International Infrastructure

for Global Security Incident Response

Moira West-Brown
Klaus-Peter Kossakowski

June 4, 1999

This work was performed at the
CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA
USA

With funding from the U.S.
Department of State

1. Overview – International Infrastructure for Global Security Incident Response

Networked information systems are being rapidly adopted by governments and businesses worldwide to improve communications, control, and competitiveness. Reliance on these systems, especially the Internet as the primary infrastructure, is likely to continue to increase. It is a complex technical and political task for nations and their commercial enterprises to protect information assets and ensure that critical operations continue even if attacked. The growth of world markets and the increase in transnational mergers compound this complexity.

As it stands today, the Internet is vulnerable to attack. The attacks are hard to prevent and respond to, and the perpetrators often go unidentified. The Internet can be abused and misused, to the detriment of all legitimate users and only to the benefit of those with malicious intent. Without steps to make the Internet a safer and more reliable environment, the operation of our critical infrastructures will remain at risk. An international effort is required to improve the general state of information technology (IT) security, because with shared risks comes shared responsibility for protecting information and the technology for its storage and transmission.

Governments are recognizing the need to protect their information and critical infrastructures in response to these threats and are responding in various ways. Some governments recognize that it is not sufficient to address only the local or national aspects of safeguarding information and critical infrastructures. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is significantly reduced. Besides the technological challenges this presents, the legal issues involved in pursuing and prosecuting intruders adds a layer of difficulty as they cross multiple geographical and legal domains. An effective solution can only come in the form of international collaboration.

In the United States, for example, Presidential Decision Directive 63 (a white paper on critical infrastructure protection) states, “Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security. … The Federal Government shall encourage international cooperation to help manage this increasingly global problem.”

In the area of law enforcement, the Internet constitutes a new patrol area in many respects. Unlike jurisdictions based on national and political borders, the digital information infrastructure does not have a central location in the physical world. So not only is responding to attacks difficult technically, but also many of the accepted methods for practicing law enforcement are ineffective. Recent G8 (Group of Eight Advanced Industrial States) and OPEC (Organization of Petroleum Exporting Countries) activities are examples of increasing recognition of this international need.

The need for an international forum to respond to IT security incidents was recognized in the early 1990s and resulted in the formation of the Forum of Incident Response and Security Teams

(FIRST). FIRST consists of 80 incident response and security teams from 19 countries and provides a closed forum for these teams to share experiences, exchange information related to incidents, and to promote preventive activities. Although other teams exist that are not yet FIRST members and new teams are continuously being established, for years to come there will not be enough teams to address the growing need for global incident response. Additionally, FIRST as it exists today is a voluntary organization with no operational element. As such, it provides an introduction service and meeting place for teams to establish trusted interactions, but it is not currently able to provide the necessary coordinated global effort or meet other needs, such as a more open flow of sensitive information and close collaboration to respond to widespread events.

In general, incident response and IT security teams consist of practitioners and technologists who have a wealth of operational experience but lack authority to make policy and security decisions in their organizations. They may also have limited funding and lack professional recognition. This has negative consequences; the team's organization may not have enough staff to respond effectively to security incidents, nor the team have sufficient authority to influence and ensure improved IT security and comprehensive response.

It is inexpensive (the cost of a personal computer and Internet access), quick (less than a minute), and easy (using freely available intruder tools) for anyone to launch attacks against our critical information infrastructures. Conversely, it is expensive (international effort and funding), long-term (research, development, and deployment), and complex (technically and politically) to take the steps needed to harden the information infrastructure to make it less susceptible to attack, and to enable us to respond more effectively and efficiently when attacks do happen.

The problems that we must address to improve our critical information infrastructures require the involvement of diverse parties, including governments, policy and law makers, law enforcement, software vendors, the research community, and practitioners such as FIRST members who have experience responding to incidents. Attempting to address the problems in one group without input and feedback from the others is likely to result in flawed or incomplete solutions. Last year the draft U.S. government legislation (the Digital Millenium Act) resulting from the World Intellectual Property Organization (WIPO) treaty resulted in a flurry of panic in the Internet security community. Practitioners, researchers, software vendors, and incident response teams realized that aspects of their work that address security flaws to reduce risk to our critical infrastructures might become illegal under the proposed legislation. This was clearly not the original intent of the treaty nor the resulting legislation. This is just one example of the urgent need for ongoing communication among policy makers, technologists, and others to ensure that future policies and agreements on a national and international scale are practical and effective.

Information exchange and interaction among many parties is paramount to producing comprehensive and practical approaches and solutions to the complex problems faced. Simply bringing parties together is not enough. We need to consider the issues that must be addressed to support a global incident response effort and to reduce the likelihood, number, and extent of IT security incidents. We believe these are the major needs:

- A reliable information technology infrastructure that can deliver essential services and preserve essential assets during attack and compromise, and recovery of full services and assets following attack
- Systems and applications for users that are more secure and that use authentication, transport, and access control mechanisms
- Protection of government, critical infrastructure, commercial, and personal information

- Improved IT security standards, both in terms of technology standards and international policies and standards
- A reduction in the technical expertise required to implement security. The same features that have made computer usage easy to understand by the user need to be employed in IT security

The vision for an international infrastructure for global IT security incident response consists of four interdependent key elements:

1. An infrastructure to enable and coordinate increasingly effective global incident response efforts to provide a higher level of response capabilities (early warnings, trends, predictive information)

2. A forum to facilitate the discussion and development of international standards, policies, and agreements that support global security incident response

3. A capability to support the improvement of information technology security through the collection, analysis, and dissemination of practical experiences, information, and lessons learned in the global incident response community

4. A professional organization to enhance the recognition and education of incident response and information technology security personnel and teams

This vision can be achieved with international participation, commitment, and cooperation among governments, law enforcement, commercial organizations, and researchers, as well as practitioners such as FIRST members, who have experience responding to incidents.

1. An infrastructure to enable and coordinate global incident response efforts

At this time, there is no infrastructure to support a coordinated global incident response effort, although there are a few components in place that can form the basis of this infrastructure. A variety of issues must be addressed when considering how to promote an effective global incident response infrastructure. These include discussions about which organizations will coordinate and participate in the development effort, how current groups and forums can fit their mission and objectives into an agenda to create a global infrastructure, and what possible structures and mechanisms might be required and effective in the future.

The recent Melissa virus attack underscores the lack of such a global response structure for incident response. Because individual teams focused on their individual or national response needs, there was no operational global response effort. Although FIRST played an essential role in the early identification of the problem and was able to notify others (due to early reports shared among its member teams), it has no operational mission or funding and so was unable to facilitate further response.

2. A forum to facilitate the discussion and development of international standards, policies, and agreements that support global security incident response

A global forum would bring together expert practitioners in the communities of law enforcement, policy making, incident response, and research to develop comprehensive and effective approaches for global incident response. Participants would provide information and

recommendations for international standards, policies, and agreements to ensure a common understanding of the information required for tracking and tracing intruder activities on a global scale and to improve the pursuit and prosecution of intruders.

To progress toward a more secure environment, technical experts need to work with one another and with law enforcement to respond to IT security incidents, and with product vendors and users to address system and network vulnerabilities. They should also collaborate with policy makers charged with developing international policies, agreements, and international standards, providing information that can influence decisions about issues affecting incident handling.

