Network Working Group
Request for Comments: 2350
BCP: 21
Category: Best Current Practice

N. Brownlee
The University of Auckland
E. Guttman
Sun Microsystems

June 1998

Expectations for Computer Security Incident Response

Status of this Memo

Copyright Notice

Abstract

The purpose of this document is to express the general Internet community's expectations of Computer Security Incident Response Teams (CSIRTs). It is not possible to define a set of requirements that would be appropriate for all teams, but it is possible and helpful to list and describe the general set of topics and issues which are of concern and interest to constituent communities.

CSIRT constituents have a legitimate need and right to fully understand the policies and procedures of 'their' Computer Security Incident Response Team. One way to support this understanding is to supply detailed information which users may consider, in the form of a formal template completed by the CSIRT. An outline of such a template and a filled in example are provided.

Table of Contents

1 Introduction

The GRIP Working Group was formed to create a document that describes the community's expectations of computer security incident response teams (CSIRTs). Although the need for such a document originated in the general Internet community, the expectations expressed should also closely match those of more restricted communities.

In the past there have been misunderstandings regarding what to expect from CSIRTs. The goal of this document is to provide a framework for presenting the important subjects (related to incident response) that are of concern to the community.

Before continuing, it is important to clearly understand what is meant by the term "Computer Security Incident Response Team." For the purposes of this document, a CSIRT is a team that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency (see Appendix A for a more complete definition). Any group calling itself a CSIRT for a specific constituency must therefore react to reported security incidents, and to threats to "their" constituency in ways which the specific community agrees to be in its general interest.

Since it is vital that each member of a constituent community be able to understand what is reasonable to expect of their team, a CSIRT should make it clear who belongs to their constituency and define the services the team offers to the community. Additionally, each CSIRT should publish its policies and operating procedures. Similarly, these same constituents need to know what is expected of them in order for them to receive the services of their team. This requires that the team also publish how and where to report incidents.

This document details a template which will be used by CSIRTs to communicate this information to their constituents. The constituents should certainly expect a CSIRT to provide the services they describe in the completed template.

It must be emphasized that without active participation from users, the effectiveness of the CSIRT's services can be greatly diminished. This is particularly the case with reporting. At a minimum, users need to know that they should report security incidents, and know how and to where they should report them.

Many computer security incidents originate outside local community boundaries and affect inside sites, others originate inside the local community and affect hosts or users on the outside. Often, therefore, the handling of security incidents will involve multiple sites and potentially multiple CSIRTs. Resolving these incidents will require cooperation between individual sites and CSIRTs, and between CSIRTs.

Constituent communities need to know exactly how their CSIRT will be working with other CSIRTs and organizations outside their constituency, and what information will be shared.

The rest of this document describes the set of topics and issues that CSIRTs need to elaborate for their constituents. However, there is no attempt to specify the "correct" answer to any one topic area. Rather, each topic is discussed in terms of what that topic means.

Chapter two provides an overview of three major areas: the publishing of information by a response team, the definition of the response team's relationship to other response teams, and the need for secure communications. Chapter three describes in detail all the types of information that the community needs to know about their response team.

For ease of use by the community, these topics are condensed into an outline template found in Appendix D. This template can be used by constituents to elicit information from their CSIRT.

It is the working group's sincere hope that through clarification of the topics in this document, understanding between the community and its CSIRTs will be increased.

2 Scope

The interactions between an incident response team and its constituent community response team require first that the community understand the policies and procedures of the response team. Second, since many response teams collaborate to handle incidents, the community must also understand the relationship between their response team and other teams. Finally, many interactions will take advantage of existing public infrastructures, so the community needs to know how those communications will be protected. Each of these subjects will be described in more detail in the following three sections.

2.1 Publishing CSIRT Policies and Procedures

Each user who has access to a Computer Security Incident Response Team should know as much as possible about the services of and interactions with this team long before he or she actually needs them.

A clear statement of the policies and procedures of a CSIRT helps the constituent understand how best to report incidents and what support to expect afterwards. Will the CSIRT assist in resolving the incident? Will it provide help in avoiding incidents in the future? Clear expectations, particularly of the limitations of the services provided by a CSIRT, will make interaction with it more efficient and effective.

There are different kinds of response teams: some have very broad constituencies (e.g., CERT Coordination Center and the Internet), others have more bounded constituencies (e.g., DFN-CERT, CIAC), and still others have very restricted constituencies (e.g., commercial response teams, corporate response teams). Regardless of the type of response team, the constituency supported by it must be knowledgeable about the team's policies and procedures. Therefore, it is mandatory that response teams publish such information to their constituency.

A CSIRT should communicate all necessary information about its policies and services in a form suitable to the needs of its constituency. It is important to understand that not all policies and procedures need be publicly available. For example, it is not necessary to understand the internal operation of a team in order to interact with it, as when reporting an incident or receiving guidance on how to analyze or secure one's systems.

In the past, some teams supplied a kind of Operational Framework, others provided a Frequently Asked Questions list (FAQ), while still others wrote papers for distribution at user conferences or sent newsletters.

We recommend that each CSIRT publish its guidelines and procedures on its own information server (e.g. a World Wide Web server). This would allow constituents to easily access it, though the problem remains of how a constituent can find his or her team; people within the constituency have to discover that there is a CSIRT "at their disposal."

It is foreseen that completed CSIRT templates will soon become searchable by modern search engines, which will aid in distributing information about the existence of CSIRTs and basic information required to approach them.

It would be very useful to have a central repository containing all the completed CSIRT templates. No such repository exists at the time of writing, though this might change in the future.

Regardless of the source from which the information is retrieved, the user of the template must check its authenticity. It is highly recommended that such vital documents be protected by digital signatures. These will allow the user to verify that the template was indeed published by the CSIRT and that it has not been tampered with. This document assumes the reader is familiar with the proper use of digital signatures to determine whether a document is authentic.

