are as follows:

1. Identify the core team and key personnel (especially technical personnel) as these are people you feel are competent to deal with incidents and obtain contact and other information.
2. Establish some kind of brass tacks or agreements regarding the availability of people who could be vital in handling incidents. Try to get an assurance from management that there will be a minimum number of hours of participation (per week, month or year) from each individual who might be involved. Try to obtain assurance that even more hours of support will be available in the case of a severe incident.
3. Be practical in dealing with organizations that make individuals available for incident response support. Sometimes, having such individuals participate in incident handling gets their focus away from their own missions. Do not have excessive demand and be ready for a "no" answer. Sometimes, grinding pressures for project delivery (e.g., meeting a major project milestone), an organization might decline to allow someone from that organization to deal with an incident. Having a back-up team (so that if one person is not available, another one can be put on the job) is thus essential.
4. Make sure that everyone, who is likely to help in dealing with incidents, is taken through appropriate training and orientation. Ensure that everyone is provided at least a minimum level of knowledge about responding to incidents and that everyone understands the importance of cooperation and teamwork (see Table H.1);
5. As far as possible, resolve leadership and authority issues in advance. In case of some incidents, having someone in charge is essential to success. On the other hand, having many people think they are in charge is extremely counterproductive.
6. Avoid calling on the individuals who are available for incident response support unless they are really needed. Remember that each time you call on such individual, you are disrupting some other business unit or group's work. You will wear out your welcome if you call on these individuals too much or if you cry wolf, that is, you call them into too many false alarms.

If your incidents are complex, establish a committee or board to monitor incident response activities. Have this body analyze crucial aspects such as challenges in obtaining personnel support, efficiency of incident response activity and others (see Table H.1). This body might be involved in pointing out to management issues that need attention and improvement (e.g., staffing issues) and might prove to be helpful in forming a timely CSRIT.

Further Reading

Additional Useful Web References

1. Read article *CIRT is an Essential Security Strategy for Every Indian Organization* at: http://searchsecurity.techtarget.in/news/1370715/CIRT-is-an-essential-security-strategy-for-every-Indian-organization (15 January 2011).
2. Read article *The Data Security Incident Management Process: Policies, Teams, and Communication* at: http://www.brighthub.com/computing/enterprise-security/articles/3098.aspx (18 January 2011).
3. Read article *Forming an Effective Incident Response Team: What's Your Mission?* at: http://www.informit.com/articles/article.aspx?p=102614# (19 January 2011).

4. **4.** Read SEI article *Creating a Computer Security Incident Response Team: A Process for Getting Started* at:
http://www.cert.org/csirts/Creating-A-CSIRT.html (21 January 2011).
5. **5.** Read article *Challenges of Managing Data Security; Causes and Effects of Data System Failures* at: http://www.brighthub.com/computing/enterprise-security/articles/3105.aspx (12 January 2011).

6. **6.** Read article *Recovering Corporate Data After a Data Security Attack* at:
http://www.brighthub.com/computing/enterprise-security/articles/3104.aspx (20 January 2011).
7. **7.** Read article *Responding to IT Security Incidents* at:
http://technet.microsoft.com/en-us/library/cc700825.aspx (21 January 2011).
8. **8.** Read article *Does Your Company Have A Computer Incident Response Team (CIRT)?* at:
http://www.collegedays.in/coll/techie/uncategorized/does-your-company-have-a-computer-incident-response-team-cirt/

Books

1. Lucas, J. and Moeller, B. (2004) *Effective Incident Response Team,* Addison-Wesley, Boston.
2. Mandia, K. and Prosise, C. (2003) *Incident Response and Computer Forensics,* McGraw Hill/Osborne, USA.
3. Schultz, E.E. and Shumway, R. (2002) *Incident Response: A Strategic Guide to Handling Systems and Network Security Breaches*, New Riders.
4. Marcus, R. and Waters, B. (2002) *Collective Knowledge*, Microsoft Press, Washington, USA.