GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

BUILDING A COMPUTER SECURITY INCIDENT RESPONSE TEAM – FACTORS TO CONSIDER

Submitted by Shankarnarayan Dharmarajan

Submitted On: 12th Nov 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

BUILDING A COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) – FACTORS TO CONSIDER

Abstract:

The Internet has grown fast and wide and with it, has the threats to the users of this vast web of interconnected computers and devices. While some threats may be mitigated, there are others that need expert hands – Incident Response Teams (IRT's) act as these expert hands. This paper attempts to present the factors and the issues to consider when setting up an IRT. This paper provides by no means an exhaustive list, yet attempts to cover as many factors as possible.

Introduction:

It sometimes seems like computer and network security products are some form of magic potions that when installed on the Network provides all the security that is necessary. Firewalls prevent unauthorized traffic, authentication mechanisms prevent unauthorized people, and encryption prevents unauthorized reading. However, all of these are preventive mechanisms. Effective security includes real-time detection and response and constantly keeping in touch with evolving threats, and proactively taking steps to overcome such threats.

No Security Infrastructure can provide 100% security and hence when security intrusions occur it is important that an effective response mechanism be adopted that enables the Organization to effectively thwart, control or limit the damage caused by that incident. Equally important as the mechanism, is the time within which such a mechanism should be put into place. A combination of these two – the mechanism and the time within which such a mechanism is out into place constitutes an Incident Response and the Team that is designated to perform and co-ordinate such an action constitutes the Incident Response Team.

Definition:

Before we continue, it is necessary to set a base so as to have a common understanding about what we will be discussing in the remaining parts of this paper. Two terms stand out and we use the definitions provided by NIST

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

NIST defines an Incident Response Team as a one that performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency

NIST also defines a Security Incident by the words "A Security incident may be defined as an event which changes the security posture of an organization or circumvents security polices developed to prevent financial loss and/or the destruction, theft, or compromise of proprietary information. Also, an event investigated by an organization due to unusual activity, which cannot be explained as a consequence of normal operations."

Constituency[1]:

The definition of Response Team uses the term Constituency. The term constituency has various definitions each relevant to the context in which such the Incident Response Team is constituted. Constituency is the area (or a domain) in which that team operates and such an area may be bounded or unbounded.

It could mean any/ all or a combination of [2]

- CSIRT for a specific domain (Virus Control / Intrusion Detection and Control/ Defacement etc)
- CSIRT for a specific area/ region
- CSIRT for specific Industries/ Applications etc
- CSIRT for the Organization/ for the community in general etc

The responsibility of an Incident Response Team however, does not stop within its own Constituency. Every constituency is dependent on other constituency and so also are others dependent on this constituency. Hence it also becomes the responsibility of every Incident Response Team to interface with other similar teams (either in a completely different domain of expertise or in a similar domain, but in a different geographical area). Such interdependencies are what allow IRT's to thrive and provide useful services to the domain that they serve.

Such interdependencies may be for multiple reasons. It may be to tell another IRT about the scope of this IRT so that relevant queries may be directed towards it, so as to learn from/ pass on new methodologies adopted by IRT's, to define new services that this IRT now wishes to offer, to co-operate and work when such scenarios arise etc.

[1] The inspiration for this section was derived from "Forming an Incident Response Team, Smith, Danny, Australian Computer Emergency Response Team", page 4, Section 3.3 [2]

[2] The inspiration for these points were derived from Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 9, Section 2.1.2.1 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The factor of – "To co-operate and work" brings about an important thought in mind – who or what team/s OR agency would take charge where there are multiple IRT's involved. A classic example involves the interaction between the Local Police for the District and the FBI. Although the Local Police Department may be in-charge of the area, they cede control soon as the FBI arrives. This is important when different IRT's work together so that they don't step on each other toes and the entire operation is carried out in a smooth and efficient manner to resolve the incident at hand within the fastest possible time and the least possible damage.

Hence, an authority may be [3]

- Full Authority where the IRT completely controls and co-ordinates all activities for that incident or a combination of incident and all other IRT's submit to it
- Authority only if / when
    - The incident is of a particular nature
    - After another agency has completed its investigation
    - It may have further consequences than what are evident etc
- Partial/ Sequential Authority where it just performs a part of the complete Incident Response procedure and has authority only for that area
- Any other types of authorities

Communication:

True, an IRT may have authority and domain knowledge. However, the IRT would be of no use of this were not communicated to the external world. Communication to the external world may not be as simple as it sounds. Before advertising to the world about the presence of an IRT, it is necessary that the IRT form for itself a Mission Statement

Mission Statement[4]

This mission statement is important so as to enable the IRT and all its employees to understand what the ultimate goal of this IRT is. What was it constituted for, what actions does it perform, its scope and responsibilities. This allows the IRT to understand its purpose and allows every IRT member to have a common thread/ bondage that ties them together and defines a reason for their existence.

[3] The inspiration for these points were derived from Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 12, Section 2.1.2.3 [1]
[4] The inspiration for these points were derived from Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 8, Section 2.1.1 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

While a mission forms a central theme, it is also necessary that the Organizations and the common man outside are aware of what services are offered by this IRT. Communication both introduces a new Organization and improves trust in the Organization.

Communication

Communication plays a very critical role in the survival of any IRT, especially so if the IRT is in its initial stages of functioning. Communication may be broadly classified into three separate initiatives – communication to its constituency and communication beyond its constituency and finally Communication from its Constituency

Communication to its Constituency [5] & [6]

Communication to its constituency begins with telling the Organization as to why the IRT was formed and what are its goals – in-short, projecting its mission statement. It also includes

1. Informing the constituency about the services that are offered by this IRT and its areas of expertise
2. Informing period when such services may be secured from the IRT
3. Who is responsible for the delivery of such services (dedicated teams/ individuals)
4. How such services may be secured from the IRT
5. How should the IRT be contacted and what are the points of contact across the geographic regions that it supports
6. What are its secure methods of communication (and maybe its Public Keys) with the Client whose incident it is responding to OR on behalf of who it is acting
7. Which are the other IRT's that it co-ordinates with and what are the services that it sources / coordinates from other IRT's
8. What Federal Agencies does this IRT have links with
9. What are the SLA's that this IRT offers and for what incident levels/ priorities, Incident Categorization
10. Legal and Liabilities, Non-disclosure statements and Agreements
11. Its Sponsorship and Affiliation
12. What vendors is it interacting with and what relation does it have with them