2.2 Relationships between different CSIRTs

In some cases a CSIRT may be able to operate effectively on its own and in close cooperation with its constituency. But with today's international networks it is much more likely that most of the incidents handled by a CSIRT will involve parties external to its constituency. Therefore the team will need to interact with other CSIRTs and sites outside its constituency.

The constituent community should understand the nature and extent of this collaboration, as very sensitive information about individual constituents may be disclosed in the process.

Inter-CSIRT interactions could include asking other teams for advice, disseminating knowledge of problems, and working cooperatively to resolve a security incident affecting one or more of the CSIRTs' constituencies.

In establishing relationships to support such interactions, CSIRTs must decide what kinds of agreements can exist between them so as to share yet safeguard information, whether this relationship can be disclosed, and if so to whom.

Note that there is a difference between a peering agreement, where the CSIRTs involved agree to work together and share information, and simple co-operation, where a CSIRT (or any other organization) simply contacts another CSIRT and asks for help or advice.

Although the establishment of such relationships is very important and affects the ability of a CSIRT to support its constituency, it is up to the teams involved to decide about the details. It is beyond the scope of this document to make recommendations for this process. However, the same set of information used to set expectations for a user community regarding sharing of information will help other parties to understand the objectives and services of a specific CSIRT, supporting a first contact.

2.3 Establishing Secure Communications

Once one party has decided to share information with another party, or two parties have agreed to share information or work together - as required for the coordination of computer security incident response - all parties involved need secure communications channels. (In this context, "secure" refers to the protected transmission of information shared between different parties, and not to the appropriate use of the information by the parties.)

The goals of secure communication are:

- Confidentiality:
  Can somebody else access the content of the communication?

- Integrity:
  Can somebody else manipulate the content of the communication?

- Authenticity:
  Am I communicating with the "right" person?

It is very easy to send forged e-mail, and not hard to establish a (false) identity by telephone. Cryptographic techniques, for example Pretty Good Privacy (PGP) or Privacy Enhanced Mail (PEM) can provide effective ways of securing e-mail. With the correct equipment it is also possible to secure telephone communication. But before using such mechanisms, both parties need the "right" infrastructure, which is to say preparation in advance. The most important preparation is ensuring the authenticity of the

cryptographic keys used in secure communication:

- Public keys (for techniques like PGP and PEM):
  Because they are accessible through the Internet, public keys must be authenticated before use. While PGP relies on a "Web of Trust" (where users sign the keys of other users), PEM relies on a hierarchy (where certification authorities sign the keys of users).

- Secret keys (for techniques like DES and PGP/conventional encryption): Because these must be known to both sender and receiver, secret keys must be exchanged before the communication via a secure channel.

Communication is critical to all aspects of incident response. A team can best support the use of the above-mentioned techniques by gathering all relevant information, in a consistent way. Specific requirements (such as calling a specific number to check the authenticity of keys) should be clear from the start. CSIRT templates provide a standardized vehicle for delivering this information.

It is beyond the scope of this document to address the technical and administrative problems of secure communications. The point is that response teams must support and use a method to secure the communications between themselves and their constituents (or other response teams). Whatever the mechanism is, the level of protection it provides must be acceptable to the constituent community.

3 Information, Policies and Procedures

In chapter 2 it was mentioned that the policies and procedures of a response team need to be published to their constituent community. In this chapter we will list all the types of information that the community needs to receive from its response team. How this information is communicated to a community will differ from team to team, as will the specific information content. The intent here is to clearly describe the various kinds of information that a constituent community expects from its response team.

To make it easier to understand the issues and topics relevant to the interaction of constituents with "their" CSIRT, we suggest that a CSIRT publish all information, policies, and procedures addressing its constituency as a document, following the template given in Appendix D. The template structure arranges items, making it easy to supply specific information; in Appendix E we provide an example of a filled-out template for the fictitious XYZ University. While no recommendations are made as to what a CSIRT should adopt for its policy or procedures, different possibilities are outlined to give

some examples. The most important thing is that a CSIRT have a policy and that those who interact with the CSIRT be able to obtain and understand it.

As always, not every aspect for every environment and/or team can be covered. This outline should be seen as a suggestion. Each team should feel free to include whatever they think is necessary to support its constituency.

3.1 Obtaining the Document

Details of a CSIRT change with time, so the completed template must indicate when it was last changed. Additionally, information should be provided concerning how to find out about future updates. Without this, it is inevitable that misunderstandings and misconceptions will arise over time; outdated documents can do more harm than good.

- Date of last update	This should be sufficient to allow anyone interested to evaluate the currency of the template.
- Distribution list	Mailing lists are a convenient mechanism to distribute up-to-date information to a large number of users. A team can decide to use its own or an already existing list to notify users whenever the document changes. The list might normally be groups the CSIRT has frequent interactions with. Digital signatures should be used for update messages sent by a CSIRT.
- Location of the document	The location where a current version of the document is accessible through a team’s online information services. Constituents can then easily learn more about the team and check for recent updates. This online version should also be accompanied by a digital signature.

3.2 Contact Information

Full details of how to contact the CSIRT should be listed here, although this might be very different for different teams; for example, some might choose not to publicize the names of their team members. No further clarification is given when the meaning of the item can be assumed.

- Name of the CSIRT
- Mailing Address
- Time zone — This is useful for coordinating incidents which cross time zones.
- Telephone number
- Facsimile number
- Other telecommunication — Some teams might provide secure voice communication (e.g. STU III).
- Electronic mail address
- Public keys and encryption — The use of specific techniques depends on the ability of the communication partners to have access to programs, keys and so on. Relevant information should be given to enable users to determine if and how they can make use of encrypted communication while interacting with the CSIRT.
- Team members
- Operating Hours — The operating hours and holiday schedule should be provided here. Is there a 24 hour hotline?
- Additional Contact Info — Is there any specific customer contact info?

