Internet Engineering Task Force
INTERNET-DRAFT
Valid for six months

Nevil Brownlee
The University of Auckland
Erik Guttman
Sun Microsystems
March 1997

Expectations for Security Incident Response

<draft-ietf-grip-framework-irt-04.txt>

Status of this Memo

Abstract

The purpose of this document is to express the general Internet community's expectations of Security Incident Response Teams. 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.

SIRT constituents have a legitimate need and right to fully understand the policies and procedures of "their" 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 SIRT. An outline of such a template and a filled in example is provided.

Table of Contents

1 Introduction

The GRIP Working Group was formed to create a document that describes the community's expectations of security incident response teams (SIRTs). 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 SIRTs. 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 "Security Incident Response Team." For the purposes of this document, a SIRT 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 SIRT 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 SIRT should make it clear who belongs to their constituency and define the services the team offers to the community. Additionally, each SIRT 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 incidents should be reported.

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

It must be emphasised that without active participation from users, the effectiveness of the SIRT'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 where they should report them to.

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 the cooperation of multiple sites and potentially multiple SIRTs. The coordination of activities across communities and organization requires that the parties understand who they are dealing with, and what sort of policies they have in place.

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 SIRTs. Resolving these incidents will require cooperation between individual sites and SIRTs, and between SIRTs. Constituent communities need to know exactly how their SIRT will be working with other SIRTs and organizations outside their constituency, and what information will be shared.

The rest of this document describes the set of topics and issues that SIRTs 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 it terms of what that topic means. For example, five types of policy statements are listed (representing those policies of interest to the community), but the content of any one of them will necessarily be specific to a given team.

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. These topics are condensed into an outline template for ease of use by the community, and is found in Appendix D. This template can be used by constituents to elicit information from their SIRT, and it provides criteria with which to measure their team's performance.

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

2 Scope

The interactions between a constituent community and an incident response team require first that the community understands 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 and the community needs to know how those communications are going to be protected. Each of these subjects will be described in more detail in the following three sections.

2.1 Publishing a SIRT Policies and Procedures

Each user who has access to a Security Incident Response Team should know as much as possible about 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 SIRT helps the constituent understand how best to report incidents and what support to expect afterwards. Will the SIRT 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 SIRT, will make interaction with it more efficient and effective.

There are different kinds of response teams. Some that have very broad constituencies (e.g., CERT Coordination Center and the Internet), others that have more bounded constituencies (e.g., DFN-CERT, CIAC), and still others that 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.

As a SIRT provides a service to a this clearly defined constituency, it should communicate all necessary information about its policies and services in a suitable form. It is important to understand that not all policies and procedures must 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 Frequently Asked Questions (FAQ), while still others wrote papers for distribution at user conferences or sent newsletters.

Another efficient way to communicate the relevant information to all concerned, not only constituents but also other teams or organizations, would be for each SIRT to publish its guidelines and procedures on its own information server. This would allow constituents to easily access it, although this does not address the problem of how a constituent or will find "his" or "her" team. People within the constituency have to discover that there is a SIRT "at their disposal." It is foreseen that completed SIRT templates will soon become searchable by modern search engines. This will aid in distributing information about the existence of SIRTs and basic information required to approach them.

It would be very useful to have a central repository containing all the completed SIRT templates. No such repository presently exists. 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 user can verify that the template was indeed published by the SIRT and that it has not been modified thereafter. This document assumes the reader has familiarity with the proper use of digital signatures to determine whether a document is authentic.

2.2 Relationships between different SIRTs

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

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

Such interactions could include asking other teams for advice, disseminating knowledge of problems and working cooperatively to resolve a security incident effecting one or more of the SIRTs' constituencies.

In establishing relationships to support such interactions, SIRTs will need to 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 SIRTs involved agree to work together and share information, and simple co-operation, where a SIRT (or any other organization) simply contacts another SIRT and asks for help or advice.

Although the establishing of such relationships is very important and affect the ability of a SIRT 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. But 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 SIRT, 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 Security Incident Response - all parties involved need secure communications channels. ("Secure" hereby relates to the protected transmission of information shared between different parties and not 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, they must be authenticated before usage. While PGP relies on a "Web of Trust" - users sign the keys of other users - PEM relies on a hierarchy - certification authorities sign the keys of users.

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

Communication is critical for 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 (like calling a specific number for checking the authenticity of keys) should be explained right away. SIRT templates provide a standardized vehicle for delivering this information.

