Internet Engineering Task Force
INTERNET-DRAFT

Nevil Brownlee
The University of Auckland
November 1996

Expectations for Security Incident Response

<draft-ietf-grip-framework-irt-03.txt>

Status of this Memo

Abstract

This document is intended to facilitate the setting of expectations regarding the operation of Security Incicident Response Teams (SIRTs). It describes the various important topics in the form of a 'template,' through which every SIRT should describe itself and its functions.

SIRT clients have a legitimate need and right to fully understand the policies and procedures of their Security Incident Response Team. A SIRT's template supplies details for the various important topics which clients must consider when selecting a SIRT.

Contents

1 Introduction

The GRIP Working Group was formed to produce guidelines and recommendations to facilitate the consistent handling of security incidents in the Internet community. Although it is focused on the Internet, many of the concepts discussed will also be useful for other forms of local- and wide-area networks and internets.

Many computer security incidents orginate outside local community boundaries and affect other 'outside' sites, and others orignate outside the local community and affect hosts or users within it. Often, therefore, the handling of security incidents will involve multiple Security Incident Response Teams. Because of this characteristic it is important for every community to have a good security policy, and to have a Security Incident Response Team (SIRT) in place to manage communications across community boundaries in a consistent way.

In the past there have been misunderstandings regarding expectations of response teams. The goal of this document is to provide a framework in which to set expectations. By defining such a framework the community can express areas and topics that need to addressed by any SIRT.

'Consistent handling' implies that any group calling itself a SIRT must react to security incidents or to threats of them in ways which the Internet community agrees to be in its general interest. Every SIRT needs to define clearly the services they offer and the level at which they are offered to clients. Such definitions will be particularly important in contracts and/or agreements which SIRTs make with their clients.

The "Expectations for Security Incident Response" is seen as resting on the work of individual SIRTs and the cooperation between them. This document therefore recommends a 'template' through which every SIRT should describe itself and its functions. It further recommends that templates should be accessible among teams, to make possible a fully effective cooperative response framework for incidents or threats across the entire domain affected by them.

1.1 Definitions

This section defines terms used in describing security incidents and response teams. For the purpose of the GRIP documents only a limited list is really needed. This should help maintain focus on the purpose of the documents, and prevent a duplication of other definitions or - even worse - a proliferation of competing definitions.

Constituency

Implicit in the purpose of a Security Incident Response Team is the existence of a constituency. This is the group of clients, sites, networks or organizations served by the team.

Security Incident

For the purpose of this document:

> 'A computer security incident is any 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,
* compromise of integrity,
* denial of service,
* misuse,
* damage.

These are very general categories. For instance the replacement of a system utility program by a Trojan Horse is an example of 'loss of integrity,' and a successful password attack is an example of 'loss of confidentiality.'

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

Security Incident Response Team

Based on two of the definitions given above:

> 'A Security Incident Response Team is a group authorized to manage response to security incidents that involve sites within its defined constituency.'

In order to be considered a SIRT, a group must:

* provide a 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 related 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.

1.2 Publishing SIRT Templates

Every SIRT should publish information about its policies and services in the form of a completed template. The simplest way for a SIRT to make its template widely available is to publish it on its own information server so that clients in its constituency can easily find it. Templates published as pages in the World Wide Web should include the phrase 'SIRT Template' in their title - this will allow Web search engines to find them easily.

Whether or not templates are published in a repository, clients - and potential clients - of a SIRT will need to be able to authenticate a template (verify that it was indeed published by the SIRT) and check that it has not been modified (for example by verifying a digital signature for it).

To facilitate interaction between SIRTs, it would be useful to have a central repository for them. The GRIP Working Group believe that some of the existing Internet archive areas could be used for this purpose. The keeper of each template repository will be responsibly for verifying the identity of each SIRT lodging a template in the repository.

1.3 Relationships between SIRTs

In some cases a SIRT may be able to operate effectively on its own. It is much more likely, however, that a SIRT will need to interact with other SIRTs. Such interactions could include:

* Responding to requests for advice (e.g. "have you seen this problem before?")
* Reporting of problems (for onward referal to other SIRTs, to service providers or to vendors)
* Working co-operatively to resolve a security incident

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 client) simply contacts another SIRT and asks for help or advice. Note also that any client wanting direct help in tracking an incident must be prepared to provide sufficient information about the incident to make tracking possible.