3. A capability to support the improvement of information technology security through the collection, analysis, and dissemination of practical experiences, information, and lessons learned in the global incident response community

Many network protocols that now form part of the information infrastructure were designed without IT security in mind. Without a secure infrastructure, it is difficult to avoid IT security problems and resolve IT security incidents. The combination of rapidly changing technology, rapidly expanding use, and new, often unimagined uses of the information infrastructure creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and even more difficult to predict.

To improve and maintain information technology and network security and to ensure the survivability of the information infrastructure, it is essential to

- Cooperate globally to monitor the state of IT security
- Identify trends in intruder activities and system and network vulnerabilities
- Provide information that enables the public and private sectors worldwide to gauge their IT security risks
- Help these sectors determine their priorities for addressing these risks

The incident response and security teams community has this information and can share it to help address these needs.

During the Melissa incident, FIRST asked its membership about the impact of the virus on their constituency to produce a global view of the activity. Because of the voluntary nature of FIRST and FIRST's lack of funding, it took almost four days from the initial activity report to solicit and receive status reports and generate the global activity summary. However, the resulting summary provided a global perspective of the geographical impact and spread of activity. This example highlights how a global perspective can be obtained, along with the need for better mechanisms and funding to support these efforts.

4. A professional organization to enhance the recognition and education of incident response and information technology security personnel and teams

A professional society for the incident response community is needed to set standards for incident response and security teams and increase their recognition and visibility. The society would promote the need for computer security incident response in the broader community and raise public awareness of the issues.

The current lack of suitably trained staff in this field and a general lack of recognition for IT security incident response teams present a major hurdle to meeting the staffing needs of the global incident response community. Without the ability to attract and retain an adequate supply of qualified staff, it will be difficult for organizations to implement any effective and reliable global incident response infrastructure.

In comparison with many professions, the field of IT security incident response is in its infancy. Although some incident response and security team training materials have been produced, little else has been done to help prepare incident response practitioners to address many difficult issues. Thus, additionally, there should be a role for a professional organization to play in influencing the curriculum used to train incident response practitioners.

Conclusion

Our critical information infrastructures and the government and businesses operations that depend on them are at risk. We share the responsibility to improve Internet security and coordinate effective international global response to IT security incidents and events. To be successful, it is paramount that we ensure participation and cooperation among governments, law enforcement, commercial organizations, the research community, and practitioners who have experience in responding to IT security incidents.

This document offers an initial framework to discuss four key elements of the SEI[1] vision for an international infrastructure for global security incident response. We plan to provide a better understanding of the nature and organizational models needed to support this vision.

Although we identified and discussed the four key elements separately, we do not believe that four separate organizations are needed to fulfill this vision. We will analyze the key elements and determine common areas that could be covered under a single organizational structure. Our initial assessment suggests the following:

- The infrastructure to enable and coordinate global incident response efforts is likely to build on existing national and local operational incident response infrastructures. This could result in cooperative international agreements. The next step for the SEI is to review existing infrastructure components and suggest any infrastructure changes that might be necessary to support an effort to coordinate global incident response. We will consider several models that may be appropriate to address this global need.

- The forum to facilitate the discussion and development of international standards, policies, and agreements that support global security incident response could possibly be an organization that is coupled with the professional organization described in the last bulleted item below. The next step for the SEI is to identify the forum's scope and participants.

- The capability to support the improvement of technology through the collection, analysis, and dissemination of practical experiences, information, and lessons learned in the global incident response community can be enhanced by an interface between the international incident response infrastructure and either the forum and/or the professional organization. The next step for the SEI is to discuss the various types of information that are appropriate to collect

[1] The Software Engineering Institute (SEI) is a federally funded research and development center located at Carnegie Mellon University and sponsored by the U.S. Department of Defense.

and to determine what mechanisms should be in place to gather, analyze, and disseminate the information.

- The professional organization that would be developed could enhance the recognition and education of incident response and security personnel. It is likely to take the form of a funded entity similar to FIRST. The next step for the SEI is to identify the various activities that such a society might undertake.

The broad mission of the international FIRST organization encompasses many of the issues identified in our vision. Although FIRST has been effective at supporting incident response activities that cross organizational and national boundaries, it currently lacks the structure, formality, funding, and operational mission to support either a coordinated global effort or other needs like a more open flow of sensitive information and close collaboration during widespread IT security events. The FIRST organization could potentially fulfill some of the components in this vision.

We will look at existing organizations, such as FIRST, to identify which key elements of the vision are currently supported and, if not, how the organization(s) could evolve to better meet the proposed vision. Finally, the SEI will work closely with members of FIRST to better determine whether FIRST could migrate from its existing structure toward an organization better able to fulfill some or all of the key elements of this global vision. As our work progresses in addressing the issues raised in this overview, we will change this document to reflect the lessons learned.

2. Introduction

Networked information systems are being rapidly adopted by governments and businesses worldwide to improve communications, control, and competitiveness. Reliance on these systems, especially the Internet as the primary infrastructure, is likely to continue to increase. It is a complex political and technical task for nations and their commercial enterprises to protect information assets and ensure that critical operations continue even if attacked. The growth of world markets and the increase in transnational mergers compound this complexity.

Information exchange and interaction among many parties is paramount to producing comprehensive and practical approaches and solutions to the complex problems we all face. These problems require the involvement of such diverse parties as governments, policy and law makers, law enforcement, software vendors, the research community, and practitioners such as members of the Forum of Incident Response and Security Teams (FIRST), who have experience responding to incidents. But simply bringing parties together is not enough. We need to consider the issues that must be addressed to support a global incident response effort and to reduce the likelihood, number, and extent of IT security incidents. We believe these are the major needs:

- A reliable information technology infrastructure that can deliver essential services and preserve essential assets during attack and compromise, and recovery of full services and assets following attack
- Systems and applications for users that are more secure and that use authentication, transport, and access control mechanisms
- Protection of government, critical infrastructure, commercial, and personal information
- Improved IT security standards, both in terms of technology standards and international policies and standards
- A reduction in the technical expertise required to implement security. The same features that have made computer usage easy to understand by the user need to be employed in IT security

The vision for an international infrastructure for global IT security incident response consists of four interdependent key elements:

1. An infrastructure to enable and coordinate increasingly effective global incident response efforts to provide a higher level of response capabilities (early warnings, trends, predictive information)

2. A forum to facilitate the discussion and development of international standards, policies, and agreements that support global security incident response

3. A capability to support the improvement of information technology security through the collection, analysis, and dissemination of practical experiences, information, and lessons learned in the global incident response community

4. A professional organization to enhance the recognition and education of incident response and information technology security personnel and teams

Although we list these elements separately, we do not believe that four separate organizations are needed to provide the international infrastructure. In this chapter we analyze the key elements in detail and discuss the organizational issues associated with them. The chapter is in draft form, as a starting point for discussion. We will revise and refine the material after receiving feedback from stakeholders.

We begin the chapter by introducing (in Sec. 2.1) the broad range of stakeholders and other parties who are involved in or affected by IT security incidents. After providing this context, we analyze (in Sec. 2.2) the key elements of the infrastructure for global incident response, including the missions, those involved in fulfilling the missions, and those who benefit from it. We identify interrelationships between the key elements, determine common areas that could be handled by a single organizational structure, and, finally, identify the need for two entities to fulfill the missions (an entity is not necessarily a single organization).