More detailed contact information can be provided. This might include different contacts for different services, or might be a list of online information services. If specific procedures for access to some services exist (for example addresses for mailing list requests), these should be explained here.

3.3 Charter

Every CSIRT must have a charter which specifies what it is to do, and the authority under which it will do it. The charter should include at least the following items:

- Mission statement
- Constituency
- Sponsorship / affiliation
- Authority

3.3.1 Mission Statement

The mission statement should focus on the team's core activities, already stated in the definition of a CSIRT. In order to be considered a Computer Security Incident Response Team, the team must support the reporting of incidents and support its constituency by dealing with incidents.

The goals and purposes of a team are especially important, and require clear, unambiguous definition.

3.3.2 Constituency

A CSIRT's constituency can be determined in any of several ways. For example it could be a company's employees or its paid subscribers, or it could be defined in terms of a technological focus, such as the users of a particular operating system.

The definition of the constituency should create a perimeter around the group to whom the team will provide service. The policy section of the document (see below) should explain how requests from outside this perimeter will be handled.

If a CSIRT decides not to disclose its constituency, it should explain the reasoning behind this decision. For example, for-fee CSIRTs will not list their clients but will declare that they provide a service to a large group of customers that are kept confidential because of the clients' contracts.

Constituencies might overlap, as when an ISP provides a CSIRT which delivers services to customer sites that also have CSIRTs. The Authority section of the CSIRT's description (see below) should make such relationships clear.

3.3.3 Sponsoring Organization / Affiliation

The sponsoring organization, which authorizes the actions of the CSIRT, should be given next. Knowing this will help the users to understand the background and set-up of the CSIRT, and it is vital information for building trust between a constituent and a CSIRT.

3.3.4 Authority

This section will vary greatly from one CSIRT to another, based on the relationship between the team and its constituency. While an organizational CSIRT will be given its authority by the management of the organization, a community CSIRT will be supported and chosen by the community, usually in a advisory role.

A CSIRT may or may not have the authority to intervene in the operation of all of the systems within its perimeter. It should identify the scope of its control as distinct from the perimeter of its constituency. If other CSIRTs operate hierarchically within its perimeter, this should be mentioned here, and the related CSIRTs identified.

Disclosure of a team's authority may expose it to claims of liability. Every team should seek legal advice on these matters. (See section 3.7 for more on liability.)

3.4 Policies

It is critical that Incident Response Teams define their policies. The following sections discuss communication of these policies to the constituent community.

3.4.1 Types of Incidents and Level of Support

The types of incident which the team is able to address, and the level of support which the team will offer when responding to each type of incident, should be summarized here in list form. The Services section (see below) provides the opportunity to give more detailed descriptions, and to address non-incident-related topics.

The level of support may change depending on factors such as the team's workload and the completeness of the information available. Such factors should be outlined and their impact should be explained. As a list of known types of incidents will be incomplete with regard to possible or future incidents, a CSIRT should also give some background on the "default" support for incident types not otherwise mentioned.

The team should state whether it will act on information it receives about vulnerabilities which create opportunities for future incidents. A commitment to act on such information on behalf of its constituency is regarded as an optional proactive service policy rather than a core service requirement for a CSIRT.

3.4.2 Co-operation, Interaction and Disclosure of Information

This section should make explicit which related groups the CSIRT routinely interacts with. Such interactions are not necessarily related to the computer security incident response provided, but are used to facilitate better cooperation on technical topics or services. By no means need details about cooperation agreements be given out; the main objective of this section is to give the constituency a basic understanding of what kind of interactions are established and what their purpose is.

Cooperation between CSIRTs can be facilitated by the use of unique ticket number assignment combined with explicit handoff procedures. This reduces the chance of misunderstandings, duplications of effort, assists in incident tracking and prevents 'loops' in communication.

The reporting and disclosure policy should make clear who will be the recipients of a CSIRT's report in each circumstance. It should also note whether the team will expect to operate through another CSIRT or directly with a member of another constituency over matters specifically concerning that member.

Related groups a CSIRT will interact with are listed below:

Incident Response Teams:

A CSIRT will often need to interact with other CSIRTs. For example a CSIRT within a large company may need to report incidents to a national CSIRT, and a national CSIRT may need to report incidents to national CSIRTs in other countries to deal with all sites involved in a large-scale attack.

Collaboration between CSIRTs may lead to disclosure of information. The following are examples of such disclosure, but are not intended to be an exhaustive list:

- Reporting incidents within the constituency to other teams. If this is done, site-related information may become public knowledge, accessible to everyone, in particular the press.

- Handling incidents occurring within the constituency, but reported from outside it (which implies that some information has already been disclosed off-site).

- Reporting observations from within the constituency indicating suspected or confirmed incidents outside it.

- Acting on reports of incidents from outside the constituency.

- Passing information about vulnerabilities to vendors, to partner CSIRTs or directly to affected sites lying within or outside the constituency.

- Feedback to parties reporting incidents or vulnerabilities.

- The provision of contact information relating to members of the constituency, members of other constituencies, other CSIRTs, or law-enforcement agencies.

Vendors:
Some vendors have their own CSIRTs, but some vendors may not. In such cases a CSIRT will need to work directly with a vendor to suggest improvements or modifications, to analyze the technical problem or to test provided solutions. Vendors play a special role in handling an incident if their products' vulnerabilities are involved in the incident.

Law-enforcement agencies:
These include the police and other investigative agencies. CSIRTs and users of the template should be sensitive to local laws and regulations, which may vary considerably in different countries. A CSIRT might advise on technical details of attacks or seek advice on the legal implications of an incident. Local laws and regulations may include specific reporting and confidentiality requirements.

