Defining Computer Security Incident Response Teams

Robin Ruefle

January 2007

ABSTRACT: A computer security incident response team (CSIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. CSIRTs can be created for nation states or economies, governments, commercial organizations, educational institutions, and even non-profit entities. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.

INTRODUCTION

Incident management includes detecting and responding to computer security incidents as well as protecting critical data, assets, and systems to prevent incidents from happening. Responding to computer security incidents does not happen in isolation. Actions taken to prevent or mitigate ongoing and potential computer security events and incidents can involve tasks performed by a wide range of participants across the enterprise. Participants include security analysts, incident handlers, network and system administrators, human resources and public affairs staff, information security officers (ISOs), C-level managers (such as chief information officers [CIOs], chief security officers [CSOs], chief risk officers [CROs]), and other managers, product developers, and even end users. One particular organizational entity that may be established to help coordinate and manage the incident management process in an organization is a computer security incident response team (CSIRT).

This article describes CSIRTs and their role in preventing, detecting, analyzing, and responding to computer security incidents.

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

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

WHAT IS A CSIRT?

A CSIRT is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility of providing part of the incident management capability for a particular organization. When a CSIRT exists in an organization, it is gen-

erally the focal point for coordinating and supporting incident response. By definition, a CSIRT must perform—at a minimum—incident handling activities [Killcrece 2002]. This entails analyzing and resolving events and incidents that are reported by end users or are observed through proactive network and system monitoring.

CSIRT incident handling activities include

- determining the impact, scope, and nature of the event or incident
- understanding the technical cause of the event or incident
- identifying what else may have happened or other potential threats resulting from the event or incident
- researching and recommending solutions and workarounds
- coordinating and supporting the implementation of the response strategies with other parts of the enterprise or constituency,1 including IT groups and specialists, physical security groups, information security officers (ISOs), business managers, executive managers, public relations, human resources, and legal counsel
- disseminating information on current risks, threats, attacks, exploits, and corresponding mitigation strategies through alerts, advisories, Web pages, and other technical publications
- coordinating and collaborating with external parties such as vendors, ISPs, other security groups and CSIRTs, and law enforcement
- maintaining a repository of incident and vulnerability data and activity related to the constituency that can be used for correlation, trending, and developing lessons learned to improve the security posture and incident management processes of an organization

A CSIRT has specialized knowledge of intruder attacks and threats as well as mitigation and resolution strategies. It understands the escalation process and works to communicate relevant information to stakeholders and customers in a timely and effective manner. In addition, a CSIRT may

- recommend best practices regarding secure configurations, defense-in-depth strategies for protecting systems, networks, and critical data and assets, and incident prevention
- perform or participate in vulnerability assessment and handling, artifact analysis,2 computer forensics evidence collection and analysis, systems and network monitoring, security policy development, and security and awareness training and education3
- provide input into or participate in security audits or assessments such as infrastructure reviews, best practice reviews, vulnerability scanning, or penetration testing

- conduct public monitoring or technology watch activities such as reviewing security Web sites, mailing list, or general news and vendor sites to identify new or emerging technical developments, intruder activities, future threats, legal and legislative rulings, social or political threats, or new defensive strategies
- support legal and law enforcement efforts through the collection and analysis of forensics evidence (provided that staff have the appropriate expertise, training, and tools)

The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective response and recovery, and work to prevent future incidents from happening.

However, a CSIRT also can—and should—provide true business intelligence to its parent organization or constituency by virtue of

- the information it collects on the types of threats and attacks that currently impact or could potentially threaten the enterprise
- its expertise in general intruder attacks and trends and corresponding mitigation strategies
- its understanding of infrastructure and policy weakness and strengths based on performed incident postmortems

CSIRT Purpose

CSIRTs can vary in purpose based on sector. For example, law enforcement CSIRTs may focus on prosecuting cybercrime incidents by collecting and analyzing computer forensics data from affected or involved systems. Government CSIRTs, on the other hand, may be involved in security awareness training and general incident handling activities but never perform any forensics activities. Forensics activities may be handled by special investigators within the government agencies instead.

CSIRT Processes Must Support the Enterprise

As organizations become more complex and capabilities such as CSIRTs become more integrated into organizational business functions, it is clear that incident management is not just the application of technology to resolve computer security events. It is also the development of a plan of action, which is a set of processes that are consistent, repeatable, of high quality, measurable, and understood within the constituency. To be successful, the CSIRTs incident response plan should be built to sustain mission-critical services and protect corresponding assets and data in the face of attacks and other malicious activity. To do this,

the plan should integrate into existing processes and organizational structures so that it enables rather than hinders critical business functions. The plan should also support, complement, and provide input into existing business and IT policies that impact the security of an organization's infrastructure, just like any other incident management processes. CSIRT operations, as part of an incident management capability, should establish processes for

- notification and communication
- analysis, response, and resolution
- collaboration and coordination
- maintenance and tracking of records
- evaluation and quality assurance

A properly structured and implemented CSIRT can be a focal point for interaction and coordination to ensure that such a plan not only exists but has proper buy-in and support throughout the enterprise.

CSIRT Structure

A CSIRT can take many forms or organizational structures. It can be a separate entity with staff assigned to perform incident handling and related activities 100% of the time, or it can be an ad hoc group that is pulled together, based on members' expertise and responsibility, when a computer security incident occurs.