In Sec. 2.3, we go on to identify, for each entity, the scope of the tasks to be undertaken, the associated requirements issues for performing those tasks; and existing organizations that meet aspects of the task needs. In Sec. 2.4, we present, for discussion, some thoughts about models to support the identified tasks and requirements issues for each of the two entities. We conclude the chapter with some preliminary conclusions (Sec. 2.5) and next steps (Sec. 2.6).

2.1 Stakeholders

This section provides context for discussing an international incident response infrastructure by considering the broad range of parties involved with or affected by incident response and related issues. In the table below, we list (in no particular order) the key stakeholders and other parties who play a role in incident response, have a vested interest in it, have an impact on it, or are affected by response activities and the issues surrounding IT security threats, incidents, and vulnerabilities. We briefly summarize each party's general interest or impact on incident response, describing the roles in which they have the greatest impact. Depending on whether we consider the local, national, or global perspective, a given party may play different roles. It is also possible for a stakeholder to fall into several categories; for example, in addition to responding to incidents within its constituency, an incident response security team (IRST) can also be a victim of an attack.

There are undoubtedly more stakeholders than we can possibly cover here, but we have included those that we believe to be the most numerous or the most critical to the success of an international infrastructure for global security incident response.

This table will be useful later, when we describe the missions, requirements issues, and tasks for each of the key elements and discuss the parties that need to be involved in or how they are affected by the various activities.

STAKEHOLDER	ROLE/IMPACT
Intruders	Perpetrate IT security incidents or activities that result in IT security incidents.
Users/constituents/sites involved in incidents	Directly affected by the incident–their systems may be involved, for example, as a source, target, or intermediary of an attack. This category includes technical staff, such as system and network administrators of the systems and networks, and local contacts, such as site security contacts. The systems and networks involved provide the data that must be analyzed to determine the nature and scope of the activity.
IT security departments and security consultants	Charged with implementing mitigation strategies or addressing other security issues and policies, resolving incidents, and analyzing attacks and recognized activities
Management	Provide leadership and direction for the approach a site takes to prevent or respond to IT security incidents.
Legal counsel	Provide guidance on an organization's legal standing in preparation for and response to IT security incidents.
Local and organizational incident response and security teams	Receive incident reports from their constituents, most commonly through intrusion detection software, other teams, or other parties. Coordinate response with sites internal and external to their constituency and other parties involved. The missions of individual teams vary, but most often teams are charged with determining the scope and nature of the activity and providing technical support in the form of mitigation and recover strategies. Examples include BCERT, Boeing's response team, and NU-CERT, Northwestern University's response team.
Coordinating incident response teams	May undertake many of the same tasks as the teams in the previous item, but their constituencies include other IRSTs, for whom they play a coordination role. They typically take the form of national teams or teams that serve specialized communities. Examples include the CERT® Coordination Center, DK-CERT (the Danish response team), and ACERT/CC (the US Army coordination center).
National critical infrastructure protection groups	Charged with protecting national critical infrastructures from IT security threats and attacks. Organizations cooperating in this effort include national law enforcement, government agencies, and the private sector that cooperate to protect national critical infrastructures from IT security threats and attacks. Examples are the US National Infrastructure Protection Center (NIPC) and the Telecommunications National Security Telecommunications Advisory Committee (NSTAC).
The military	In many countries, the military relies on the Internet for some of their operation, support, and communications activities. Many use the same technology for their internal infrastructures. Information warfare is a major topic in this community as network infrastructures provide an additional virtual battlefield that is vulnerable to attack.

Cooperative security groups	Cooperate at some level in an effort to provide effective response to IT security incident and events. Participants are collections of security teams and other parties, including cooperative groups in the anti-virus, security scanner, and incident response communities. Examples include FIRST and the European Institute for Computer Anti-Virus Research (EICAR).
Providers of network services or content or other services	Can be involved at many levels including identifying the source of network traffic associated with an incident or assisting in blocking or diverting network traffic in response to an incident.
Law enforcement	Determine if a crime has been committed and, if so, gather evidence relating to the crime and attempt to identify and prosecute the perpetrator(s). This may include cooperation on a local, national, or international level. For example, Interpol's Computer Crime Committee facilitates information exchange and coordination among national computer crime squads.
Technology vendors	Identify the underlying security weakness(es) and develop mitigating strategies in the form of patches or workarounds to address security problem(s) in the technology they produce. Most commonly called upon when an incident involves a new attack type or variant of an existing attack type. Technology vendors have the ability to improve the security of technology if there is a business need and they have information on the appropriate standards to implement. Examples include Sun Microsystems and Cisco Systems.
Security product vendors	Have a vested interest in keeping their products up to date to protect against, counteract, or mitigate known threats and vulnerabilities. This group includes developers and vendors of anti-virus, software and e-commerce, firewall, and encryption products. Examples include Network Associates Inc. (NAI) and Internet Security Systems (ISS).
Security experts	Assist any of the other parties involved in response to incidents. They are called in if particular technical expertise is required. They should not be confused with consultants. These experts are very few in number and provide the authoritative voice on specific areas of technical expertise. This group can be advocates for best security practices.
Media relations department	Work with reporters from the media during an incident (if it draws media attention). In anticipation of media inquiries, sites, IRSTs, and others involved in an incident often alert their media relations departments so they can be prepared to appropriately handle the media.
Media	Report on IT security incidents and issues. IT security incidents are a hot topic for the media, particularly incidents that have a wide scale impact or that involve high profile sites. The information reported by the media can have a direct (positive or negative) impact on other parties' abilities to effectively respond to incidents.
Funding bodies, sponsors	Provide funding for organizations involved in limiting the impact of or responding to IT security incidents. The amount of funding available has a direct impact on their ability to work effectively. It is important that funding bodies and sponsors are kept apprised of IT security issues and the associated cost/benefit tradeoffs.

Governments, policy/law makers	Provide the legal framework to facilitate and encourage appropriate use of technology to support commercial, educational, and national information flow, and make provision for legal recourse for inappropriate activities. This group includes government information security agencies such as those that certify products (Orange Book, IT-SEC) or provide certification and other security infrastructure services.
Insurance companies	Directly involved in IT security incidents if recovering the resulting losses. Are also interested from a risk assessment perspective; with access to data on the cost and impact of security incidents, they can improve their actuary data and set appropriate coverage levels and costs.
Internet community at large	Have a stake in the overall state of IT security. People want to be confident that their personal or sensitive information is not at risk and that they can rely on the integrity of services provided to them. Although given sites may not be directly involved in a given incident, they may be using the same vulnerable technology that is being exploited in that incident. So the Internet community in general wants to know how to protect itself from known forms of incident activity.
Society at large	As more and more systems critical to the society's survival are now interconnected or accessible via telecommunication or data networks every member of a society have a stake in the overall state of IT security, even if they are not directly using IT.
International organizations dealing with information security	In response to a growing need for international action and coordination, more and more international organizations will get involved in IT security issues. A current example is the Security of Telecommunications and Information Systems Branch of Directorate-General XIII (Telecommunications, Information Market and Exploitation of Research) of the European Commission. (This agency has supported research activities but has not yet mounted any specific activities of its own.)
The education and research communities	Seek guidance on the range and scope of IT security issues to address in curricula– from software engineering practices (how to build secure systems) to network design (how to specify secure architectures) and input on research in new IT security areas such as has occurred with firewalls and intrusion detection.
International standard-setting bodies	Involved in establishing international standards for telecommunications and information networks that have implications for IT security. These include International Organization for Standardization (ISO) and the Internet Engineering Task Force (IETF).
Private sector security-related organizations	Provide IT security expertise. There is a variety of organizations, including commercial and fee-for-service organizations. In addition, there are professional associations devoted to information systems security, and industry associations whose efforts are focussed, in part, on IT as it pertains to their industry. Examples are SRI Consulting's International Information Integrity Institute (I-4) and the ESF (European Security Forum).