Press:
A CSIRT may be approached by the press for information and comment from time to time.

An explicit policy concerning disclosure to the press can be helpful, particularly in clarifying the expectations of a CSIRT's constituency. The press policy will have to clarify the same topics as above more specifically, as the constituency will usually be very sensitive to press contacts.

Other:
This might include research activities or the relation to the sponsoring organization.

The default status of any and all security-related information which a team receives will usually be 'confidential,' but rigid adherence to this makes the team to appear to be an informational 'black hole,' which may reduce the likelihood of the team's obtaining cooperation from clients and from other organizations. The CSIRT's template should define what information it will report or disclose, to whom, and when.

Different teams are likely to be subject to different legal restraints requiring or limiting disclosure, especially if they work in different jurisdictions. In addition, they may have reporting requirements imposed by their sponsoring organization. Each team's template should specify any such constraints, both to clarify users' expectations and to inform other teams.

Conflicts of interest, particularly in commercial matters, may also restrain disclosure by a team; this document does not recommend on how such conflicts should be addressed.

A team will normally collect statistics. If statistical information is distributed, the template's reporting and disclosure policy should say so, and should describe how to obtain such statistics.

3.4.3 Communication and Authentication

You must have a policy which describes methods of secure and verifiable communication that you will use. This is necessary for communication between CSIRTs and between a CSIRT and its constituents. The template should include public keys or pointers to them, including key fingerprints, together with guidelines on how to use this information to check authenticity and how to deal with corrupted information (for example where to report this fact).

At the moment it is recommended that as a minimum every CSIRT have (if possible), a PGP key available. A team may also make other mechanisms available (for example PEM, MOSS, S/MIME), according to its needs and the needs of its constituents. Note however, that CSIRTs and users should be sensitive to local laws and regulations. Some countries do not allow strong encryption, or enforce specific policies on the use of encryption technology. In addition to encrypting sensitive information whenever possible, correspondence should include digital signatures. (Please note that in most countries, the protection of authenticity by using digital signatures is not affected by existing encryption regulations.)

For communication via telephone or facsimile a CSIRT may keep secret authentication data for parties with whom they may deal, such as an agreed password or phrase. Obviously, such secret keys must not be

published, though their existence may be.

3.5 Services

Services provided by a CSIRT can be roughly divided into two categories: real-time activities directly related to the main task of incident response, and non-real-time proactive activities, supportive of the incident response task. The second category and part of the first category consist of services which are optional in the sense that not all CSIRTs will offer them.

3.5.1 Incident Response

Incident response usually includes assessing incoming reports about incidents ("Incident Triage") and following up on these with other CSIRTs, ISPs and sites ("Incident Coordination"). A third range of services, helping a local site to recover from an incident ("Incident Resolution"), is comprised of typically optional services, which not all CSIRTs will offer.

3.5.1.1 Incident Triage

Incident triage usually includes:

- Report assessment	Interpretion of incoming incident reports, prioritizing them, and relating them to ongoing incidents and trends.
- Verification	Help in determining whether an incident has really occurred, and its scope.

3.5.1.2 Incident Coordination

Incident Coordination normally includes:

- Information categorization	Categorization of the incident related information (logfiles, contact information, etc.) with respect to the information disclosure policy.
- Coordination	Notification of other involved parties on a need-to-know basis, as per the information disclosure policy.

3.5.1.3 Incident Resolution

Usually additional or optional, incident resolution services include:

- Technical Assistance — This may include analysis of compromised systems.
- Eradication — Elimination of the cause of a security incident (the vulnerability exploited), and its effects (for example, continuing access to the system by an intruder).
- Recovery — Aid in restoring affected systems and services to their status before the security incident.

3.5.2. Proactive Activities

Usually additional or optional, proactive services might include:

- Information provision — This might include an archive of known vulnerabilities, patches or resolutions of past problems, or advisory mailing lists.
- Security Tools — This may include tools for auditing a Site’s security.
- Education and training
- Product evaluation
- Site security auditing and consulting

3.6 Incident Reporting Forms

The use of reporting forms makes it simpler for both users and teams to deal with incidents. The constituent can prepare answers to various important questions before he or she actually contacts the team, and can therefore come well prepared. The team gets all the necessary information at once with the first report and can proceed efficiently.

Depending on the objectives and services of a particular CSIRT, multiple forms may be used, for example a reporting form for a new vulnerability may be very different from the form used for reporting

incidents.

It is most efficient to provide forms through the online information services of the team. The exact pointers to them should be given in the CSIRT description document, together with statements about appropriate use, and guidelines for when and how to use the forms. If separate e-mail addresses are supported for form-based reporting, they should be listed here again.

One example of such a form is the Incident Reporting Form provided by the CERT Coordination Center:

- ftp://info.cert.org/incident_reporting_form

3.7 Disclaimers

Although the CSIRT description document does not constitute a contract, liability may conceivably result from its descriptions of services and purposes. The inclusion of a disclaimer at the end of the template is therefore recommended and should warn the user about possible limitations.

In situations where the original version of a document must be translated into another language, the translation should carry a disclaimer and a pointer to the original. For example:

> Although we tried to carefully translate the original document from German into English, we can not be certain that both documents express the same thoughts in the same level of detail and correctness. In all cases, where there is a difference between both versions, the German version will prevail.

The use of and protection by disclaimers is affected by local laws and regulations, of which each CSIRT should be aware. If in doubt the CSIRT should check the disclaimer with a lawyer.

Appendix A: Glossary of Terms

This glossary defines terms used in describing security incidents and Computer Security Incident Response Teams. Only a limited list is included. For more definitions please refer to other sources, for example to the Internet User's Glossary [RFC 1983].