An ad hoc CSIRT, though, has a harder time participating in proactive activities such as security and awareness training, security assessments, security information dissemination, and network monitoring because their day-to-day activities are not necessarily incident response related.

Regardless of its form or structure, a CSIRT provides a stable cadre of staff with incident handling expertise who understand the functional business processes of their organization as well as the general nature of their network infrastructure. This allows for a more focused, rapid, and standardized response effort. It is the CSIRT, generally, working in collaboration with other IT and security experts, that determines (a) how an attack or threat will impact an infrastructure, (b) which methods to use to contain and eradicate attacks and threats, (c) which methods to use to verify that normal operations can be resumed, and (d) who updates and alerts relevant stakeholders on the status of the threat and the response actions that need to be implemented.

Incident Tracking and Correlation

Most CSIRTs maintain some type of incident tracking database or system to record information about reported incidents and any response actions taken to resolve or mitigate the incident. Such a system allows any incoming incident report to be correlated against existing incidents to determine if they are related or part of a larger incident. Such a tracking system also allows team members to quickly find mitigation strategies and response steps used to resolve incidents so that research time and analysis can be reduced, possibly leading to a more timely response and decreasing the impact on constituency systems.

Similar types of tracking systems are also maintained to track reported vulnerabilities and actions taken to mitigate them. Using incident and vulnerability tracking systems can allow information to be correlated across incidents to determine any interrelationships, patterns, common intruder signatures, common targets, or common vulnerabilities being exploited. Typical information that may be correlated includes IP address; hostnames; ports, protocols, services, applications, or operating systems used or exploited; and organizational sector or business functions affected. Such analysis can identify relationships between malicious attacks and exploited vulnerabilities. Based on the output of correlation activities, trend analysis can be done to determine emerging attack patterns and security problems that need to be addressed.

Performing Incident Postmortems

CSIRTs are also involved in improvement activities. After major computer security incidents occur, or when incidents are not handled in a timely or effective manner, a CSIRT will generally perform a postmortem of the incident and its response. This postmortem will identify the strengths and weakness of the response effort. Such reviews can identify weaknesses and holes in systems, infrastructure defenses, or policies that allowed the incident to take place. It can also identify problems with communication channels, interfaces, and procedures that inhibited the efficient resolution of the reported problem.

CSIRTs in Software Development Organizations

CSIRTs can be established in all kinds of organizations: government, commercial, law enforcement, educational, and even software development. The latter may even require two types of CSIRT within the organization:

- a product or vendor CSIRT that handles problems from the customers relating to security vulnerabilities in the developed software
- an organizational CSIRT that provides incident handling for issues relating to the vendor organization's own internal systems, networks, and data

The reason that two teams are needed is to avoid a conflict of interest between customer issues and internal organizational issues.

The product CSIRT would receive and investigate reports of vulnerabilities in the software or hardware products produced by their parent entity. The product CSIRT might work with other CSIRTs or security experts such as the CERT Coordination Center (CERT/CC) or Internet Security Systems (ISS) to define and understand the technical characteristics of the vulnerability and any related exploits. The product team would also work with others to

- define the scope and impact of the problem (how many platforms, what other software may be affected, and the results of any exploitation)
- develop a resolution strategy (such as a patch or workaround)
- disseminate the information in a bulletin or advisory to its customers and possibly the general public

The organizational CSIRT would receive incident reports for suspicious activity related to internal company assets. They may also monitor organizational networks and systems for malicious activity, and coordinate the resolution of any incidents within the enterprise.

If the software product is sold or used by other organizations, those organizations internal CSIRTs may also have valuable information on security issues related to the software. Customers' internal CSIRTs are probably dealing with incidents relating to the use of the software in a production environment. They may have additional information about threat environments, usability issues, and problems encountered when the software is used in a real business context that can be useful to the software developers. These organizational customer CSIRTs can also provide feedback on whether the design and support of the software facilitates or hinders incident response.

SUMMARY

Various acronyms and titles have been given to CSIRT organizations over the years. These titles include

- CSIRT - Computer Security Incident Response Team
- CSIRC - Computer Security Incident Response Capability or Center
- CIRC - Computer Incident Response Capability or Center
- CIRT - Computer Incident Response Team
- IHT - Incident Handling Team
- IRC - Incident Response Center or Incident Response Capability

- IRT - Incident Response Team
- SERT - Security Emergency Response Team
- SIRT - Security Incident Response Team

Depending on the organization's structure, some teams have a broader title along with a broader scope, such as security team, crisis management team, or even resiliency team.

Another acronym used by various organizations, especially countries setting up a centralized incident management coordination capability, is CERT.4

All of these titles, however, still refer to the same basic type of organization, one that provides services and support, to a defined constituency, for preventing, handling and responding to computer security incidents. Although their purpose and structure may be different, they still perform similar functions to detect, analyze, and mitigate computer security incidents. This ensures that critical business assets and data are protected and that incidents are handled in a repeatable, quality-driven manner.

REFERENCES

[Killcrece 2002]

Killcrece, Georgia; Kossakowski, Klaus Peter; Ruefle, Robin; & Zajicek, Mark. *CSIRT Services*. (2002).

[Killcrece 2005]

Killcrece, Georgia. "Incident Management." *Build Security In*. (2005).

[West Brown 2003]

West Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark.*Handbook for Computer Security Incident Response Teams (CSIRTs)*(CMU/SEI-2003-HB-002, ADA413778). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

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

DM-0001120