[5] The inspiration for these points derived from "Forming an Incident Response Team, Smith, Danny, Australian Computer Emergency Response Team", page 5, Section 3.3.2 [2]

[6] The inspiration for these points were derived from Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 13-14, Sections 2.1.2.4 2.1.2.5 and 2.2.1.1 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

13. Security Incidents that have happened over the last period and what steps may be taken to protect against them
14. Potential threats/ incidents and what steps may be taken
15. The follow-up and follow-through where such capabilities may exist with the Organization/ Person that the IRT is servicing
16. and last but not the least – HOW CAN/ DOES THE IRT PROTECT ITSELF

Communication TO and FROM beyond its Constituency [7 and 8]

Most factors being common as described in the previous section, this also adds others specific to inter-IRT relationships

1. How will this IRT securely communicate with other IRT's and vice versa
2. Who will be responsible for the communication and for what part
3. When will/ may such communications happen
4. What responses and from whom may they be accepted
5. What priority would be given to this IRT and under what circumstances
6. What SLA's may be negotiated
7. What NDA's, Legal and Liabilities govern these agreements/ associations
8. How secure is information of this IRT with the new IRT
9. What other benefits can they bring
10. What Federal agencies do they have a relation with and how that expand this IRT's scope
11. What are their policies and how will such influence the operations of this IRT
12. What regulations are they bound by and how can their geographic reach be leveraged on
13. What information of theirs do we have access to and vice-versa

Communication FROM its Constituency [7 and 8]

While communication to the constituency is important, it is also important that the constituency also revert back with the same vigor and enthusiasm so as to allow provide and derive the best and the latest information / patches/ responses/ solutions from the IRT

1. What incidents have taken place in your Organization and how did you overcome the same – this may serve as a lesson to the IRT itself and

[7] The inspiration for this section was derived from "Forming an Incident Response Team, Smith, Danny, Australian Computer Emergency Response Team", page 5, Section2 3.3.2 and 3.3.3 [2]
[8] The inspiration for these points were derived from Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 13-14, Sections 2.1.2.4 and 2.1.2.5 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

which it can use to help other Organizations that may not have such skills/ time to experiment and react
2. Information to understand its spread and reach, and maybe its rate of spread to alert other constituencies
3. The type of systems and devices, the periods between which it affects
4. The situations that cause it to affect
5. The end result of a system or device that it has affected
6. Others

These and many more such communication are important factors allowing the IRT to serve its constituency to the best of its ability. The best constituency is that where its constituents share the burden and bear a responsibility towards that IRT hence allowing the IRT to work in the best interests of all it serves.

Although we have described what needs to be communicated, it is necessary to also look into how this communication should be achieved – this varying based on the domain of the IRT, the area in which the IRT is being considered and the means available within such areas.

Communication may be achieved with the help of pamphlets and flyers OR they may be achieved with the help of bill-boards. They may be achieved with, through promotional campaigns, through advertising over multiple media, through the associations that the IRT has built with other IRT's. Alternatively, the IRT may be advertised by its associate companies, the company that promotes it or that it ally's with, e-mails, USEnet, press-releases etc.

Whatever be the means of communication adopted, it has to be oriented towards garnering the support of the members of the constituency that it intends to support without which the concept would not fly. It is more like a politician running through his election campaign. The end result of this is that the existence of the IRT and the services that it intends to offer has to be made known to the constituents. It forms the most grueling part and hence sufficient understanding and study of the constituency should be made before the launch.

Communication Infrastructure

Assuming that communication has been successfully completed, the next step is to be able to successfully respond to brave few (after all everyone is circumspect about revealing information to a little known team) who report their incidents to the IRT. This is a very crucial phase as the entire future of the IRT now depends on these few and their marketing prowess.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The first pair of questions that now arise – what means of communication & services have been promised and what SLA's have been promised at the time of marketing the IRT.

Communication means vary – telephones, Internet mail, Web forms etc. What ever the means adopted or advertised these have to be in place and tested long before the first call comes in.

Phones:

Phones are very critical and are the first means of communication that a party will reach out to when an incident strikes. Hence, it should be available at all costs. Phone systems are of varying nature and the right system needs to be chosen. Generally, phone systems should have

1. Capability for call pick up and transfer from any extension on the premise
2. A centralized call switching system
3. A system to switch and answer calls where the person is not available at that time
4. Accessibility to National and International dialing
5. Capacity to interface with existing infrastructure and be upgradeable in future to meet anticipated requirements
6. Capability to categorize (where appropriate) calls and constituents
7. Capability to redirect suitably (through a system or an operator) when responding to calls beyond the scope of this IRT
8. May require multiple Telephone service providers (probably, just for redundancy)
9. Capability to interface with a pager / mobile phone system / network to contact while on the move or at site
10. It may also be essential to define a system that protects against miscreants and overcomes "Denial of Service"

FAX:

FAX is another major component to be considered. A FAX system is useful from multiple angles. For one it can be used where the phone system is not accessible. It may also be use for communicating and sending relevant details during the non-working hours of the IRT. It may also be used to transfer log sheets, diagrams and anything that may need to be written and sent out over paper. Sometimes, with electronic mail systems going down, FAX may be the best form of communication. However one needs to consider

1. The FAX is always replenished with paper
2. It is available and accessible as a dedicated FAX machine and not a phone-cum-FAX

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3. Maybe where the FAX can store data in electronic form in memory and later be able to reproduce on paper (where incoming information is faster than what can be pronted)
4. Capable of National and International dialing
5. It is similarly subject to Denial of Service attacks

Round the Clock Contact and Contact on the move:

We do not know when an Incident can strike. Hence it is important that (although the IRT may have defined hours in which they attend to services – based on the type of services), they may need to have a system that accepts & logs/ records calls that can be attended to the next working hour.