Constituency:
Implicit in the purpose of a Computer Security Incident Response Team is the existence of a constituency. This is the group of users, sites, networks or organizations served by the team. The team must be recognized by its constituency in order to be effective.

Security Incident:
For the purpose of this document, this term is a synonym of Computer Security Incident: any adverse event which compromises some aspect of computer or network security.

The definition of an incident may vary between organizations, but at least the following categories are generally applicable:

- Loss of confidentiality of information.
- Compromise of integrity of information.
- Denial of service.
- Misuse of service, systems or information.
- Damage to systems.

These are very general categories. For instance the replacement of a system utility program by a Trojan Horse is an example of ' compromise of integrity,' and a successful password attack is an example of 'loss of confidentiality.' Attacks, even if they failed because of proper protection, can be regarded as Incidents.

Within the definition of an incident the word 'compromised' is used. Sometimes an administrator may only 'suspect' an incident. During the response it must be established whether or not an incident has really occurred.

Computer Security Incident Response Team:
Based on two of the definitions given above, a CSIRT is a team that coordinates and supports the response to security incidents that involve sites within a defined constituency.

In order to be considered a CSIRT, a team must:

- Provide a (secure) channel for receiving reports about suspected incidents.

- Provide assistance to members of its constituency in handling these incidents.
- Disseminate incident-related information to its constituency and to other involved parties.

Note that we are not referring here to police or other law enforcement bodies which may investigate computer-related crime. CSIRT members, indeed, need not have any powers beyond those of ordinary citizens.

Vendor:

A 'vendor' is any entity that produces networking or computing technology, and is responsible for the technical content of that technology. Examples of 'technology' include hardware (desktop computers, routers, switches, etc.), and software (operating systems, mail forwarding systems, etc.).

Note that the supplier of a technology is not necessarily the 'vendor' of that technology. As an example, an Internet Service Provider (ISP) might supply routers to each of its customers, but the 'vendor' is the manufacturer, since the manufacturer, rather than the ISP, is the entity responsible for the technical content of the router.

Vulnerability:

A 'vulnerability' is a characteristic of a piece of technology which can be exploited to perpetrate a security incident. For example, if a program unintentionally allowed ordinary users to execute arbitrary operating system commands in privileged mode, this "feature" would be a vulnerability.

Appendix B: Related Material

Important issues in responding to security incidents on a site level are contained in [RFC 2196], the Site Security Handbook, produced by the Site Security Handbook Working Group (SSH). This document will be updated by the SSH working group and will give recommendations for local policies and procedures, mainly related to the avoidance of security incidents.

Other documents of interest for the discussion of CSIRTs and their tasks are available by anonymous FTP. A collection can be found on:

- ftp://ftp.cert.dfn.de/pub/docs/csir/
  Please refer to file 01-README for further information about the content of this directory.

Some especially interesting documents in relation to this document are as follows:

- ftp://ftp.nic.surfnet.nl/surfnet/net-security/cert-nl/docs/reports/R-92-01
  This report contains the Operational Framework of CERT-NL, the CSIRT of SURFnet (network provider in the Netherlands).

- For readers interested in the operation of FIRST (Forum of Incident Response and Security Teams) more information is collected in Appendix C.

- http://hightop.nrl.navy.mil/news/incident.html
  This document leads to the NRL Incident Response Manual.

- http://www.cert.dfn.de/eng/team/kpk/certbib.html
  This document contains an annotated bibliography of available material, documents and files about the operation of CSIRTs with links to many of the referenced items.

- ftp://info.cert.org/incident_reporting_form
  This Incident Reporting Form is provided by the CERT Coordination Center to gather incident information and to avoid additional delays caused by the need to request more detailed information from the reporting site.

- http://www.cert.org/cert.faqintro.html
  A collection of frequently asked questions from the CERT Coordination Center.

Appendix C: Known Computer Security Incident Response Teams

Today, there are many different CSIRTs but no single source lists every team. Most of the major and long established teams (the first CSIRT was founded in 1988) are nowadays members of FIRST, the worldwide Forum of Incident Response and Security Teams. At the time of writing, more than 55 teams are members (1 in Australia, 13 in Europe, all others in North America). Information about FIRST can be found:

- http://www.first.org/

The current list of members is available also, with the relevant contact information and some additional information provided by the particular teams:

- http://www.first.org/team-info/

For CSIRTs which want to become members of this forum (please note that a team needs a sponsor - a team which is already a full member of FIRST - to be introduced), the following files contain more information:

- http://www.first.org/about/op_frame.html
  The Operational Framework of FIRST.

- http://www.first.org/docs/newmem.html
  Guidelines for teams which want to become members of FIRST.

Many of the European teams, regardless of whether they are members of FIRST or not, are listed by countries on a page maintained by the German CSIRT:

- http://www.cert.dfn.de/eng/csir/europe/certs.html

To learn about existing teams suitable to one’s needs it is often helpful to ask either known teams or an Internet Service Provider for the "right" contact.

Appendix D: Outline for CSIRT Template

This outline summarizes in point form the issues addressed in this document, and is the recommended template for a CSIRT description document. Its structure is designed to facilitate the communication of a CSIRT's policies, procedures, and other relevant information to its constituency and to outside organizations such as other CSIRTs. A 'filled-in' example of this template is given as Appendix E.