It is beyond the scope of this document to address all 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 all issues and topics relevant to the interaction of constituents with "their" SIRT, we suggest that a SIRT publish all information, policies and procedures addressing their constituency as a document, following template given in Appendix D. The template structure arranges items, making it easy to supply specific information, was done for the example in Appendix E. While no recommendations are made as to what a SIRT should adopt for their policy or procedures, different possibilities are outlined to give some examples. The most important thing is that a SIRT has a policy and that

that those who interact with the SIRT can 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 for supporting their constituency.

3.1 Contact Information

Full details of how to contact the SIRT should be listed here, although this might be very different for different teams. Some might choose to restrict the availability of names of all team members. No further clarification is given when the meaning of the item can be assumed.

- Name of the SIRT

- 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 outlined so users can determine if and how they can make use of secure communication while interacting with the SIRT.

- Team members

- Other information — The operating hours and holiday schedule should be provided here. Is there a 24 hour hotline? Is there any specific customer contact info? (See also section 3.4.5).

3.2 Document Updates

Details of a SIRT change with time, so the completed template must indicate when it was last changed. Additionally, information should be provided to learn about how to find out about future updates. Without this, it is inevitable that misunderstandings and misconceptions will arise over time; an outdated document will 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 cover the constituency and any other groups the SIRT has frequent interactions with.

  Digital signatures should be used for update messages sent by a SIRT.

- Location of the document

  The location where a current version of the document should be 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,

3.3 Charter

Every SIRT 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 statements:

- Mission statement
- Constituency
- Sponsor / 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 SIRT. In order to be considered a 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 definitions.

3.3.2 Constituency

A SIRT's constituency can be determined in many 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 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 the perimeter will be handled.

If a SIRT decide, not to disclosure their constituency, they should explain the reasoning behind this decision. For example for-fee SIRTs will not list their clients but declare that they provide a service to a large group of customers that are kept confidential because of the clients' contract.

Constituencies might overlap, as when an ISP provides a SIRT, but delivers services to customer sites which also have SIRTs. The Authority section of the document (see below) should make such relationships clear.

3.3.3 Sponsoring Organization / Affiliation

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

3.3.4 Authority

Based on the relationship between team and constituency this section will be very different from one team to another. While an organizational SIRT will be given its authority by the management, a community SIRT will be supported and chosen by the community, usually in a advisory role.

SIRTs may not have authority to intervene in the operation of all the systems within their perimeter. They should identify the scope of their control as distinct from the perimeter of their constituency; if other SIRTs operate hierarchically within their perimeter, these should be identified and addressed here.

A 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

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 opportunity for more detailed definition and to address non-incident related topics.

The level of support might change, depending on factors like workload or completeness of 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 SIRT should also give some background on the "default" support for each reported incident.

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 pro-active service policy rather than a core service requirement for a SIRT.

3.4.2 Co-operation and Interaction with other Organizations

This section should make explicit which related groups with which the SIRT routinely interacts with. Such interactions are not related to the Security Incident Response provided, but are used to facilitate better cooperation on technical topics or services. By no means should details about cooperation agreements be given out, the main objective of this section is to give the constituency a basic understanding what kind of interactions are established and what their purpose is. Examples of these are listed below.

Incident Response Teams:
A SIRT will often need to interact with other SIRTs. For example a SIRT within a large company may need to report incidents to a national SIRT, and a national SIRT may need to report incidents to national SIRTs in other countries to deal with all sites involved in a large-scale attack.

Vendors:
Larger vendors have their own SIRTs, but smaller vendors may not. In such cases a SIRT will need to work directly with a vendor to suggest improvements or modifications, to analyse the technical problem or to test provided solutions.

Law-enforcement agencies:
These include the police and other investigative agencies. SIRTs and users of the template should be sensitive to local laws and regulations, which may vary considerably in different countries. A SIRT 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 SIRT may be approached by the Press for information and comment from time to time. This is discussed in more detail immediately below.

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

3.4.3 Reporting and Disclosure

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 as a 'black hole.' Its 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 restraints, 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.

'Disclosure' includes (but is maybe not limited to):

- Reporting incidents within the constituency to other teams. By this, site related information might become public knowledge, accessible for everybody, especially the press.

- Handling incidents occurring within the constituency, but reported from outside it.

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

- Acting on reports of incidents occurring outside the constituency.

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

- Feed-back to parties reporting incidents or vulnerabilities.

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

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

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

A team will normally collect statistics. If such information are distributed, the template's reporting and disclosure policy should say so, and should list methods to obtain such statistics.