Alternatively, the IRT may provide for a system where the constituents may contact it or designated personnel of the IRT after its normal working hours. A third system may provide a 24-hour contact and assistance system provisioning dedicated subject matter experts. All of these require a communication facility – either through a Mobile phone system, a pager or through Wireless data infrastructure (such as those supported by the 802.11a, b, g systems, Infrared, Bluetooth etc)

Additionally, the numbers provisioned may be to a paid or to a Toll free number. Here also, given the skeletal staff that a lot of IRT's observe during non-office hours, it is important to have a system that protects from miscreants, false alarms and attempts for Denial of Service

ISP Connectivity: Most other forms of mass communication require connectivity to the Internet and hence to an ISP. While considering an ISP connection, the following thoughts need to be kept in mind

1. Capability to quickly (based on call volume) be able to access information that is there on the internet
2. May be able to remotely log into the components affected by the incident
3. Be able to connect to other sites and other IRT's
4. Access to Internet mail for communication purposes
5. Access to Internet for
    a. Education of the staff
    b. To keep themselves up-to-date of the potential threats and methods to overcome
    c. Maintain and update a local database of information
    d. Download useful tools that may be used for reconnaissance/ to thwart
    e. Connect and communicate with constituents frequently about potential threats and how they may be overcome
    f. Be a part of useful chat of lists, mailing lists etc
    g. and a multitude of other needs

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

6. Connect to more than one ISP
    a. To provide for redundancy
    b. To take the advantage of different types of services (Leased, Frame Relay, Wireless etc)
    c. To take advantages of different types of SLA's
    d. To take advantages of the geographic reach
    e. To consider the facilities offered by the ISP's (filtering, hosting, etc)
    f. Trust and influence of the ISP in the market
7. Relationships of the IRT with the ISP
8. Policies of the sponsoring/ supporting, affiliated Organizations etc

E-mail:

Email is one among the most used and most abused of all communication mechanisms and its need and usefulness in today's setup needs no campaigning. The benefits of e-mail need not be stressed. Most Computer Security IRT's today respond though only e-mail or through phone and only where there is a situation of extreme importance do they come to your door-step. However factors need to be considered when setting up an E-mail infrastructure.

Primarily it is important that this e-mail be able to receive and address all type of communication format and also be secure. How secure – secure from the angle of being able to encrypt and confidentially transmit and receive data (PGP may be a method of use) as also filtering the right type of e-mail to be received by this IRT, avoiding spam email and other such similar filtering. The fact that this organization is an IRT itself is a reason for this e-mail setup being the target of attacks.

It is also important to know when and where to use what type of e-mail – based on comfort level of the users, compatibility with other mailing systems, its interfacing capability with other formats, its features etc. This provides faster and easier incident resolution given the users comfort and its capability to interface.

It can serve as the primary means of communication where the affected organization may be able to send and receive information, network diagrams, infrastructure details, logs, historical information etc. Again, this confidence to send/ receive information is there as long as the constituent is sure that the confidentiality and integrity of the information was maintained. PGP or Digital signature may be used. Hence a secure e-mail system assumes primary importance.

Another e-mail system may enable interfacing with a central or regional database that is constantly updated. With the help of a appropriate interface, it may be possible to pro-actively inform constituents of impending incidents

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

and how they may protect themselves. Some Organizations may regard this as spam, but most are thankful about it. In other cases automatic e-mail responses for dedicated classes of incidents may be enabled.

Some may use e-mail as a way to trigger the response, while others may offer a priority to the means by which information reaches them (phone first, email next etc). It is important that the IRT's members' official mail-ids be never revealed. These may sometimes be used as Trojan horses mediums to get into the IRT network. All mail should be channeled through the right interfaces for that incident and criticality through tracking numbers, incident referrals etc

Over the Web:

What needs to be said about the ubiquitous web? It is everywhere and accessible by everyone. One of the best ways that may be used to access the IRT may be through the web. The IRT may provide for a form – generic or customize to the different services that it provides.

These forms contain information that needs to be filled by the constituent when he needs access to the services of the incident team. Generally these forms are just compact enough to capture all the information that the IRT is looking for and may be a real bet where the IRT is always busy OR where the constituent can afford to wait that bit longer for the response. The forms may then be mailed to the IRT or they may be passed on though other means. The same forms may also be used by the IRT to set priorities where phone based incidents are attended first and then the e-mail based and finally the web based and so on.

It enables creating a structured approach to help IRT team members to collect all the information form the prospective constituent and to serve as a record while helping him with the response. The same may be used by a co-coordinator to try and allow the constituent to explore options while the experts are busy with another call.

Such forms also provide another benefit where they may be used as logs and records of the incidents that were attended to – may be for statistical analysis – to understand its spread, how many systems were affected, how, the financial impact etc, the symptoms faced, the solutions provided, the options tried (to act as a database etc). Whereas the web based methodology enables direct recording of the information at the first go, in all the other means of contact the information needs to be collated and accumulated – either from the different sources that have attended to the call or have provided solutions. Such information may also be quickly shared with other IRT's with which this IRT co-ordinates or works in association with.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

IP Addressing and Sub-netting

Communication media uses the standard protocol, IP. Every setup is offered an IP Address or a set of IP address. Being an independent entity the IRT needs to apply for its own IP Address space. These may be derived from agencies like APNIC or the local representative for the geography. Alternatively, the Service Provider may provide the same. When using the services of multiple providers, IP Addressing needs to be carefully planned and implemented.

Given the lack of large IP spaces, it also becomes the responsibility of the IRT to conserve IP addresses as far as possible. This necessitates the use of Private Address space and concepts like NAT and PAT (Port Address Translation).

Sub-netting is necessary to ensure logical division of the IRT into its constituent networks – some that may need public and others that need private spaces. This also helps better plan and isolate portions of the network. With geographic spread, it may be necessary to plan and scope the addressing across regions. Where the networks are divided in to multiple types of network each defining to a particular level of security, the same may be achieved through the use of subnetting. Networks may be divided in to "Public", DMZ (providing limited facilities), Private and Highly Secure Networks. The DMZ may be provided controlled access from within and from the outside, the Private Network may contain the LAN of the IRT whereas the Highly Secure may contain the Test Equipment of the IRT. Other Networks comprising the Database Server, the Storage and the backup and other Severs may also be provided.