1. Document Information
1.1 Date of Last Update
1.2 Distribution List for Notifications
1.3 Locations where this Document May Be Found

2. Contact Information
2.1 Name of the Team
2.2 Address
2.3 Time Zone
2.4 Telephone Number
2.5 Facsimile Number
2.6 Other Telecommunication
2.7 Electronic Mail Address
2.8 Public Keys and Encryption Information
2.9 Team Members
2.10 Other Information
2.11 Points of Customer Contact

3. Charter
3.1 Mission Statement
3.2 Constituency
3.3 Sponsorship and/or Affiliation
3.4 Authority

4. Policies
4.1 Types of Incidents and Level of Support
4.2 Co-operation, Interaction and Disclosure of Information
4.3 Communication and Authentication

5. Services
5.1 Incident Response
    5.1.1. Incident Triage
    5.1.2. Incident Coordination
    5.1.3. Incident Resolution
5.2 Proactive Activities

6. Incident Reporting Forms

7. Disclaimers

Appendix E: Example - 'filled-in' Template for a CSIRT

Below is an example of a filled-in template for a fictitious CSIRT called XYZ-CSIRT. This text is for example purposes only, and does not constitute endorsement by the working group or the IETF of any particular set of procedures or policies. While CSIRTs are welcome to use any or all of this text if they wish, such use is of course not mandatory, or even appropriate in most cases.

CSIRT Description for XYZ-CERT

1. About this document

1.1 Date of Last Update

This is version 1.01, published 1997/03/31.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list <xyz-cert-info@xyz-univ.ca>. Subscription requests for this list should be sent to the Majordomo at <xyz-cert-info-request@xyz-univ.ca>; the body of the message should consist of the word "subscribe". Send the word "help" instead if you don't know how to use a Majordomo list manager. This mailing list is moderated.

1.3 Locations where this Document May Be Found

The current version of this CSIRT description document is available from the XYZ-CERT WWW site; its URL is
http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.txt
Une version francaise de ce document est igalement disponible:
http://www.xyz-univ.ca/xyz-cert/francais/CSIRT-descr.txt
Please make sure you are using the latest version.

1.4 Authenticating this Document

Both the English and French versions of this document have been signed with the XYZ-CERT's PGP key. The signatures are also on our Web site, under:
http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.asc
http://www.xyz-univ.ca/xyz-cert/francais/CSIRT-descr.asc

2. Contact Information

2.1 Name of the Team

"XYZ-CERT": the XYZ University Computer Emergency Response Team.

2.2 Address

XYZ-CERT
XYZ University, Computing Services Department
12345 Rue Principale
UniversityTown, Quebec
Canada H0H 0H0

2.3 Time Zone

Canada/Eastern (GMT-0500, and GMT-0400 from April to October)

2.4 Telephone Number

+1 234 567 7890 (ask for the XYZ-CERT)

2.5 Facsimile Number

+1 234 567 7899 (this is *not* a secure fax)

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

<xyz-cert@xyz-univ.ca> This is a mail alias that relays mail to the human(s) on duty for the XYZ-CERT.

2.8 Public Keys and Other Encryption Information

The XYZ-CERT has a PGP key, whose KeyID is 12345678 and whose fingerprint is
  11 22 33 44 55 66 77 88 88 77 66 55 44 33 22 11.
The key and its signatures can be found at the usual large public keyservers.

Because PGP is still a relatively new technology at XYZ University, this key still has relatively few signatures; efforts are underway to increase the number of links to this key in the PGP "web of trust". In the meantime, since most

fellow universities in Quebec have at least one staff member who knows the XYZ-CERT coordinator Zoe Doe, Zoe Doe has signed the XYZ-CERT key, and will be happy to confirm its fingerprint and that of her own key to those people who know her, by telephone or in person.

2.9 Team Members

Zoe Doe of Computing Services is the XYZ-CERT coordinator. Backup coordinators and other team members, along with their areas of expertise and contact information, are listed in the XYZ-CERT web pages, at
http://www.xyz-univ.ca/xyz-cert/teamlist.html

Management, liaison and supervision are provided by Steve Tree, Assistant Director (Technical Services), Computing Services.

2.10 Other Information

General information about the XYZ-CERT, as well as links to various recommended security resources, can be found at
http://www.xyz-univ.ca/xyz-cert/index.html

2.11 Points of Customer Contact

The preferred method for contacting the XYZ-CERT is via e-mail at <xyz-cert@xyz-univ.ca>; e-mail sent to this address will "biff" the responsible human, or be automatically forwarded to the appropriate backup person, immediately. If you require urgent assistance, put "urgent" in your subject line.

If it is not possible (or not advisable for security reasons) to use e-mail, the XYZ-CERT can be reached by telephone during regular office hours. Telephone messages are checked less often than e-mail.

The XYZ-CERT’s hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday except holidays).

If possible, when submitting your report, use the form mentioned in section 6.

3. Charter

3.1 Mission Statement

The purpose of the XYZ-CERT is, first, to assist members of XYZ University community in implementing proactive measures to reduce the risks of computer security incidents, and second, to assist XYZ community in responding to such incidents when they occur.

3.2 Constituency

The XYZ-CERT's constituency is the XYZ University community, as defined in the context of the "XYZ University Policy on Computing Facilities". This policy is available at
http://www-compserv.xyz-univ.ca/policies/pcf.html

However, please note that, notwithtanding the above, XYZ-CERT services will be provided for on-site systems only.

3.3 Sponsorship and/or Affiliation

The XYZ-CERT is sponsored by the ACME Canadian Research Network. It maintains affiliations with various University CSIRTs throughout Canada and the USA on an as needed basis.

3.4 Authority

The XYZ-CERT operates under the auspices of, and with authority delegated by, the Department of Computing Services of XYZ University. For further information on the mandate and authority of the Department of Computing Services, please refer to the XYZ University "Policy on Computing Facilities", available at
http://www-compserv.xyz-univ.ca/policies/pcf.html

The XYZ-CERT expects to work cooperatively with system administrators and users at XYZ University, and, insofar as possible, to avoid authoritarian relationships. However, should circumstances warrant it, the XYZ-CERT will appeal to Computing Services to exert its authority, direct or indirect, as necessary. All members of the XYZ-CERT are members of the CCSA (Committee of Computer Systems Administrators), and have all of the powers and responsibilities assigned to Systems Administrators by the Policy on Computing Facilities, or are members of University management.