2.2 Missions

In our vision of an international infrastructure for global IT security incident response, there are four key elements.

1. **An infrastructure** to enable and coordinate increasingly effective global incident response efforts to provide a higher level of response capabilities (early warnings, trends, predictive information)
2. **A forum** to facilitate the discussion and development of international standards, policies, and agreements that support global security incident response
3. **A capability** to support the improvement of information technology security through the collection, analysis, and dissemination of practical experiences, information, and lessons learned in the global incident response community
4. **A professional organization** to enhance the recognition and education of incident response and information technology security personnel and teams

In this section, we review each key element, discuss the issue that it addresses, and define its mission. Next, we identify who is involved in fulfilling the mission and single out those best served by it. Finally, we consider potential interrelations among elements.

The mission statements reflect the high-level goals, objectives, and priorities for achieving our vision of a global incident response infrastructure. Each statement provides a focus for considering the overall goals and objectives in setting up this infrastructure.

In identifying the major parties involved in fulfilling each mission and the constituencies that will reap the most benefit, we do not go into detail. Instead, we refer readers to the list of stakeholders in Section 2.1.

The following discussion of key elements and the missions associated with them is in preliminary form; it will be refined after we receive feedback on the appropriateness of the missions themselves and input on the major stakeholders.

2.2.1 **Element 1 - An infrastructure** to enable and coordinate increasingly effective global incident response efforts to provide a higher level of response capabilities (early warnings, trends, predictive information)

There is an urgent and ongoing need to provide a global infrastructure to provide a fast, effective, and comprehensive response to computer security incidents on a local, national, and international scale. At this time, there is no infrastructure to support a coordinated global incident response effort. As a result, a number of problems arise within the Internet community.

> **Responding quickly and effectively.** Response to the recent Melissa virus attack demonstrates current limitations. Because individual teams focused on their individual or national response needs, there was no operational global response effort. Although FIRST played an essential role in the early identification of the problem and was able to notify others (because member teams shared early reports), it has no operational mission

or funding and so was unable to facilitate further response. The lack of global coordination during the Melissa attack only reemphasizes our need for a global response structure for incident response.

Contacting others during an incident. Although teams generally document the contact information for all organizations that they work with during an incident, many do not routinely maintain a current list of contacts. As a result, individual teams do not tend to keep reliable, complete contact information for other teams in the IRST community. It is imperative that teams do not scramble to find appropriate contact information in an emergency situation. This information needs to be known in advance and be readily available.

It is not only important to know whom to call, but it is also important to know what information must be exchanged to most effectively facilitate response and to ensure that the information is exchanged securely.

Establishing policies and procedures. The pioneer IRSTs, formed in the late 1980s, were faced with defining their own appropriate operational guidelines with little or no experience on which to draw from. It has taken years for these now-established teams to develop comprehensive policies and procedures for their internal operations. Today, newly forming teams are not much better off than the early pioneers were, as little documented guidance is available.

Moreover, the IRST community as a whole is still sorely lacking in the area of policies and procedures to support operations among teams. The progress being made in this area is limited and slow. It is mostly limited to a few isolated groups of IRSTs who work together regularly and have a business need to reach agreement. Progress typically comes to a halt when teams become overwhelmed by the number of issues that need to be addressed before they can reach agreement–such as no common agreement on terminology, definitions, and priorities.

Forming cooperative relationships among teams. Currently, many teams agree to cooperate based on trust alone; they have no supporting contractual agreements to provide the foundation for their interactions. In fact, it is even more complex than that, as in some cases trust has been developed between individuals from given teams. So when trusted individuals leave those teams, the trust relationship may go with them. This can potentially result in the isolation of teams that were once part of a cooperative IRST community. Additionally, the information communicated between two teams during an incident is not well defined. The extent of the information might depend on who is involved, their experience with the other team involved, and the specific staff members who are interacting.

Gaining entry to the IRST community today can be a difficult and lengthy process. The community is ready to embrace new members, but it is wary of interacting with new IRSTs unless an existing member of the trusted community can vouch for them. So some new teams are in a “Catch-22” situation, wanting to contribute, but needing to gain acceptance and mentoring from an existing member of the community before they can begin to gain broader acceptance. As most teams have no charter or funding to act as mentors to new members of the community, finding a mentor and introducer is not as easy a task as it sounds.

Moreover, because there is no formal mentoring process for new members of the community, the guidance given to new teams can vary widely depending on the experiences and time available from their mentoring team. As a result, the IRST community expands at a much slower rate than is needed, and the teams operate with a widely varying set of operations and standards. The community needs to ensure and adopt a sponsorship process that doesn't depend on the good will of individual teams and ensures that each team meets an agreed-upon minimum level of operational standards.

Today's approach is not reliable, does not scale, and it must be made more effective. It is critical to have a global response infrastructure to replace a less reliable system based on trust between individuals with a reliable and effective system based on global understanding/agreement.

Providing security information to constituents. Local response efforts dedicated to individual communities (based on geographical location, organizational entity, service provided, or other criteria) are imperative to ensure that we all obtain response services that are appropriate for our needs. Each community has its own specific needs to address including: technology base, language, time zone, jurisdiction (organizational, local, national, and international). However, the need for local response efforts does not eliminate the need for communication on a broader scale. Intruders are international in their movements and activities and so we must pool our response activities to ensure that we can respond appropriately.

For example, only a small percentage of the current IRST community researches and generates original source material for security advisories and alerts that advise the community on preventing and recovering from ongoing intruder threats. Currently, the members of the IRST community as a whole are adept at tailoring this source material to best suit the needs of its constituents and redistributing the modified material through local distribution channels. The community is continuing to improve the quality of and the speed at which information in these alerts is provided. Communication channels need to continue to broaden to reach additional stakeholders. A global incident response infrastructure would continue to provide support for and enhance these rapid alert mechanisms.

Governments are finally recognizing the need to protect their information and critical infrastructures in response to security threats and are responding in various ways. Some governments recognize that it is not sufficient to address only the local or national aspects of safeguarding information and critical infrastructures. We suggest that the path to addressing these threats lies in providing an effective and comprehensive global response to IT security response on a local, national and international scale.

A global incident response infrastructure would be the most effective way to facilitate response and to ensure that information is exchanged securely. This approach helps to ensure that response is effective, reliable, and timely.

We propose the following mission statement for the first key element:

2.2.1.1 Mission 1

Provide effective and comprehensive global response to IT security response on a local, national and international scale by

Providing an infrastructure to enable and coordinate global incident response efforts;

Coordinating activities of IRSTs throughout the world; and

Supporting the formation, operation and integration of IRSTs into the global incident response infrastructure.