Routing Protocol

Where the network is spread across multiple geographies, choosing the right routing protocol is very essential as also when interconnecting with Service Providers and other IRT's

Equipment

Well, we got all the information about the incident – through either mail, or phone or through the web etc or a combination of means. What do we do with all this information? Moreover as the IRT's are dealing with both known and unknown incidents, it is critical that they understand the impact of the solutions that they are providing. To achieve this it is important the every IRT has a self sufficient set of Networking, Computing and Security devices that they may use to either connect to the Network where the incident has taken place or where they may be safely tested.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Test Equipment [9]

The data collected from the constituents should be analyzed to derive information and provide a response to the constituent. This requires that the IRT keep itself updated with the latest equipment that are available in the market and choose to invest, rent or lease the best and maybe the latest equipment in the market. This equipment should serve the needs of the constituent to the maximum and best possible way.

Test equipment can range from devices, to software and in certain cases even copies of virus/ Trojans. Other test equipment includes simulation tools, traffic generation tools, result evaluation tools and a host of other associated paraphernalia.

Such testing may be done in-house where possible or at Organization which has been affected. Sometimes lack of funds may prevent the Organization or the IRT from investing into the equipment. In such cases facilities that offer such capabilities or the judgment of the IRT personnel need to be used. Such facilities should not use critical data and may be provisioned on a different subnet itself.

Where the IRT is testing vulnerability or a virus, Trojan etc, a separate subnet should be adopted so not to disrupt the production / affected network. In certain cases, it may be necessary to simulate as far as possible the network and the activities in which the incident actually took place. This approach needs very careful consideration by the IRT to ensure that it does not do further damage to the setup. In certain other cases, the IRT may provide the facility for penetration testing of the affected site.

Test equipment may not be enough – the facility should also possess sufficient documentation and documentation equipment so that the results are quickly documented and evaluated. Test should be planned – the objective of the test, the tools need, tools available, what results to gather, how to gather and finally who, the when and how the analysis will take place.

Equipment for Facility

Assuming that communication has been successfully completed, the IRT will now need equipment to constitute a network of its own. This Network will involve Switches and Routers for regular LAN and WAN connectivity. To connect to the other Networks they will need a secure communication link between themselves and the external party. The external party may be

[9] The inspiration for this section was derived from "Forming an Incident Response Team, Smith, Danny, Australian Computer Emergency Response Team", page 15, Section 4.4.4 [2]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

another IRT with which this IRT has / proposes to have a long standing relationship which may justify a dedicated line with a backup OR it where "when necessary" interactions exist, a VPN or other similar lines may be established.

Where the IRT wishes to log into a Clients Network, it may need the use of a secure VPN tunnel with high degree of encryption. It needs a Firewall for the Internet connectivity OR may and may need an IDS for detecting external or Internal Intrusions. Content Filtering (this could constitute malicious code filtering Anti-virus software etc) may be another point to consider.

Once announced, an IRT itself becomes a target of attack and hence a lot of the IRT's credibility depends on how immune it can remain and how well it can respond to incidents against itself.

The need to project itself to the outside world necessitates a Domain Name and a Web page reflecting the activities of the IRT, any warnings to the outside world, responses to incidents. All of these are communicated through the all pervasive Internet. This requires the services of components like Web Server, DNS Server one or more suitably placed DHCP Server for addressing – maybe with multiple scopes. An Intranet for internal users, an Extranet for partners and their associated equipments may be another thought.

Other things to consider include the Operating Systems for the desktops, for the different Servers, the Proxy etc. Authentication and authorization form another area of concern – who will authorize or may be authorized and with what liberties/ restrictions – what information needs to be accounted and logged for further analysis from the IRT's own network etc.

Authentication, Authorization and Accounting (AAA) also plays a role when others – either known partners or people over the Internet connect to the IRT. What rights and privileges do they have, what activities of theirs need to be logged and accounted for, when, for what duration etc?

Database and Storage

In the previous paragraphs we spoke about equipment that is needed to test and connect. Here we speak about equipment needed to store information. Apart from itself generating volumes of information, an IRT receives and collects a vast amount of information from external sources. Apart from this confidential client information is also collected during period of incidents.

All this information must be cleanly and securely stored. Some may require long time storage while others may require storage for very short periods. Still others may be highly confidential information where as some may warrant public knowledge. A storage infrastructure with a database may be essential

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

in these scenarios. Information or data needs to be stored in a quickly and easily accessible way on these storage devices. Multiple database vendors and storage vendors provide varying solutions. Databases enable quick, easy, sequential or random access to information stored on their databases. Storage Infrastructures vary (based on the choice of cost, applications, speed of data retrieval etc) from SAN or NAS to Direct Attached Storage. A new concept integrating NAS and SAN to FAS is now gaining popularity. Associated with the storage adopted is its paraphernalia of switches, cables – some proprietary, others standard etc.

Data being susceptible to corruption, one or more levels of redundancy may be necessary. Such levels of redundancy include information storage redundancy, access component redundancy, network redundancy etc.

Backup and Shredder

Data may get corrupted; confidential data may be accessed unauthorized etc. All these require some form of a dedicated backup and retrieval procedure that ensures that essential data is regularly backed up and maintained confidentially. It is also important that such data be periodically tested for retrieval to ensure that it will available at the time of crises. Another reason for the backup of data is to ensure that data that is not immediately necessary need not fill up precious storage space.

As a precautionary measure, it may be necessary to maintain a Disaster Recovery (DR) site that provides as a backup in the event of the primary failing. All data that is backed up may have an additional copy that is maintained at such places

Media used for backup may vary from off-line backup using tape media to online backup where the information synchronously or asynchronously travels to a remote site and may be backed up on another disk based system. Data backed up may or may not be encrypted.

While important data needs to be backed up and maintained, there may be some data that are of one time use or maybe too confidential to be maintained after their intended use. Such information should be deleted and destroyed. These may be on electronic media like low-level formatting may need to be used or on magnetic media where degaussing may need to be used. Printed Data may need to pass through the shredder. Others (not very confidential) may be disposed off in the waste-paper basket (beware of dumpster divers) and still others may need to be burned after shredding[10].

[10] The inspiration for this section was derived from "Forming an Incident Response Team, Smith, Danny, Australian Computer Emergency Response Team", page 16 Section 4.5 [2]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Safe [11]

Some documents may need the use of safe – typically physical assets like Hard-disks, Printed paper or Tapes with backup data. Safes must be Fire and Tamper proof, being maintained at a safe and secure place

Staff and their Skills

While the IRT begins all the staff are fully equipped to deal with small numbers of requests that arise from the constituency. As the importance and the popularity of the IRT increases, the number of calls and the time to address the call varies inversely. In this case, it is necessary that additional staff be sourced for the IRT to meet the demand.