Members of the XYZ University community who wish to appeal the actions of the XYZ-CERT should contact the Assistant Director (Technical Services), Computing Services. If this recourse is not satisfactory, the matter may be referred to the Director of Computing Services (in the case of perceived problems with existing policy), or to the XYZ University Office of Rights and Responsibilities (in the case of perceived errors in the application of existing policy).

4. Policies

4.1 Types of Incidents and Level of Support

The XYZ-CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, at XYZ University.

The level of support given by XYZ-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the XYZ-CERT's resources at the time, though in all cases some response will be made within one working day. Resources will be assigned according to the following priorities, listed in decreasing order:

- Threats to the physical safety of human beings.
- Root or system-level attacks on any Management Information System, or any part of the backbone network infrastructure.
- Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.
- Compromise of restricted confidential service accounts or software installations, in particular those used for MIS applications containing confidential data, or those used for system administration.
- Denial of service attacks on any of the above three items.
- Any of the above at other sites, originating from XYZ University.
- Large-scale attacks of any kind, e.g. sniffing attacks, IRC "social engineering" attacks, password cracking attacks.
- Threats, harassment, and other criminal offenses involving individual user accounts.
- Compromise of individual user accounts on multi-user systems.
- Compromise of desktop systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. netnews and e-mail forgery, unauthorized use of IRC bots.

- Denial of service on individual user accounts, e.g. mailbombing.

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. The XYZ-CERT will support the latter people.

While the XYZ-CERT understands that there exists great variation in the level of system administrator expertise at XYZ University, and while the XYZ-CERT will endeavor to present information and assistance at a level appropriate to each person, the XYZ-CERT cannot train system administrators on the fly, and it cannot perform system maintenance on their behalf. In most cases, the XYZ-CERT will provide pointers to the information needed to implement appropriate measures.

The XYZ-CERT is committed to keeping the XYZ University system administration community informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

While there are legal and ethical restrictions on the flow of information from XYZ-CERT, many of which are also outlined in the XYZ University Policy on Computing Facilities, and all of which will be respected, the XYZ-CERT acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, the XYZ-CERT will otherwise share information freely when this will assist others in resolving or preventing security incidents.

In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no expectation of confidentiality from the XYZ-CERT. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist.

Information being considered for release will be classified as follows:

- Private user information is information about particular users, or in some cases, particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons.

  Private user information will be not be released in identifiable form outside the XYZ-CERT, except as provided for below. If the identity of the user is disguised, then the information can be released freely (for example to show a sample .cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).

- Intruder information is similar to private user information, but concerns intruders.

  While intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CSIRTs tracking an incident.

- Private site information is technical information about particular systems or sites.

  It will not be released without the permission of the site in question, except as provided for below.

- Vulnerability information is technical information about vulnerabilities or attacks, including fixes and workarounds.

  Vulnerability information will be released freely, though every effort will be made to inform the relevant vendor before the general public is informed.

- Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity. Embarrassing information may concern a site or a particular user or group of users.

  Embarrassing information will not be released without the permission of the site or users in question, except as provided for below.

- Statistical information is embarrassing information with the identifying information stripped off.

  Statistical information will be released at the discretion of the Computing Services Department.

- Contact information explains how to reach system administrators and CSIRTs.

  Contact information will be released freely, except where the contact person or entity has requested that this not be the case, or where XYZ-CERT has reason to believe that the dissemination of this information would not be appreciated.

Potential recipients of information from the XYZ-CERT will be classified as follows:

- Because of the nature of their responsibilities and consequent expectations of confidentiality, members of XYZ University management are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.

- Members of the Office of Rights and Responsibilities are entitled to receive whatever information they request concerning a computer security incident or related matter which has been referred to them for resolution. The same is true for the XYZ Security Department, when its assistance in an investigation has been enlisted, or when the investigation has been instigated at its request.

- System administrators at XYZ University who are members of the CCSA are also, by virtue of their responsibilities, trusted with confidential information. However, unless such people are also members of XYZ-CERT, they will be given only that confidential information which they must have in order to assist with an investigation, or in order to secure their own systems.

- Users at XYZ University are entitled to information which pertains to the security of their own computer accounts, even if this means revealing "intruder information", or "embarrassing information" about another user. For example, if account aaaa is cracked and the intruder attacks account bbbb, user bbbb is entitled to know that aaaa was cracked, and how the attack on the bbbb account was

executed. User bbbb is also entitled, if she or he requests it, to information about account aaaa which might enable bbbb to investigate the attack. For example, if bbbb was attacked by someone remotely connected to aaaa, bbbb should be told the provenance of the connections to aaaa, even though this information would ordinarily be considered private to aaaa. Users at XYZ University are entitled to be notified if their account is believed to have been compromised.

- The XYZ University community will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general XYZ community. There is no obligation on the part of the XYZ-CERT to report incidents to the community, though it may choose to do so; in particular, it is likely that the XYZ-CERT will inform all affected parties of the ways in which they were affected, or will encourage the affected site to do so.

- The public at large will receive no restricted information. In fact, no particular effort will be made to communicate with the public at large, though the XYZ-CERT recognizes that, for all intents and purposes, information made available to the XYZ University community is in effect made available to the community at large, and will tailor the information in consequence.

- The computer security community will be treated the same way the general public is treated. While members of XYZ-CERT may participate in discussions within the computer security community, such as newsgroups, mailing lists (including the full-disclosure list "bugtraq"), and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from XYZ-CERT experience will be disguised to avoid identifying the affected parties.

- The press will also be considered as part of the general public. The XYZ-CERT will not interact directly with the Press concerning computer security incidents, except to point them toward information already released to the general public. If necessary, information will be provided to the XYZ University Public Relations Department, and to the Customer Relations group of the Computing Services Department. All incident-related queries will be referred to

these two bodies. The above does not affect the ability of members of XYZ-CERT to grant interviews on general computer security topics; in fact, they are encouraged to do to, as a public service to the community.