3.4.4 Communication and Authentication

Methods of secure and verifiable communication should be established. This is necessary for communication between SIRTs and between a SIRT 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 to).

At the moment it is recommended that every SIRT has - if possible - as a minimum, a PGP key available. Teams 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 SIRTs 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 digitally 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 SIRT may keep secret authentication data for parties with whom they may deal, such as an agreed password or phrase.

3.4.5 Point of Customer Contacts

More detailed contact information might 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 (like addresses for mailing list requests) these should be explained here.

3.5 Services

Services provided by each SIRT can be differentiated by whether they relate to the main task, which is incident response, or are provided in addition (optional in regard to the definition of a SIRT).

Incident response, which usually includes:

- Verification — Help with the verification of incidents, as well as their scope.

- Technical Assistance — This may include analysis of compromised systems.

- Eradication — Elimination of the effects of a security incident.

- Recovery — Aid in restoring affected systems and services to their status before the security incident.

- Notification of other involved parties

Additional or optional services, which might include:

- Information provision — This might include an archive of known vulnerabilities, patches or resolutions of past problems.
- Security Tools

- Education and training

- Product evaluation

- Site security auditing and consulting

3.6 Incident Reporting Forms

The use of reporting forms makes it simplier for both sides, users and teams, to deal with incidents. The constituent may prepare answers to various important questions before he or she actually contacts the team and 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 single SIRT, multiple forms may be used, for example a reporting form for a new vulnerability will be very different for 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 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 for such form is the Incident Reporting Form provided by the CERT Coordination Center:

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

3.7 Disclaimers

Although the document does not constitute a contract, liability might 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.

It should be noted that some forms of reporting or disclosure relating to specific incidents or vulnerabilities can also imply liability, and SIRTs should consider the inclusion of disclaimers in such material.

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 is the binding version.

The use of and protection by disclaimers is effected by local laws and regulations. Therefore each SIRT should be sensitive and if in doubt should check the disclaimer with a lawyer.

4 Appendix A: Glossary of Terms

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

Constituency:

Implicit in the purpose of a 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 to be effective.

Security Incident:

For the purpose of this document this term is synonym to 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 of 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, might be regarded as an Incident.

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 really occurred.

Security Incident Response Team:

Based on two of the definitions given above, a SIRT 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 SIRT, 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. SIRT members, indeed, should not need to 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 Services Provider (ISP) might supply routers to each of its customers, but the 'vendor' is the manufacturer, being the entity responsible for the technical content of the router, rather than the ISP.

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.

5 Appendix B: Related Material

Important issues in responding to security incidents on a site level are contained in [RFC 1244], 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 SIRTs 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 SIRT 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 SIRTs with links to many of the referenced.

- 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 by requesting the sites for more detailed information.

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

6 Appendix C: Known Security Incident Response Teams

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

- http://www.first.org/

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

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

For SIRTs which want to become members of this forum (please note, that a team needs a sponsor - a team already 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 member of FIRST.

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

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

To learn about existing teams and maybe more suitable teams for one's need it is always a good approach, to ask either existing teams or an Internet Service Provider for the "right" contact.

7 Appendix D: Outline for SIRT Template

This outline summarizes the issues addressed in this document in a logical structure suitable to communicate the policies and procedures for the interaction with SIRTs easily to the team's constituency. A 'filled-in' example of this template is given as Appendix E.

1. Contact Information
1.1 Name of the Team
1.2 Address
1.3 Time Zone
1.4 Telephone Number
1.5 Facsimile Number
1.6 Other Telecommunication
1.7 Electronic Mail Address
1.8 Public Keys and Encryption Information
1.9 Team Members
1.10 Other Information

2. Document Updates
2.1 Date of Last Update
2.2 Distribution List for Notifications
2.3 Locations where this Document May Be Found

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

4. Policies
4.1 Types of Incidents and Level of Support
4.2 Cooperation and Interaction with Other Entities
4.3 Disclosure of Information
4.4 Communication and Authentication
4.5 Points of Customer Contacts

5. Services
5.1 Incident Response
5.2 Proactive Activities

6. Incident Reporting Forms

7. Disclaimers

8 Appendix E: Example - 'filled-in' Template for a SIRT

Below is an example, a filled-in template for a SIRT called XYZ to avoid any confusion with existing teams. By no means does this example imply, that a new founded SIRT should reuse this text. It is for example purposes only.

SIRT Template for XYZ-SIRT

Note: no digital signature is currently available for this SIRT Template. We'll put one up as soon as the technology is adopted by XYZ Enterprises.