2.2.1.2 Stakeholders

This mission directly addresses the goals and calls for the involvement of these stakeholders:
- Local and organizational IRSTs
- Coordinating IRSTs
- National critical infrastructure protection groups
- Technology vendors
- Security product vendors

In addition, the following stakeholders are most likely to be dependent on the infrastructure and/or directly affected by its "work":
- Intruders
- Users/constituents/sites involved in incidents
- Management
- Legal counsel
- Providers of network services, content, or other services
- Law enforcement
- IT security departments and security consultants
- Cooperative security groups

To some degree, all the stakeholders described in Section 2.1 have a vested interest in the infrastructure's existence, particularly through their reliance on the alerts and advisories issued in response to ongoing threats.

Other stakeholders who will either directly benefit from or be parties to the infrastructure's mission include
- Security experts
- The military
- Funding bodies, sponsors
- Governments, policy/law makers
- Private sector security-related organizations
- Media
- Society at large

2.2.1.3 Interrelationships

Among the stakeholders in a global infrastructure, the focus of many will be the lessons learned from the mid-term (3-12 months) and longer-term (greater than 12-months) analysis of data collected by the infrastructure. The mid-term focus is covered by key element 3 (a capability) and the longer term analysis is likely to be addressed by the education and research communities as a result of the activities of key element 4 (a professional organization).

A variety of issues must be discussed when considering how to promote an effective global incident response infrastructure: which organizations will coordinate and participate in the development effort, how current groups and forums can fit their mission and objectives into an agenda to create a global infrastructure, and what possible structures and mechanisms might be required and effective in the future.

Based on the past experiences within the IRST community (which we'll describe in more detail in Section 2.4 Organizational Models), we know that it is not possible to build this global infrastructure as a single organization. Instead of a monolithic approach, global incident response efforts are best based on the global coordination of response activities ranging in scale. These response activities should be carried out by infrastructure components with a very few hierarchical levels to support effective communication and allow for the suitable level of coordination. The number of infrastructure components operating on an international level should be very small (a maximum of one per nation), with more components on a national level and other interested organizations represented at the base level. The overall coordination will likely be handled by a limited number of international coordination centers.

2.2.2 **Element 2 - A forum** to facilitate the discussion and development of international standards, policies, and agreements that support global security incident response

A global forum would bring together expert practitioners in the communities of law enforcement, policy making, incident response, and research to develop comprehensive and effective approaches for global incident response. Participants would provide information and recommendations for international standards, policies, and agreements to ensure a common understanding of the information required for tracking and tracing intruder activities on a global scale and to improve the pursuit and prosecution of intruders.

Attempting to address the problems in one group without input and feedback from the others is likely to result in flawed or incomplete solutions. For example, last year the draft U.S. government legislation (the Digital Millenium Act) resulting from the World Intellectual Property Organization (WIPO) treaty resulted in a flurry of panic in the Internet security community. Practitioners, researchers, software vendors, and incident response teams realized that aspects of their work that address security flaws to reduce risk to our critical infrastructures might become illegal under the proposed legislation. This was clearly not the original intent of the treaty nor the resulting legislation. This problem is not limited to the U.S. In Australia, similarly flawed legislation is underway and the IT security community is rallying attempts to address it. This type of legislation is just one example of the urgent need for ongoing communication among policy makers, technologists, and others to ensure that future policies and agreements on a national and international scale are practical and effective.

Among the problems to be addressed are the following:

Facilitating interaction and understanding. To progress toward a more secure environment, technical experts need to work with one another and with law enforcement to respond to IT security incidents, and with product vendors and users to address system and network vulnerabilities. They should also collaborate with policy makers charged with developing international policies, agreements, and international standards, providing information that can influence decisions about issues affecting incident handling.

Although the cooperation between various communities involved in incident response has certainly improved since the Internet worm event in 1988, contact needs to improve still more in order to facilitate an effective response to Internet security threats. As these communities have grown and evolved over time, a smaller percentage of individuals remain in each community who fully understand the needs, constraints, and requirements of any of the other communities. In some cases, the communities do interact, but this interaction is limited and is insufficient to address the growing need. Attempting to address the problems in one group without input and feedback from the others is likely to result in flawed legislation or incomplete solutions that don't achieve their intended effects. Along with creating difficulties in creating legislation, faulty communication can also lead to unreasonable expectations from law enforcers. More broadly, the current tendency toward a more isolated system limits the exchange of ideas among communities.

There are many system administrators who believe that law enforcement should investigate every IT security incident. Reality and available resources soon make it clear that such expectations are not reasonable. Law enforcement agents who are new to the IT security arena often attempt to apply traditional investigative methods to IT security incidents. This can result in frustration on all sides as the technologists and practitioners involved attempt to explain the technology issues that make this arena unique.

Today, little discussion takes place between a very small cross-section of the stakeholders. The discussion that does take place is mostly limited to IRSTs, some product vendors, practitioners and some law enforcement representatives. This results in limited exchange of ideas amongst the communities. This lack of cross-community communication is a major factor contributing to the lack of progress resulting from no common lobby voicing IT security and response issues. Unless information flow is increased across the stakeholder community, we will continue to fail to understand each other's roles and will be unable to attain the overall vision.

Suggested approaches to addressing the problems we all face need to take into consideration the constraints and concerns of all the communities involved. This will help foster understanding and set reasonable expectations. From such interactions come better relationships and a more effective response. It is important to foster a common understanding that we all have a common goal – improving security benefits us all. Helping these communities to focus on the common goal will help to facilitate progress towards it.

Establishing standards. The IRST and law enforcement communities have been struggling with the issues of standards relating to IT security issues for many years with little or no progress. If you ask members of both communities the question "what is an incident?" or "what types of incidents constitute a crime?" the responses you receive will

vary widely and will lack consistency. The lack of progress stems from two main problem areas – lack of available resources and striving for consensus. The resources needed to address the immediate needs of their constituencies leave both communities with little or no time and commitments to address some of the larger community-wide challenges – such as standards issues. We need standards agreement to enable us to make sense of the data we have and to give us a common understanding of the issues.

Although the overall investment needed from the community in the standards area is still significant, the size of the community has grown and continues to grow. If the effort to set standards is shared within the community and with other stakeholders, it will minimize the resources required from any individual organization. When groups have come together to attempt to address such challenges, the scope of the problem that they have attempted to address at any one time has been too broad. But, moreover, the community has striven to reach consensus and agreement to address international level issues before attempting to address issues at a local or national level. Such issues can be addressed by developing suggestions and forming recommendations at a local level and then seeking national adoption before attempting to reach international consensus. However, decentralized and distributed bottom-up approaches in the IT arena have resulted in standards battles (e.g. ISO/OSI vs. TCP/IP or PGP vs. PEM). There, is a need for both approaches to be applied, bottom up and top down. So, while growing bottom up there should be discussion and consensus to limit the number of options.

The proposed mission statement for the second key element is the following:

2.2.2.1 Mission 2

Provide an open forum for law enforcement, policy makers, technology developers, IRSTs and practitioners to improve IT security and global incident response on a local, national and international scale by

Fostering the exchange of information and innovations;

Improving policies and practice by identifying and addressing IT security and global incident response issues; and

Promoting IT security and global incident response issues for the benefit of humanity.