- Other sites and CSIRTs, when they are partners in the investigation of a computer security incident, will in some cases be trusted with confidential information. This will happen only if the foreign site's bona fide can be verified, and the information transmitted will be limited to that which is likely to be helpful in resolving the incident. Such information sharing is most likely to happen in the case of sites well known to XYZ-CERT (for example, several other Quebec universities have informal but well-established working relationships with XYZ University in such matters).

  For the purposes of resolving a security incident, otherwise semi-private but relatively harmless user information such as the provenance of connections to user accounts will not be considered highly sensitive, and can be transmitted to a foreign site without excessive precautions. "Intruder information" will be transmitted freely to other system administrators and CSIRTs. "Embarrassing information" can be transmitted when there is reasonable assurance that it will remain confidential, and when it is necessary to resolve an incident.

- Vendors will be considered as foreign CSIRTs for most intents and purposes. The XYZ-CERT wishes to encourage vendors of all kinds of networking and computer equipment, software, and services to improve the security of their products. In aid of this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to identify and fix the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

- Law enforcement officers will receive full cooperation from the XYZ-CERT, including any information they require to pursue an investigation, in accordance with the Policy on Computing Facilities.

4.3 Communication and Authentication

In view of the types of information that the XYZ-CERT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be

sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the XYZ-CERT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within XYZ University, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (PGP in particular is supported).

5. Services

5.1 Incident Response

XYZ-CERT will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- Investigating whether indeed an incident occured.
- Determining the extent of the incident.

5.1.2 Incident Coordination

- Determining the initial cause of the incident (vulnerability exploited).
- Facilitating contact with other sites which may be involved.
- Facilitating contact with XYZ University Security and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

5.1.3 Incident Resolution

- Removing the vulnerability.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, etc.
- Collecting evidence where criminal prosecution, or University disciplinary action, is contemplated.

In addition, XYZ-CERT will collect statistics concerning incidents which occur within or involve the XYZ University community, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of XYZ-CERT's incident response services, please send e-mail as per section 2.11 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.2 Proactive Activities

The XYZ-CERT coordinates and maintains the following services to the extent possible depending on its resources:

- Information services
  - List of departmental security contacts, administrative and technical. These lists will be available to the general public, via commonly-available channels such as the World Wide Web and/or the Domain Name Service.
  - Mailing lists to inform security contacts of new information relevant to their computing environments. These lists will be available only to XYZ University system administrators.
  - Repository of vendor-provided and other security-related patches for various operating systems. This repository will be available to the general public wherever license restrictions allow it, and will be provided via commonly-available channels such as the World Wide Web and/or ftp.
  - Repository of security tools and documentation for use by sysadmins. Where possible, precompiled ready-to-install versions will be supplied. These will be supplied to the general public via www or ftp as above.

- "Clipping" service for various existing resources, such as major mailing lists and newsgroups. The resulting clippings will be made available either on the restricted mailing list or on the web site, depending on their sensitivity and urgency.
- Training services
  - Members of the XYZ-CERT will give periodic seminars on computer security related topics; these seminars will be open to XYZ University system administrators.
- Auditing services
  - Central file integrity checking service for Unix machines, and for any other platforms capable of running "tripwire".
  - Security level assignments; machines and subnetworks at XYZ University will be audited and assigned a security level. This security level information will be available to the XYZ University community, to facilitate the setting of appropriate access privileges. However, details of the security analyses will be confidential, and available only to the concerned parties.
- Archiving services
  - Central logging service for machines capable of Unix-style remote logging. Incoming log entries will be watched by an automated log analysis program, and events or trends indicative of a potential security problem will be reported to the affected system administrators.
  - Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports will be made available to the XYZ University community.

Detailed descriptions of the above services, along with instructions for joining mailing lists, downloading information, or participating in certain services such as the central logging and file integrity checking services, are available on the XYZ-CERT web site, as per section 2.10 above.

6. Incident Reporting Forms

There are no local forms developed yet for reporting incidents to XYZ-CERT. If possible, please make use of the Incident Reporting Form of the CERT Coordination Center (Pittsburgh, PA). The current version is available from:

ftp://info.cert.org/incident_reporting_form

7. Disclaimers

> While every precaution will be taken in the preparation of information, notifications and alerts, XYZ-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

4 Acknowlegdements

The editors gratefully acknowledge the contributed material and editorial scrutiny of Anne Bennett. Thanks also to Don Stikvoort for assistance reworking the description of Incident Response Team services.

5 References

[RFC 2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.

[RFC 1983] Malkin, G., "Internet Users' Glossary", FYI 18, RFC 1983, August 1996.

6 Security Considerations

This document discusses the operation of Computer Security Incident Response Teams, and the teams' interactions with their constituencies and with other organizations. It is, therefore, not directly concerned with the security of protocols, applications, or network systems themselves. It is not even concerned with particular responses and reactions to security incidents, but only with the appropriate description of the responses provided by CSIRTs.

Nonetheless, it is vital that the CSIRTs themselves operate securely, which means that they must establish secure communication channels with other teams, and with members of their constituency. They must also secure their own systems and infrastructure, to protect the interests of their constituency and to maintain the confidentiality of the identity of victims and reporters of security incidents.

7 Authors' Addresses

Nevil Brownlee
ITSS Technology Development
The University of Auckland

Phone: +64 9 373 7599 x8941
EMail: n.brownlee@auckland.ac.nz

Erik Guttman
Sun Microsystems, Inc.
Bahnstr. 2
74915 Waibstadt Germany

Phone: +49 7263 911484
EMail: Erik.Guttman@sun.com

8 Full Copyright Statement