In establishing relationships to support such interactions, SIRTs will need to decide what kinds of agreements can exist between themselves so as to share yet safeguard information, whether this relationship can be

disclosed, and if so to whom?

1.4 Establishing Communications between SIRTs

Once two SIRTs have agreed to work together - as outlined above - they need to establish secure communications channels. This section outlines some of the issues involved in this.

When a SIRT (SIRT A) wishes to establish a working relationship with another SIRT (SIRT B), a responsible person from SIRT A will need to contact a similarly responsible person at SIRT B. The SIRT B person then has the problem: "how do I know who I'm talking to?"

It is very easy to send forged e-mail, and not hard to establish a (false) identity by telephone. PGP and PEM provide effective ways of securing e-mail, but securing voice communications is much harder. At present call-back is probably the only simple authentication method. This may change as technologies such as scrambled telephones, or PGP-phone on the Internet become available.

PGP relies on a 'web of trust,' built up by having known (and trusted) people sign PGP keys. This model could also be used for SIRTs. To achieve this each SIRT should publish a list of the SIRTs they have peering arrangements (i.e. working relationships) with, including PGP public keys for them and the expiry dates of those keys.

2 Description Template: Security Incident Response Team

The Template is summarized in the section immediately below, and the remainder of the document describes its components. A 'filled-in' example of a template is given as Appendix C.

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 (STU-III, secure facsimile...)
1.7 Electronic Mail Address
1.8 Public Keys and Other Encryption Information
1.9 Team Members

2. Template Updates

2.1 Date of Last Update

3 Purpose of the Template

The Template which this document proposes is expected to be used by a response team to describe what it does, and in the process create criteria against which its performance can be measured. The Template does not attempt to specify a "correct" way for the team to operate, but does recommend on specific policies and functions seen as necessary for such a team to play a consistent role in the overall security framework. It also comments on additional roles a team might include in the ambit of its operations.

The primary purposes of the Template are:

- to help SIRTs improve the way they operate;

- to improve interactions between different SIRTs, and between SIRTs and other organizations such as vendors and law-enforcement agencies;

- to note necessary interactions with their constituencies in setting expectations and defining policies;

- to help new groups understand what it takes to "be" a SIRT.

A Template might appear to provide a marketing tool for comparing different teams, but this kind of marketing use (or abuse) is strongly discouraged by the GRIP Working Group.

3.1 Other Related Material

This 'Framework for Response Teams' document is the first produced by the GRIP Working Group. A second document will set out guide-lines for technology vendors to help them handle security incidents. The definition of terms given in the next section applies to both documents.

Another relevant IETF document is RFC 1244, the Site Security Handbook, produced by (and being updated by) the Site Security Handbook Working Group (SSH). Site requirements and recommendations are covered by the Handbook, while response team expectations and procedures are addressed by the GRIP documents.

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

* ftp://ftp.nic.surfnet.nl/surfnet/net-security/cert-nl/docs/reports/R-92-01

Some especially interesting documents are:

* CERT-NL Framework
  ftp://ftp.cert.dfn.de/pub/csir/docs/cert-nl.opframe.txt

* FIRST potential members
  ftp://ftp.first.org/pub/first/newmemlt.txt
  ftp://ftp.first.org/pub/first/profile.txt

ftp://ftp.first.org/pub/first/op`frame.txt

http://www.first.org/first

* NRL Incident Response Manual
  http://hightop.nrl.navy.mil/news/incident.html

* Bibliography
  http://www.cert.dfn.de/eng/team/kpk/certbib.html

4 The Security Incident Response Team Template

This material which follows is addressed to those responsible for Security Incident Response Teams.

4.1 Template Updates

Details of a Securty IRT change with time, so the template must indicate when it was last changed, who will be informed of future changes, and (by implication) who will not. Without this, it is inevitable that misunderstandings and misconceptions will arise over time.