2.2.2.2 Stakeholders

Because this mission calls for an open forum, there are many stakeholders that need to be active within the forum to make it effective and successful:

- Local and organizational IRSTs
- Coordinating IRSTs
- National critical infrastructure protection groups
- The military
- Cooperative security groups
- Providers of network services, content, or other services
- Law enforcement

- Technology vendors
- Security product vendors
- Security experts
- Funding bodies, sponsors
- Governments, policy/law makers
- Insurance companies
- International organizations dealing with information security
- Education and research communities
- International standard-setting bodies
- Private sector security-related organizations

Aside from the intruder community, every other stakeholder benefits from the fulfillment of this mission.

2.2.2.3 Interrelationships

Because of the need for a global discussion and representation within this forum, only one forum is needed. Other existing organizations whose missions may intersect to some extent with this forum will be strong liaisons, but we believe that no other organization will emphasize the global incident response effort as strongly as this forum. Local (national) discussion of local (national) issues, special interest groups/chapters would have representation within the global forum. Since local participation is essential for the success of this mission, their contributions en masse would create and shape the direction of this forum.

Given the overall goal - to improve global incident response - this forum must form a strong alliance with key element 4 (a professional organization). The success and impact of the forum will also depend on the information it obtains from the global incident response infrastructure. This information flow will come via key element 3 (a capability).

2.2.3 Element 3 - A capability to support the improvement of information technology security through the collection, analysis, and dissemination of practical experiences, information, and lessons learned in the global incident response community

To improve and maintain information technology and network security and to ensure the survivability of the information infrastructure, it is essential to

- Cooperate globally to monitor the state of IT security
- Identify trends in intruder activities and in system and network vulnerabilities
- Provide information that enables the public and private sectors worldwide to gauge their IT security risks
- Help these sectors determine their priorities for addressing these risks

The IRST community has access to data that can provide much of the information and can share it to help address these needs. The Melissa incident provides a good example again. FIRST asked its membership about the impact of the virus on their constituency to produce a global view of the activity. Because of the voluntary nature of FIRST and its lack of funding, it took almost four days from the initial activity report to solicit and receive status reports and generate the global

activity summary. Even so, the resulting summary provided a global perspective of the geographical impact and spread of activity. This example highlights how a global perspective can be obtained, along with the need for better mechanisms and funding to support these efforts.

These are some problems associated with collecting, analyzing, and disseminating practical experiences, information, and lessons learned in the global incident response community:

Dealing with the growth and evolution of an inherently insecure infrastructure. changes. Many network protocols that now form part of the information infrastructure were designed without IT security in mind. Without a secure infrastructure, it is difficult to avoid IT security problems and resolve IT security incidents. The combination of rapidly changing technology, rapidly expanding use, and new, often unimagined uses of the information infrastructure creates a volatile situation in which the nature of threats and vulnerabilities is difficult to assess and even more difficult to predict.

Meeting needs of the broad community. IRSTs generally focus on providing information to meet their constituent's needs rather than the needs of the broader community. The information that they are most likely to generate includes statistics and scenarios to help fulfil their own needs (for their constituency, to get funding or for internal operational needs). Additionally, experience has shown that when operational and information dissemination needs in this field compete for resource, the overriding need to meet operational demands wins.

Sharing useful information. In the course of their work, many stakeholders have access to information that would benefit others. For instance, a typical system administrator or IT security manager may be able to calculate the cost of recovering from an IT security incident at an individual site. However, when communicating with an IRST, this person often discusses only the technical issues relating to the incident and not the financial ones. So the financial impact at a given site and the overall financial impact of a large-scale event across multiple sites is not captured. Many of the stakeholders would greatly benefit from the availability of such data. Information available in the IRST community identifies that many currently used IT practices and deployed applications in the broader community are insecure. However, much of this information has not been disseminated.

Correlating information. Anyone attempting to gather the limited information available in this area will soon find that due to the lack of standards outlined in the discussion of the earlier key elements, it is often hard or impossible to correlate the information provided from different sources. Moreover, much of the information never makes its way outside the organization boundaries of the teams due to privacy reasons and the fact that few teams structure their data in a way that readily supports access to it in a sanitized form.

Ensuring timeliness. When researchers have finally gained access to the data and analyzed it, the delay of several years between the timestamp of the data and the distribution of the resulting analysis makes the results of limited use because technology innovations are moving so rapidly. We need timely access to data so we can make the most effective improvements in this arena on the appropriate time scale. In fact, because data is so lacking in certain areas, our perceived understanding of the real problem and appropriate solution(s) may be off the mark. Aggregation of available data might show a different picture of the arena than is expressed today by experts.

2.2.3.1 Mission 3

Provide accurate and timely information covering all aspects of IT security and global incident response activities which are of interest on a local, national and international scale by

Acting as a clearing house and distribution center for sanitized information from the global incident response infrastructure and

Providing a global perspective of the state of the threat by collecting and analyzing available incident related data from all available sources.

2.2.3.2 Stakeholders

The information resulting from this mission would be useful to every stakeholder, although in varying degrees:

- Intruder
- Users/constituents/sites involved in incidents
- Management
- Legal counsel
- Local and organizational IRSTs
- Coordinating IRSTs
- National critical infrastructure protection groups
- The military
- Cooperative security groups
- Providers of network services, content, or other services
- Law enforcement
- Technology vendors
- Security product vendors
- Security experts
- Media relations
- Media
- Funding bodies, sponsors
- Governments, policy/law makers
- Insurance companies
- Internet community at large
- Society at large
- International organizations dealing with information security
- Education and research communities
- International standard-setting bodies
- Private sector security-related organizations

To fulfill mission 3, working relationships are important both to meet the goals and to improve the kind of work involved. In addition, cooperation with stakeholders might be necessary to resolve open questions that need to be solved in order to provide information. Examples include

- Global incident response infrastructure components
- Local and organizational IRSTs

- Coordinating IRSTs
- National critical infrastructure protection groups
- Technology vendors
- Security product vendors
- Law enforcement
- Governments, policy/law makers
- Education and research communities

2.2.3.3 Interrelationships

The first key element (an infrastructure) will handle information dissemination of immediate and very short-term impact such as advisories and other alerts and immediate issues. These activities are part of the immediate charter of most IRSTs that exist today. But to ensure improvement, we all have a vested interest in taking the lessons learned today and ensuring that we do not make the same mistakes again in the future. The rapid software development cycle that industry is faced with today requires input and lessons to be available in within a 3-6 month time span, and there is general community interest in annual developments.

Any resulting data analysis available after a year or more is possible under this mission, but is not the main goal. Such longer term work will result in other efforts supported by key element 4 (a professional organization) such as via the research and education communities.

The third key element (a capability) will focus on analysis and data manipulation for the use and benefit of many audiences. Many portions of the infrastructure will have generated collated and sanitized information for their own needs. However, not only is a truly global picture needed, but it is also important to be able to characterize activity or data from specific organizational types and also compare and contrast the situation from different perspectives. One major audience with a critical need for the data will be the second key element (a forum). It therefore makes sense to position this key element as a collaborative effort between the infrastructure entities and the forum organization.