Background Check

Although sourcing per-se may not sound like a big job – consider the fact that this is an IRT and we are dealing with confidential information of people who have been affected OR have the potential to be affected. You may be the first to know about an incident or the first to know about vulnerability. In any such scenario, trust and confidence in the individual plays a major role. Typical considerations like

1. Who is he/ she
2. What is his / her background and what references does he have
3. What level of confidence does his previous company pose in him
4. Does he have any previous history or previous law records of illegal activities

Staff Expertise

Most people believe that the most important factor that is necessary to get into a IRT is Technical background – this is true to some extent – but not completely. There are various other factors that also need to be considered when hiring them. Some of these may be broadly defined as follows

1. The Technical Knowledge of the Staff. Broadly speaking he/ she should have the capability for [12]
    a. Public data networks (telephone, ISDN, X.25, PBX, ATM, frame relay)

[11] The inspiration for this section was derived from "Forming an Incident Response Team, Smith, Danny, Australian Computer Emergency Response Team", page 16 Section 4.5 [2]

[12] The text below was reproduced from the Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 135, Section 4.5.1 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

b. The Internet (aspects ranging from architecture and history to future and philosophy)
c. Network protocols (IP, ICMP, TCP, UDP)
d. Network infrastructure elements (router, DNS, mail-server)
e. Network applications, services and related protocols (SMTP, HTTP, FTP, TELNET)
f. Basic security principles
g. Risks and threats to computer and networks
h. Security vulnerabilities/weaknesses and related attacks (IP spoofing, Internet sniffer and computer viruses)
i. Network security issues (firewalls, virtual private networks)
j. Encryption technologies, Digital Signatures, Cryptographic Hash Algorithms
k. host system security issues from both a user and system administration perspective (backups, patches)
l. Intrusion Detection Systems and Intrusion Prevention Systems

Specifically, he may need to have knowledge of

a. Thorough Operating System knowledge – one or more than one – the security issues that it faces and the ways and means to overcome the same
b. Need to have knowledge of Vulnerability Assessment and Penetration Testing
c. Computer Security Forensic Analysis
d. Industrial Espionage
e. Software Coding and debugging
f. Maybe the need for specific devices and components that the IRT deals with
    i. A product from a particular vendor
    ii. Only Virus, Worms or Trojan attacks and hence knowledge of different types and products of Anti-virus software
g. High Security Area clearance – operations and procedures when operating with Governmental Agencies

He also needs to have interpersonal skills that include[13]

a. Common sense to make efficient and acceptable decisions whenever there is no clear information
b. Rulings under stress or severe time constraints
c. Effective oral and written communication skills (in native language and English) to interact with constituents and other teams
d. Diplomacy when dealing with other parties, especially the media and constituents

[13] The text below was reproduced from the Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 135, Section 4.5.1 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

e. Ability to follow policies and procedures
f. Willingness to continue education
g. Ability to cope with stress and work under pressure
h. Team player
i. Integrity and trustworthiness to keep a team's reputation and standing
j. Willingness to own up to one's own mistakes
k. Problem solving to address new situations and efficiently handle incidents
l. Time management, in order to concentrate on priority work
m. React appropriately to Constituents emotions

Staff Retention[14]

Not only is the initial staff hiring sufficient. It is also important that good staff be retained and be allowed to grow with the Organization. Among the most primary cause of Retention problems is the high rate of burn-out. While a lot of days may pass peacefully with the staff engaging themselves in their day to day work – testing, documenting, education etc there may be days when a new virus has struck or that the security has just been breached at a local constituents premise etc. Hectic activity soon follows and the whole place or a set of people suddenly swing into action – working day and night they clear the incident which sometimes runs into many days of the week and maybe even over the weekend. Such people need to be given a break from their work pressure.

There may be others that have monotonously been at their post for the last many weeks and sometimes months – these people need a break, a rotation from their jobs so as not to get them bored with their jobs and leaving to learn fresh technology in other Organizations

Personnel need to be rotated, they should be given a chance to express themselves, participate and involve themselves into Seminars, Conferences and other activities of the Organization. They may need to attend trainings to augment their skills. Basically, they need a growth path that they see and perceive to be right.

Staff Training

The initial training of the staff may be focused on being trained in the respective job responsibilities. These are sufficient for a period of time after which it becomes essential for the staff to be trained in either specific areas of preferences or in new areas where the IRT wishes to foray. Training may also be

[14] The inspiration for the following section from the Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 140, Section 4.5.5 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

to learn and understand better techniques, software and hardware that have evolved over the months and years.

Training also is a method to allow in-house expertise to be recognized and advertised. Some employees may have their potential/ expertise in specific areas. These employees may train their other staff and bring them upto their own level. Trainings may be in the form of case-studies, technical descriptions, applying thought, finding alternate solutions to a problem

While on one side this advances the Technical knowledge of the individual, on the other side it also builds camaraderie and team skills within the staff. They being to work as a team and their efficiencies improve in understanding problems better, digging for details (new methods of investigation that they learn from their/ other colleagues and friends) etc. This can also have role play; improve communication skills – both internally and with the constituency

This can also help in improving local policies based on staff experiences and communicating the needs of the IRT, its new proposed policies and approaches etc.

Staff Arrival and Exit Procedures[15]

An IRT is like any other Organization – staff is added onto its rolls and staff leaves its rolls. When staff are added onto the rolls they should be run through an induction program that clearly spells the policies and procedures adopted by the IRT, a he/ she should be provide with a clear definition of the roles and responsibilities that he/ she has been inducted for, what is expected of him/ her and made clear as to what will be the consequences if he fails to meet the above. He / She should be provided with all necessary tools and devices to perform his duties. He/ She should also be made to sign a bond with the company that he has understood what all what has been communicated to him and that he / she will abide by it.