1. Contact Information

1.1 Name of the Team

"XYZ-SIRT": the XYZ Computer Emergency Response Team.

1.2 Address

XYZ SIRT
XYZ Enterprises
Private Bag 12-345
MyTown
MyCountry

1.3 Time Zone

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

1.4 Telephone Number

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

1.5 Facsimile Number

+1 234 567 7654 (this is *not* a secure fax)

1.6 Other Telecommunication

None available.

1.7 Electronic Mail Address

<xyz-sirt@sirt.xyz.org>

1.8 Public Keys and Other Encryption Information

Encryption is not currently available, but we plan to install PGP as soon as possible. Our PGP public key will appear here as soon as it is available.

1.9 Team Members

Jane Doe of Computing Services is the XYZ-SIRT coordinator. Other team members will be listed here once their participation is confirmed.

2. Document Updates

2.1 Date of Last Update

Please see the bottom of this Web page for this information.

2.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list <xyz-sirt-info@sirt.xyz.org>. (Subscription request should go to <xyz-sirt-info-request@sirt.xyz.org>.)

2.3 Locations where this Document May Be Found

This template is available from the XYZ SIRT WWW site; its URL is

http://www.sirt.xyz.org/op_frame.html

The template will be signed with the XYZ-SIRT's PGP key.

3. Charter

3.1 Mission Statement

The purpose of the XYZ-SIRT is, first, to assist members of XYZ 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-SIRT's constituency is the XYZ SIRT community, as defined in the context of the "XYZ Policy on Computing Facilities".

3.3 Sponsors and/or Affiliation

None.

3.4 Authority

The XYZ-SIRT operates under the auspices of, and with authority delegated by, the Department of Computing Services of XYZ Enterprises. The Department in turn receives its authority from the formal ruling bodies of XYZ, as set out in the "Policy on Computing Facilities". The XYZ-SIRT has no direct authority over systems at XYZ Enterprises at large. However, it benefits from the direct authority of Computing Services with respect to systems managed by this Department. Also, because Computing Services manages the XYZ Enterprises Network, and is responsible for connectivity to it, the Department has indirect authority over systems in other departments, inasmuch as the Department can order such systems to be disconnected from the network should circumstances warrant it.

The XYZ-SIRT expects to work cooperatively with system administrators and users at XYZ, and, insofar as possible, to avoid authoritarian relationships. However, should circumstances warrant it, the XYZ-SIRT will appeal to Computing Services to exert its authority, direct or indirect, as necessary.

4. Policies

4.1 Types of Incidents and Level of Support

The XYZ-SIRT is authorized to address all types of computer security incidents which occur, or risk occurring, at XYZ Enterprises.

The level of support given by XYZ-SIRT will vary depending on the type and severity of the incident or issue, the type of consituent, the size of the user community affected, and the XYZ-SIRT's resources at the time.

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-SIRT will support the latter people.

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

4.2 Cooperation and Interaction with Other Entities

- Other sites:

  The XYZ-SIRT will cooperate with other SIRTs (security incident response teams) and with system administrators at other sites, to the extent that their bona fide can be verified. Should provincial or national SIRTs be constituted, XYZ-SIRT will explore the possibility of peer relationships with them. The possibility of peer relationships with close neighbors will also be explored; unofficial cooperative climates already exist between XYZ and several nearby universities and large corporations. While there are no legal requirements that XYZ-SIRT provide any information to any body outside XYZ (aside from law enforcement agencies), XYZ-SIRT will provide such information when the good of the community justifies it. However, unless identifying information is needed to track an incident in progress, such information will be stripped from the report (unless the affected department gives its permission that the real information be used).
- Vendors:

  The XYZ-SIRT 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:

  XYZ has its own Security Department. (I NEED TO LOOK UP THE RELATIONSHIP BETWEEN COMPUTING SERVICES, XYZ SECURITY, AND OUTSIDE POLICE FORCES.) Informal working relationships already exist between some system administrators at XYZ and the local police; interest has been expressed by all parties in formalizing these relationships. Any progress made in that area will be reflected in this section. In the meantime, authorized and unauthorized users of the XYZ Computing Facilities should be aware that the XYZ-SIRT will cooperate fully with law enforcement agencies in detecting, reporting, documenting, and prosecuting violations of the law; users concerned about confidentiality are referred to the XYZ "Policy on Computing Facilities".