2.2.4 Element 4 – A professional organization to enhance the recognition and education of incident response and information technology security personnel and teams

A professional society for the IRST community is needed to set standards for incident response and security teams and increase their recognition and visibility. The society would raise awareness of the need for computer security incident response in the broader community and about the issues involved.

In general, IRSTs consist of practitioners and technologists who have a wealth of operational experience but lack authority to make policy and security decisions in their organizations. They may also have limited funding and lack professional recognition. This has negative consequences; the team's organization may not have enough staff to respond effectively to security incidents, nor may the team have sufficient authority to influence and ensure improved IT security and comprehensive response.

Without an organization to enhance the recognition and guide the education of IR and IT security personnel and teams, these issues are significant:

Meeting IRST staffing needs. The current lack of suitably trained staff in this field and a general lack of recognition for IRSTs present a major obstacle to meeting the staffing needs of the global incident response community. Without the ability to attract and retain an adequate supply of qualified staff, it will be difficult for organizations to implement any effective and reliable global incident response infrastructure.

Training IRST professionals. In comparison with many professions, the field of IT security incident response is in its infancy. Although some incident response and security team training materials have been produced, little else has been done to help prepare incident response practitioners to address many difficult issues. Most incident response staff members learn their trade through on the job experience. This approach is fraught with problems as some teams have little or no resources to apply to appropriate training and new staff members are often left to teach themselves – often by repeating mistakes and learning lessons that are already known by others. This results in inconsistent levels of service being provided and new threats and exploits may be initially overlooked. Thus, additionally, there should be a role for a professional organization to play in influencing the curriculum used to train incident response practitioners.

Defining a minimum set of standards. There are differing opinions in the IRST community on the right set of steps to take in response to an incident and what does and does not constitute appropriate actions on behalf of an IRST staff member. For example, is it all right to probe systems that are thought to be the source of intruder activities? In the past, some teams have considered it appropriate to access (without gaining prior permission) systems that have been compromised and are being used by intruders to store exploit scripts. Others do not.

It is important that a minimum set of professional standards are set for IRST staff. This will help improve the recognition of and respect for this profession and will help to improve the overall effectiveness of work in this field.

2.2.4.1 Mission 4

To promote and support the field and practice of incident response activities on a local, national and international scale by

Promoting and enhancing the image and status of the IRST community;

Setting and upholding standards for the IRST profession and community; and

Supporting the development and improvement of the global incident response infrastructure.

2.2.4.2 Stakeholders

All people who work in the field of incident response and/or who are part of a component of the global incident response infrastructure are affected by mission 4, as are all who are closely affiliated with the work. These include

- Local and organizational IRSTs
- Coordinating IRSTs
- National critical infrastructure protection groups
- Law enforcement
- Technology vendors
- Security product vendors

In addition, the following stakeholders might be interested in becoming part of the professional organization because of their area of expertise or interest:

- Cooperative security groups
- Providers of network services, content, or other services
- Security experts
- International organizations dealing with information security
- Education and research communities
- Private sector security-related organizations

Finally, partnerships and collaboration on specific issues of mutual interest can be expected to be attractive for various other stakeholders and the professional organization:

- Insurance companies
- International organizations dealing with information security
- International standard-setting bodies
- Private sector security-related organizations

2.2.4.3 Interrelationships

Like the second key element (a forum), because of the need for a global representation within this professional organization and the need for global standards and guidelines, only one such body is really needed. Other organizations might have similar missions that make them potential liaisons (for example, ISOC/IETF or IEEE, which set standards related to security of technology). However, we believe that no other body can emphasize the global incident response effort as strongly as this organization, that no other would be so closely be affiliated to the global incident response infrastructure, and that acceptance of standards and guidelines can be easily achieved. Nor is any existing body representing IRST staff as a profession; rather, working in the IRST field is not recognized as a profession at all. To facilitate local (national) discussion of local (national) issues, special interest group or chapters might be good approaches. If these bodies will exist, it is understood that they themselves should participate within the global body.

2.2.5 Conclusion

Having considered the missions associated with the four key elements and their interrelationships, it is clear that no single entity or organization can encompass all four missions. There is, however, a clear distinction between key element 1 (an infrastructure) and the others. Key element 1 stands apart because it requires operational activities and access to sensitive information and it relies on trusted interactions among multiple entities involved in incident response activities on a local, national, and international scale.

As previously described, the third key element (a capability) is directly dependant on the first as a source of information, but its outputs support the activities of the two remaining key elements (a forum and a professional organization). As a result, the third key element could stand alone, or be

combined with any of the other key elements. Experience has shown that when operational and information dissemination needs in this field compete for resource, the overriding need to meet operational demands wins. If the third key element is to be successful, it needs to be separated from the operational global infrastructure, yet seeking funding for the third key element as a stand-alone entity would be difficult. Although many are prepared to pay for resulting reports in a form useful to them, it is much harder to obtain individual funding for the sanitizing data or in-depth analysis. As a result, the third key element is best positioned from both an operational and funding perspective when directly coupled with one of the remaining two key elements.

The missions of the remaining two elements (forum and professional organization) are closely related but separate. If these missions were undertaken by separate organizational entities, there could be duplication of some effort and competition for funding and support. So we suggest grouping the key elements 2, 3, and 4 under a single organizational umbrella to ensure that the success and progress of these missions flourish while minimizing duplication of effort.

Throughout the remaining discussion in this chapter, we will concentrate on two different roles while researching tasks, requirements issues, existing resources, and possible models to implement these roles:

With this understanding, we can explore the tasks associated to fulfill the missions for each key element in more detail and suggest appropriate organizational implementations for them.

Role 1: A global infrastructure for incident response to fulfill mission 1 and provide the necessary information in support of mission 3.

Role 2: An organization

- **representing the field of incident response as a profession (mission 4);**
- **providing a forum for the improvement of IT security and incident response (mission 2); and**
- **providing the capability to support the improvement of IT security (mission 3) in cooperation with Role 1.**

2.3 Tasks, Requirements Issues, and Current Resources

In this section, we consider the tasks associated with fulfilling the two roles outlined in Section 2.2.5. We then identify the general requirement issues for each mission within the role. We have limited ourselves at this stage to identifying the list of requirements issues that need to be addressed; we do not specify set the values or standards of the requirements. We conclude our discussion of each role by listing groups that exist today that contribute in some way to the role and briefly noting how they do or do not fulfill the need.

We have attempted to categorize tasks for each mission as either "sensitive" or "open." We consider sensitive tasks as those involving information of a sensitive nature, which cannot be made public unless sanitized; for example, specific details of sites involved in an incident and details of how to exploit security problems for which no fixes are currently available. We consider open tasks those involving information that is not sensitive. For some missions only open tasks are listed as we did not identify sensitive tasks associated with fulfilling the mission.

This and the remaining sections of the document are in still in preliminary form and should be considered as work in progress. We will update and refine these sections after gathering input from the stakeholder communities.

As noted in Section 2.2.5, we expect some overlap between the missions. Overlaps are reflected accordingly in the current tasks listed in this section. At this time, we have not fully completed our analysis and structuring of the task lists and requirements issues. In particular, the tasks for missions 2-4 need additional review to ensure that they are listed appropriately. As with previous sections we have not yet attempted to prioritize the information provided on tasks, requirements issues or current resources.