Upon his exit from the IRT all privileges provided (except those legally permitted) by the IRT should be withdrawn. This should be done immediately or within a minimum defined and safe period. Withdrawing privileges include returning Identity cards, blocking access to sensitive areas, removal of his/ her mail-identifiers, post exit contact details etc. In addition he/ she should also be counseled as to how he/ she is bound to certain non-disclosure, certain proprietary information etc and an exit sign-off signaling his / her agreement to them should be taken. It should also be made public that he/ she left the services of the company and that no further dealings should be made with this individual after a particular date

[15] Term taken and ideas derived from "Handbook for Computer Security Incident Response Teams", Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 138, Section 4.5.3 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Dealing with Technology

Technical training that may be provided to the staff is dependent on the Technology that this IRT wishes to deal with. The IRT should identify Technology that it would deal with and address – this could be technology from a product vendor or a particular class of technologies or type of products (only Anti-virus, only intrusion detection), or only a particular type of job (Computer Forensics etc). This allows both, the Organization and the employee's to focus on such training, the employees to know what they are expected to know and understand and complement each others skills to achieve the response to an incident.

Budget and Funding

A lot of the factors that we spoke about earlier are dependent on what budget the IRT has. When its starts, the IRT may have a limited budget, but as it grows OR as Organizations and Groups come forward to fund it, it slowly is able to meet its needs.

Funding may be for a specific purpose or funding may be generic. In all cases, the IRT must ensure that when requests for funding go out, they consider all the issues at hand – maintaining the infrastructure like phones, communication equipment, links, training, the test equipments, tools and tackles etc. Funding may also be through a method where some of the services – say Computer Forensics, Vulnerability Assessment and Penetration Testing are provided as a paid service and the funding provided by these in combination with external funding sustain the IRT.

Identify Depth of Analysis[16]

The more an Incident is analyzed, the better the solution/s to overcome it and the better it is understood. This can lead to better and more long lasting solutions, more effective future reaction mechanisms, lead to better understanding of other similar incidents and their co-relation to new incidents.

While on one hand the greater depth to which an incident is understood, the better. This may not be possible in all the cases. This may be due to budget contains, time constraints, people constraints, lack of proper knowledge/ depth of knowledge, tools and many more things. Hence the IRT should be able to strike a balance of where it needs to stop analyzing such incidents and at what depth. This may directly affect its capacity to respond to the incidents and curb its capacity to provide better solutions –however these can be overcome by being more specific when defining the services that it

[16] Term taken from "Forming an Incident Response Team, Danny Smith, Australian Computer Emergency Response Team", page 9, Section 3.9 [2]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

provides. The IRT may provide limited information on certain areas, while providing a complete walk through with the constituent in other more familiar incidents. The IRT may provide work-around in some situations while it may redirect them to IRT's that can better service their calls in other cases. Sometimes, this IRT may seek the help of another IRT for an area in which it has no expertise and then pass on that information to the constituent. This serves in self-learning and of solving the constituent's problems

Information Library and Database

Well, we spoke about the staff learning new things through training through interaction etc. However there should be a methodology for this and facilities should be provided for this. This includes

a. Setting up Libraries that subscribe and provide access to
    i. Periodicals and Journals
    ii. Reference Materials
    iii. Books on various technologies – both dedicated and generic
b. Access to Internet – which may be considered as the worlds largest library
    i. Secure access to dedicated databases setup by other IRT's
    ii. Access to mailing lists that deal with specific issues or generic security issues
    iii. Access to specific vendor related issues, bugs, announcements of new vulnerabilities
    iv. Access to dedicated forums and their databases

It is also necessary that the IRT maintain its own database and secure / restricted information portal that can act as a knowledgebase for its own staff. Every incident that is solved by a particular team/s is documented on this database. It may contain what information was received, how it was diagnosed, what additional data was considered, what assumptions were made and why, what approach was taken and how the incident was finally resolved. It may also contain where additional information on such topics may be found – books, journals, website url's, newspaper clippings.

Some other means of maintaining ones information database includes visiting other IRT's, communicating and discussing their approaches and methodologies, performing joint simulation exercises, any past reading up case-studies. It may also include meeting up with experts in the area of concern, understanding technologies and capturing that, providing the facility of e-learning/ distance learning

Perhaps among the best and most efficient approach may be to download/ purchase tools off the web, from the market etc and simulate scenarios using such tools in dedicated and isolated labs. This provides first hand information on

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

both – how to respond to such incidents, and what functionalities such tools have – the data derived can then be fed into the database and be made useful to others.

Policies:

Policies are fundamental to an Organization. They spell out how that Organization functions and will function in defined circumstances. An IRT is more than an Organization – it defines and formulates responses for its constituency and hence it is necessary that it has on its own a set of policies that define the way it operates. It is also necessary that this policy / set of policies be communicated to its constituents at a high level as also to the other Organizations and IRT's that it works with.

Information Policies specify how information present with the IRT will be handled – of clients, of other IRT's and Professional Organizations and its own internally generated information. These may further be classified as Information Categorization[17] and Information Disclosure Policy. This includes how information is categorized – public information, private information, confidential information, internal information etc as also when information of a particular category needs to be revealed or disclosed to a third part what policies are followed – ensuring that the constituent is informed if it is his data, how to disclose information gathered from another IRT, or how to reveal information to a Professional Organization etc

Security Policy:

Security Policy is defined as the means, measures and technologies that will be adopted to maintain the security of information. This could range through the encryption technology, the Anti-virus policy, user authentication policy etc

Press Policy:

This discusses the policies that will be adopted when dealing with the press, when revealing information to the press etc. This policy needs to be very clear. It may influence the image of Organizations falling under the constituency if some information is revealed, alternatively the wide reach of the press may help in carrying information on some potential threat and means to overcome the same.

Call Policy:

[17] Handbook for Computer Security Incident Response Teams, Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 114 – 115, Section 4.2.2 and 4.2.3 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

How is a call handled once it comes into the IRT? What factors influence its priorities, how will it be processed and how will information be communicated back to the constituent. Different calls may be given different priorities – phone calls may be provided first priority, e-mail next and web-based calls will be provided third preference (here we assume that the constituents are responsible users of the respective media). Alternatively, incidents of a particular nature or a particular gravity, of a particular Organization/ Individual profile would be given preference over others.

Legal and Law Enforcement:

The following policies are concerned with how anything that has legal implications OR what policies will be adopted when the IRT deals with Law Enforcement Authorities.

All policies have three important constituents – they have an Attribute, the Content of the Policy and it's being validated followed by finally its Enforceability. Attribute refers to the characteristics of the policy – it should be clear, concise, useable, enforceable etc. The content refers to what should be done when the policy is being implemented on – may be the roles, the responsibilities, the procedures, its relation and maintainability etc. Finally it should be enforceable practically under all conditions for which the policy was derived. This must be validated so as to ensure that they are enforceable, they are in the true spirit, they do not violate other similar policies etc.