4.1.1 Date of last update

This should be sufficient to allow anyone interested to evaluate the currency of the template.

4.1.2 Distribution list for Template Updates

Persons on this list are notified automatically whenever the template is changed. The list might normally cover the constituency and any other groups the SIRT has frequent interactions with. Readers not on the list can then recognise that they should check the central repository (above) for possible updates.

Digital signatures should be used for update messages sent by a SIRT to those on its distribution list.

4.2 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:

* mission statement
* constituency
* sponsor / affiliation
* authority

4.2.1 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 provide incident response, by definition.

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

4.2.2 Constituency

A SIRT's constituency (as defined above) 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 (below) should explain how requests from outside the perimeter will be handled.

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

People within the constituency have to learn that there is a Security IRT for their purposes; the building of a trusted relationship with the constituency is an on-going process which never ends.

4.2.3 Sponsoring organization / affiliation

The sponsoring organization, which authorises the actions of the SIRT, should be given next. Defining the affiliation amounts to stating: "Who is your God?".

4.2.4 Authority

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 hierachically within their perimeter, these should be identified.

4.3 Policies

4.3.1 Types of incidents and level of support

The types of incident which the team is authorised to address and the level of support which the team will contribute when assisting with each type of incident should be summarized here in list form. The Services section (later) provides opportunity for more detailed definition.

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.

4.3.2 Co-operation and interaction with other organizations

This section should make explicit the related groups with which the SIRT routinely interacts. 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.

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.

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.

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.

4.3.3 Reporting and Disclosure

The default status of any and all security-related information which a team receives can only be 'confidential,' but rigid adherence to this makes the team 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. Each team's template should specify any such restraints, both to clarify clients' expectations and to inform other teams.

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

An explicit policy concerning disclosure to the Press can be helpful, particularly in clarifying the expectations of a SIRT's constituency.

'Disclosure' includes:

- reporting incidents within the constituency to other teams;
- 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.

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

A team will normally collect statistics. If they are distributed, the template's reporting and disclosure policy should say so, and should list the recipients.

4.3.4 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.

At the moment it is recommended that every SIRT have, as a minimum, a PGP key available, since PGP is available world-wide. Teams may also make other mechanisms available, for example PEM.

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.

4.4 Services

Services should be defined in two sections, as listed below.

* direct incident response
  + verification of incident
  + technical assistance and analysis to understand the compromise of a system
  + notification of other involved parties
  + eradication
  + recovery

* optional
  + information provision

- vulnerability archive
- patches and resolutions

+ tools
+ education
+ audit and consulting
+ product evaluation

4.5 Incident reporting Forms

Samples of reporting forms used by the SIRT (or pointers to them) should be included at this point in a template.

4.6 Disclaimers

Although the template 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 recommended.

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

In situations where the original version of a template 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 our German template 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 for our operation.

5 Secondary Purposes of this Document

The primary audience of this document are the administrators responsible for communities of users, i.e. 'constituencies.' This section provides some brief notes on what SIRT clients should expect of their teams.

An incident response team exists primarily to support the clients in its constituency. It is vital that those clients understand what they should expect of their team. Provided that a SIRT has published its template, a constituent/client should be able to read the template and

discover what to expect, for example in such areas as privacy and

confidentiality of information, and whether the response team will be contacting downstream sites. Clients should certainly expect a SIRT to provide the services they detail in their template.

An important aspect of incident response is the 'follow through' - every incident should be investigated and appropriate actions taken. Clients should be encouraged by their SIRT to report incidents so that they can be acted upon. It must be emphasised that without active participation (especially reporting) from clients the effectiveness of the services they depend on can be greatly diminished. As a minimum, clients need to know that they should report security incidents, and know how and where they should report them.

Individual users (i.e. those who are not part of an organisation which provides a SIRT for its members) who observe a security incident should ask their Internet Service Provider for details of the most suitable SIRT to report it to.

Appendix B (below) provides some pointers to SIRTs which were known when this document was published.

6 Appendix A: Note on procedure definitions

Policies and statements of services in the template have to be implemented as procedures, but descriptions of those procedures should not be included in the template.