- The Press:

  The XYZ-SIRT will not interact directly with the Press. If necessary, information will be provided to the XYZ Public Relations Department, and to the Customer Relations group of the Computing Services Department. All queries will be referred to these two bodies.
- The XYZ SIRT community:

  Details of incidents may be released to Computing Services management, XYZ management, or the Computer Resources Committee; these bodies will be charged with maintaining the confidentiality of the information. General report of incidents, summaries of multiple incidents, and statistics may be made available to the general XYZ community, with identifying information stripped (except where permission has been obtained from the affected parties). There is no obligation on the part of the XYZ-SIRT to report incidents to the community, though it may choose to do so; in particular, it is likely that the XYZ-SIRT will inform all affected parties of the ways in which they were affected.
- The public at large:

  In general, no particular efforts will be made to communicate with the public at large, though the XYZ-SIRT recognizes that, for all intents and purposes, information made available to the XYZ community is in effect made available to the community at large, and will tailor the information in consequence.
- The computer security community:

  While members of XYZ-SIRT 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-SIRT experience will be disguised to avoid identifying the affected parties.

In the paragraphs above, the "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 usage of a facility; such intruders may have no expectation of confidentiality from the XYZ-SIRT. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist.

4.3 Disclosure of Information

The following types of information will be stored and handled by XYZ-SIRT:

- Contact info for constituents.
- Technical info about a vulnerability.
- Technical info about XYZ facilities.
- Information about incidents:
    - Statistical summaries
    - Admission of incident of certain type
    - Admission of root compromise
    - Admission of packet sniffing attack
    - Admission that user accounts were compromised
    - Description of incident
        - Identity of affected systems
        - Identity of affected people
        - Identity of perpetrator

Recipients of information are - depending on the need to know - are as follows:

- XYZ management
- Computing Services management
- Affected sysadmin at XYZ
- Affected sysadmin (or SIRT) at another site

- Affected user(s) at XYZ
- All sysadmins potentially concerned (potentially vulnerable) at XYZ
- All sysadmins at XYZ
- All users potentially concerned at XYZ (information will leak to general public)
- All users at XYZ (ditto)
- Computer security community
- Peer sysadmins and SIRTs
- Vendors
- Law enforcement

4.4 Communication and Authentication

In view of the types of information that the XYZ-SIRT 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.

Where it is necessary to establish trust, for example before relying on information given to the XYZ-SIRT, 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, 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.

4.5 Points of Customer Contact

The preferred method for contacting the XYZ-SIRT will be e-mail. If this is not possible, or not advisable for security reasons, the XYZ-SIRT can be reached by telephone during regular office hours.

5. Services

5.1 Incident Response

XYZ-SIRT will help users and administrators to handle the technical and organizational aspects of incidents. By that, it will provide and facilitate:

- to understand the extend of the incident
- ...

5.2 Proactive Activities

The XYZ-SIRT will coordinate and maintain the following services to the extent possible depending on its resources:

- Information services
  - List of departmental security contacts, administrative and technical.
  - Mailing lists to inform security contacts of new information relevant to their computing environments.
  - Repository of vendor-provided and other security-related patches for various operating systems.
  - Repository of security tools for use by sysadmins.
  - "Clipping" service for various existing resources, such as major mailing lists and newsgroups.
- Auditing services
  - Central file integrity checking service for Unix machines.
  - Security level assignments; machines at XYZ will be audited and assigned a security level.
- Archiving services
  - Records of security incidents handled.

6. Incident Reporting Forms

There are no own forms developed yet for reporting incidents to XYZ-SIRT. If possible, please make us of the Incident Reporting Form of the CERT Coordination Center (Pittsburgh, PA). The actual 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-SIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

9 References

[RFC 1244] P. Holbrooks, J. Reynolds / Site Security Handbook. - July 23, 1991. - 101 pages. - FYI 8.

[RFC 1983] G. Malkin / Internet Users' Glossary. - August 16, 1996. - 62 pages. - FYI 18.

10 Security Considerations

This document discusses issues of the operation of Security Incident Response Teams, and the teams interactions with their constituency. It is therefore not directly concerned with the security of protocols, applications or network systems themselves. It is not even concerned about the response and reaction to security incidents.

Nonetheless, it is vital that SIRTs 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.

11 Authors' Addresses

Nevil Brownlee
ITSS Technology Development
The University of Auckland

Phone: +64 9 373 7599 x8941
E-mail: n.brownlee@auckland.ac.nz

Erik Guttman
Sun Microsystems, Inc.
Gaisbergstr. 6
69115 Heidelberg Germany

Phone: +49 6221 601649
E-Mail: eguttman@eng.sun.com

This document expires September 26, 1997.