Legal and Law Enforcement

Legal and Law Enforcement[18]

Legal and Law enforcement are very crucial factors when considering the working of IRT's. All legal issues should be resolved before the operations of the IRT begin. Certain countries and certain constituencies have legal laws that the IRT's should consider and abide by. It is important that the IRT frame policies, rules and regulations governing itself, its interactions with its constituency, other IRT's etc and that fall within the gamut of rules and laws specified by the agencies.

Again, it is also important that the information that is possessed by the IRT, both because of its interactions with the constituency or because of its interaction with external agencies, information derived within – the disclosure and use all of these should be within the bounds of the legal framework. Some countries and geographical regions have different rules as compared to

[18] Inspiration for this section was taken from "Handbook for Computer Security Incident Response Teams", Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 92, Section 3.7.4.5 [1]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

other regions – maybe between different states in the same country, it is essential that the policies and the operations of the IRT's in these areas conform to the rules and laws of that area. The same activity may be a violation of a rule in one state while it may be permitted under certain circumstances in another.

Legal issues should be an important point for consideration when signing Contractual Agreements – understanding the jurisdiction under which such a contract works, the framework of the contract, what are binding, the common-mans meaning of legal words. While defining Service Levels, it is also important to understand what the legal implications are of not delivering to that service level. Service Level definitions are very subjective and hence the IRT should be all the more careful that the intended meaning of the level is conveyed through the agreement.

Policies and procedures adopted by the IRT should fall within the Legal framework. Waivers and Disclaimers need to conform to the legal laws of the country, the sate or the Organizations. Inappropriate disclaimers should be removed as also inappropriate waivers. When signing contracts or other legal information, such clauses may not stand water in regions that have strict laws and may even cause the contract to fall through. In other places, it may not be as easy to waive off responsibilities.

When adhering to Non-Disclosure agreements, strict observance of the laws is necessary as the information provided is very confidential and critical to the company that provided such information. The legal penalties for leak of disclosure of such information – either inadvertently or intentionally may can be millions of dollars in penalties or maybe imprisonment in some cases. Such non-disclosure agreements stop not only at the team/s that handles the information – the entire Organization is responsible to respect it and it does not stop even if the employee leaves the Organization

Other factors include providing legal advice to its constituents. Generally, the IRT is regarded as a safe bet for legal clarifications on Information Security, disclosure etc. Only where such technical expertise exists should advice be provided, else the person/ persons should be redirected to a legal expert. Incorrect advice can make one liable for prosecution. Moreover as the laws are highly local, it is important that one or more local legal advisors/ experts assist the IRT where such advice is being provided.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Liability [19] and 20

While still talking of Law, the IRT must specify what its liabilities are if there is a breach. While this does not make it immune to the law, this atleast clarifies to the Organization/ individual accepting its services as to what legal responsibilities the IRT will accept for a breach. Liabilities may be for a SLA breach, breach by information disclosure, breach of a contract, incorrect or incomplete advice, propagating false information etc

This may also help reduce the financial impact that the breach may have on the IRT. Moreover, it also clarifies the stand that the IRT takes in the event of a breach as also improves the image of the IRT. While some countries/ regions are very strict about liabilities, others offer a more relaxed approach and hence it is subject to local laws and local legal advice must be taken before liabilities are announced

The IRT in Operation

While the IRT is in operation, it is essential that it performs and maintains some defined routine and procedures. These procedures include

1. Regularly updating the database
2. Visiting some well known sites and analyzing information on newly discovered vulnerabilities
3. Finding ways to improve the response time to more familiar incidents
4. External Interactions (with IRT's, constituency, Professional Organizations etc)
5. Understanding new technologies and tools and may include experimenting with them in the lab
6. Data backup
7. Others

Apart from these routine tasks, the work of an IRT remains largely dependent on the occurrence of an incident. Once an incident occurs, based upon the incident a defined procedure may need to be followed to completion or partially. Where the incident is familiar and operational procedures are already documented, the team just follows the procedures. Where such documentation does not exist, the team reacts to understand the implications of the new incident, find solutions for

[19] Inspiration for this section was taken from "Handbook for Computer Security Incident Response Teams", Moria West Brown, Don Stikvoort, Klaus Peter, Kossakowski, 1998, page 39, Section 2.3.2.2 [1]
[20] Inspiration for this section was derived from "Responding to Customer's Security Incidents--Part 3: Following Up After an Incident", Sun Microsystems, Article Courtesy: Prentice Hall PTR, Ref Section: 3 [7]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

it, contact other IRT's, search on the web, try different ideas and experiment with new methods, simulate in the lab etc

When an IRT is in operation, and an incident occurs, it is essential that the IRT operates in a certain manner where data about the incident is clearly recorded, documented and maintained. These factors are documented in a manual like format that forms the Operational procedure for attending to a call – a few parameters are described here

1. Recording the Incident characteristics
2. Recording the Infrastructure on which the incident was discovered
3. Recording when the incident was first reported, and how was it sighted
4. Recording what damage the incident has caused
5. Recording how the damage will affect the Organization or the individual in concern
6. Recording the type of help required and the SLA's defined
7. Allocating a trouble ticket and redirecting to a subject matter expert
8. The subject matter expert working with the client to solve the problem if it may be cone using the collected information
9. Attempt to try generic procedures that may solve/ alleviate the problem
10. Collect additional information form the client where required
11. Attempt to determine the solution OR an approach to the solution from external parties or from colleagues
12. Test the solution where necessary (if the solution deviates from a well known or well adopted solutions)
13. Implement the solution, discuss the solution with the client
    a. Discuss the solution
    b. Discuss with him with the pros and the cons of the solution
    c. Discuss the effects of the solution
    d. Discuss the additional software / hardware that may need to be downloaded/ purchased
    e. Guide the constituent through the solution implementation

Although these represent at the high level the routine work that needs to be done by the IRT personnel, there are further steps that this needs to be broken up into to enable the staff to effectively carry out their duties and provide a consistent approach to all the constituents that contact it.

These details need to be presented in the form of a manual – one that needs to be rigorously followed. This serves another purpose in that it acts as a checklist [21]and helps the user to have all the details that need to be collected – whether he personally handles or works with another subject matter expert to handle the case OR when the case has to be finally documented OR where the case may need to be discussed with some external agencies.