The following notes are intended to assist those seeking to form or to improve their SIRTs.

* External
  + identify other response teams
  + define supported clients:
    - by domain, through registration system, other means
  + establish secure communication practices
    - use of network, cell-phones, etc
  + define information that a client site must/should provide
    - use of reporting forms

* Internal
  + secure the team's infrastructure
  + protect information servers
  + protect sensitive data
  + define expiry of sensitive data

+ define disposal practice for sensitive data
+ establish methods for gathering and keeping statistics

+ establish 'knowledge base' of lessons learned from past incidents
+ create practical implementations of disclosure policies
+ document explicit practices for disclosure to the Press

The Site Security Handbook is a first resource to consult in securing a team's infrastructure. SIRT-specific security measures may evolve later.

7 Appendix B: Known Incident Response Teams

FIRST is the Forum of Incident Response and Security Teams. Information about FIRST can be found via their World Wide Web home page:

http://www.first.org/first

This page contains pointers to 'Team Contact Information' for SIRTs who are FIRST members, and to 'Teams with WWW Servers.'

8 Appendix C: Example: a 'filled-in' template

```
<HTML>
<HEAD>
    <TITLE>SIRT Template for XYZ SIRT</TITLE>
</HEAD>

<P>
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.
<P>

<XMP>

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. Template Updates

 2.1 Date of Last Update
        Please see the bottom of this Web page for this information.

 2.2 Locations where this Template May Be Found
        This template is available from the XYZ SIRT WWW
        site; its URL is
           http://www.xyz.org/THIS-INFORMATION-NOT-YET-AVAILABLE
>>   The template will be signed with the XYZ-SIRT's private PGP
>>   key. (WHAT TO DO? Sign just the template? The whole Web
>>   page? Try ASCII armor? Or have the signature separate?)

        There are no plans for the automatic distribution of fresh
        copies of this template after updates; please make sure that
        you are using the latest version by checking our Web site.

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 contituency 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

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

4.2 Level of Support

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 endeavour 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.

4.3 Disclosure of Information

>> &&&&&&&&&&&&&&&&&&&&

>> Difficult section; not done yet. Also, it overlaps heavily

>> with the section below; I'm not sure of the best way to

>> separate them. Questions not yet addressed:

- reporting incidents within the constituency to other teams;
- 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.

Food for thought:

Types of info:

- 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 info:
- 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 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 neighbours 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 eny 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 formalising 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 interect 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.

4.5 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 neighbour 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.

4.6 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

>> &&&&&&&&&&&&&&&&&&&&&&&&7

>> This section requires a lot of thought.

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; important issues of relevance to operating environments in use at the XYZ will be reported and archived.

- Auditing services
  - Central file integrity checking service for Unix machines.
  - "Tiger teams".
  - Security level assignments; machines at XYZ will be audited and assigned a security level: not all machines require or can attain the same level of security, but it is important to know which ones are reasonably secure and which are not.
- Archiving services
  - Central logging services for Unix machines.
  - Records of security incidents handled.

6. Incident Reporting Forms

>> &&&&&&&& Not done yet; I'll probably use an existing
>> one from somewhere initially.

7. Disclaimers

>> -- resp. for technical disclosures (bugtraq) etc.?
>> -- resp. for results for XYZ-SIRT advice?
>> &&&&&&&&&&&&&&&&&&&7
>> WILL NEED XYZ LEGAL COUNSEL ON THIS?

8. Additional Information

The version of this template published in this RFC will undoubtedly be out of date by the time you see it; it is intended as an example only. Please pick up a fresh copy from our Web site if you actually need information about XYZ-SIRT.

History of this template:

```
   1996/07/29  Jane Doe, version 1.0
      THIS VERSION HAS ABSOLUTELY NO MANAGEMENT APPROVAL!

</XMP>

</BODY>
</HTML>
```

9 Security Considerations

This document discusses the operation of Security Incident Response Teams, and is therefore not directly concerned with the security of protocols or network systems themselves.

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.

10 Author's Address

Nevil Brownlee
ITSS Technology Development
The University of Auckland

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