[21] Inspiration for this checklist was derived from "Responding to Customer's Security Incidents—Part 2: Executing a Policy" Sun Microsystems, Article Courtesy: Prentice Hall PTR, Ref Section: 7 [6]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The manual may also need to contain the SLA's that may be allocated to the different types of cases that are presented to it, call resolution times for the same, the Liabilities and the legal implications of the same, what steps to take when there are non-disclosure agreements, warranty's, disclaimers etc

Contacts[22]

When responding to an incident, it is important that the case-in-charge be familiar with the list of all contacts that apply to that call. These can include

1. The Client contacts (these may be achieved through a single contact or multiple contacts)
    a. The Technical personnel
    b. The legal personnel to see is any response approaches may affect the constituent legally
    c. Finance and Purchase personnel
    d. Application Personnel to understand the Application
2. The External contacts including
    a. Subject Matter Experts in other IRT's
    b. Experienced professionals
    c. Personnel that have solved similar problems
    d. External Subject Matter experts (with whom he/ she has already worked and established his/ her credibility)
    e. Product vendors of products that may have been affected
    f. Generic Solution providers etc
3. Internal Contacts
    a. To help judge the priority that needs to be assigned to the call
    b. To determine the SLA's and the NDA's that this solution will affect
    c. To determine the Subject Matter Experts within the Organization
    d. To determine the other people that have provided similar solution in the Organization
    e. To determine the people that have tested products and solutions that may be used for this requirement
    f. Others

These are built through e-mail, through phone conversations, through browsed websites, through mailing lists/ forums that the IRT is a part of, through friends, through attending seminars and conferences etc. All these form a database that needs to be maintained and should be accessible to all concerned as incidents don't arrive announced and anyone may need access to this for whatever purpose to solve the problem

[22] This term is taken from "Forming an Incident Response Team, Danny Smith, Australian Computer Emergency Response Team", page 24, Section 7.4 [2]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Proactive and Preventive Approaches[23]

Proactive and preventive approaches are a way that the IRT attempts to communicate with the members of its constituents to ensure that they stay out of danger and that the financial or other impact of the incident is limited or controlled.

1. These include "what to do" databases when affected by vulnerabilities
2. Proactive information relay to enable the members of the constituency to take preventive measures before hand and may be achieved through
    a. leaflets circulated to the constituents
    b. notices on the web
    c. periodic mailer updates
3. Advisories – similar to CERT advisories
4. Presentations to the public and to specific Organizations
5. Panel discussions, Meetings and Conferences
6. Writing in Journals and Magazines that are widely read in the community
7. Making demonstrations of how vulnerabilities affect them to the public/ dedicated Organizations that are under the constituency
8. Provide training and courses

Interaction with the World Outside

Apart from working within the Organization the IRT has to interact with a large number of well known National and International Organization implying the need for co-ordination with any or all of these. These may include the CERT equivalents of the different countries that they work with, the NIST's, Organizations like FEMA, FIRST etc.

Working with these Organizations provides multiple benefits. It allows them to connect and interact to other Organizations within their area, their community and around the world as a whole. This provides them with information on the types of vulnerabilities that are striking the different parts of the world, the effect of the same, the solutions that have been developed to overcome these. They could use the community to ask for solutions to specific problems thus ensuring a faster response to the incident and to the constituent

Basically, this IRT is forewarned and can pass on the same information to its clients, thus reducing the impact on its own constituency. It may also act as the source for further providing solutions to the outside world. It may be a media that this IRT uses to access certain databases of these large Organizations. The same may be used as launch pads to raise issues that

[23] This term is taken from "Forming an Incident Response Team, Danny Smith, Australian Computer Emergency Response Team", page 22, Section 7 and page 27, Section 8 [2]

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

may be used in discussion forums and these may act as further inputs to passing laws and rules, implementing regulations.

Also they may use the tests and outcomes of test scenarios from these large Organizations and use such tests to save on local investment into the same tests. Others may provide test procedures that may be adopted or slightly modified to suit local requirements. Some may provide tools that may be used by the IRT for tests.

The Final Notes

Although a large number of factors are covered here, these only form the tip of the iceberg. There are many more issues that need to be considered, debated on, and provisioned for and to be managed. The factors provided here only enable an Organization to get a start. Moreover, as in every case – the establishment of an IRT is to a large extent dependent on the local laws, its interpretation, feasibility, manageability etc. Local sponsorship and management also make a huge impact on the IRT's survival. All in all, the ultimate aim of any IRT is that it be recognized and gain the respect in its constituency.

References:

1. Handbook for Computer Security Incident Response Teams
   URL: http://csrc.nist.gov/publications/nistpubs/800-3/800-3.pdf

2. Forming an Incident Response Team, Danny Smith, Australian Computer Emergency Response Team
   URL: http://www.auscert.org.au/render.html?it=2252&cid=1938

3. Developing a Security Incident Response Team (SIRT)
   URL
   www.metasecuritygroup.com/library/whitepapers/DevelopingASecurityIncidentResponseTeam.pdf

4. csrc.nist.gov/publications/nistpubs/ 800-12/handbook.pdf

5. http://www.first.org/about/first-description.html and http://www.first.org/about/mission.html and http://www.first.org/about/op_frame/op_frame.20030627.html

6. Responding to Customer's Security Incidents—Part 2:
   URL: http://www.informit.com/isapi/product_id~%7BDD4B8188-79B8-4585-A30D-ACDF0E4BC16D%7D/element_id~%7B1B5B1B51-3497-4E26-89AE-FE05232513D7%7D/st~%7BEEA4B8BA-4464-4E41-BE37-B668A7ACCF61%7D/content/articlex.asp
7. Responding to Customer's Security Incidents—Part 3
   URL: http://www.informit.com/isapi/product_id~{BAA09954-2121-4D90-A469-

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2F460682408C}/session_id~{5ACDC6F5-D9AC-4695-A28B-2F95D5054D96}/content/index.asp

8. Corporate Incident Handling Guidelines
URL http://www.sans.org/rr/papers/index.php?id=645

9. Computer Incident Response Team
URL: http://www.sans.org/rr/papers/index.php?id=641

© SANS Institute 2003, Author retains full rights.