2.3.1 Role 1: A Global Infrastructure for Incident Response

2.3.1.1 Tasks for Mission 1

Sensitive Tasks

The majority of the work conducted by the infrastructure is sensitive in nature. As a result, most of the sensitive tasks associated with fulfilling the overall vision appear here. These tasks can be divided into 5 groups that fall into the following topic areas:

1. Response to events and incidents
2. Information about the internal work of the infrastructure
3. Integration of new infrastructure components
4. A closed forum facilitating the specific needs of the infrastructure components
5. Critical external collaboration needs for the infrastructure.

1. Response to Events and Incidents

- Enable authenticated and confidential interactions between infrastructure components to
  - Exchange information related to requests, incidents, vulnerabilities, attacks, artifacts, and threats, etc.
  - Coordinate activities in response to incidents, vulnerabilities, attacks, artifacts, and threats, etc.
  - Inform other infrastructure components about progress made in response to new vulnerabilities, attacks, and threats, etc.
- Enable private and effective cooperative work between infrastructure components to
  - Analyze specific requests, incidents, vulnerabilities, attacks, artifacts, and threats, etc.
- Enable appropriate and effective coordination to
  - Enforce an agreed-upon minimum response level by infrastructure components in regard to incidents, vulnerabilities, attacks, artifacts, and threats, etc.
  - Ensure a collective response from the infrastructure components in regard to major events that have a global impact.

2. Information About the Internal Work of the Infrastructure

- Provide information about the internal work of the infrastructure components to
  - Allow the analysis of information regarding incidents, vulnerabilities, attacks, artifacts, and threats, etc. by the organization fulfilling mission 3
  - Share the global aggregation of data in a suitable format protecting the victims and sites involved in incidents as best as possible while providing as much as possible.

3. Integration of New Infrastructure components

- Provide a mentoring process to
  - Ensure that each infrastructure component understands its role and agrees to meet the minimum response level requirements
  - Educate infrastructure components in guidelines, standards, policies, and procedures
  - Ensure that each infrastructure component is integrated at the appropriate level
- Act as a clearing house to
  - Prevent inappropriate groups from undermining the infrastructure by posing as part of it
  - Ensure minimum levels of quality assurance throughout the infrastructure – such as agreed-upon levels of minimum response.
- Enable improvement and evolution of the infrastructure by
  - Developing and maintaining a vision for an effective and efficient global incident response infrastructure
  - Developing and recommending guidelines, standards, policies, and procedures for the work of the infrastructure. This includes prototypes for infrastructure components, interactions within the infrastructure and externally (e.g., law enforcement), consideration of specifics within nations, etc.
  - Building working groups to address specific topics of common interest for infrastructure components such as common terminology, classification schemes for attacks and vulnerabilities, etc.
  - Helping law enforcement establish their own teams that provide a center of competence for law enforcement incident response
  - Coordinating and overseeing changes in the interactions of components by encouraging the formation of new coordination centers
  - Continually reviewing missions, goals and services to adapt to current and projected change

4. Closed Forum Facilitating the Specific Needs of the Infrastructure Components

- Provide a closed forum for infrastructure components to
  - Participate in informal discussions of topics that are of interest and are sensitive in nature
  - Participate in discussions of interest to a subset of infrastructure components of similar types (geographic and team/service type) to share experiences and discuss common problems and issues

5. Critical External Collaboration Needs for the Infrastructure

- Organize closed and in-depth training by infrastructure components of
  - law enforcement (including international organizations)
  - legal staff (including international forums)
  - governmental agencies (including international organizations)
- Organize and provide training of infrastructure components by
  - law enforcement (including international organizations)
  - legal staff (including international forums)
  - governmental agencies (including international organizations)

Open Tasks

The work of the infrastructure generates information for the benefit of the broader community. As a result, there are open tasks associated with propagating the public information provided by the infrastructure and an ongoing need to promote its efforts.

- Provide information about the infrastructure and its work to
  - Educate others about how to make best use of the infrastructure
  - Advocate the minimum level of authority and position in organizational structure for new infrastructure components to be effective
  - Further distribute information publicly disseminated by infrastructure components
  - Provide infrastructure components with information suitable for their specific constituents
  - Provide ongoing awareness of the need for the global incident response infrastructure and how effective it is at meeting it's mission; that is, how the information infrastructure is affected by incidents and events addressed by the mission of the global IR infrastructure
  - Enable contacts with the infrastructure components by providing references for them, indicating the role they play and the constituency they serve
  - Ensure that parties know how to interact with the infrastructure and the policies that are in effect (information sharing, press policy)

- Lobby with other stakeholders such as
  - Media to voice opinions related to incident response and the infrastructure

2.3.1.2 Requirements Issues for Role 1

Because many of the global infrastructure's tasks are sensitive in nature, it is natural to expect that it will have the most rigid set of requirements associated with successfully fulfilling its mission. There are three groups of requirements issues that need to be addressed for this role.

1. Functionality of the infrastructure
2. Coverage
3. Sensitivity and security

1. Functionality of the Infrastructure
Exchange, coordination, and leadership
- Information flow
- Control flow
- Timeliness of interactions

This first group of issues relates to how the infrastructure functions. The functionality of the infrastructure is based on the exchange of information, the coordination of actions, and collaboration on specific topics and operational issues. To maintain, develop, and foster collaboration within the infrastructure, leadership is necessary.

It is also critical to determine how, when, and between whom information is exchanged, what information is exchanged, and how the flow of information is controlled. Issues that need to be addressed include:
- Who accepts incident reports?
- How are such reports transferred within the infrastructure?
- What infrastructure components should received what types of reports?

In addition to functionality, we must consider the service level provided by the infrastructure and other related requirements. One of the most obvious problem areas here is the timeliness of interactions because much of the flow of information within the infrastructure will be time critical. This is difficult to ensure on a global level given availability issues such as time zones and other factors. It is critical to the success of the infrastructure to ensure that information on ongoing incidents or new attack types is shared appropriately and quickly (a span of minutes and hours).

2. Coverage
- infrastructure components in each country

To allow the accessibility of the infrastructure, components must be readily available from within each country or area - "in reach" - to allow easy (same language) access for reporting and follow-up during the response process. Considering that every nation operates under a different jurisdiction and has its own set of legal requirements, it is most appropriate to ensure that at least one infrastructure component exists in every country. This is also necessary to provide truly global response. Many countries will have multiple components. How components within a country interact and how the rest of the infrastructure views them is an additional aspect of requirement 1.

Service levels are also associated with coverage. Not only does geographical/national coverage need to be ensured, but also the coverage must be timely and sufficient resources must be available to handle all incoming requests and reports.

3. Sensitivity and Security
- Attack
- Privacy
- Confidentiality
- Authenticity
- Availability / Survivability
    - Crisis
    - Attack

The data collected, stored, and maintained by the infrastructure is highly sensitive and demands a high degree of security. The infrastructure must ensure that sensitive information is kept confidential and that it is not inappropriately disclosed externally.

Data is generated by "customers" and through cooperative work within the infrastructure. Neither set of data might be readily available outside the infrastructure. Examples are information that enables someone to compromise the victims of attacks and incidents or to access data specifically available on new attacks, vulnerabilities, or exploit programs.

The existence of this sensitive data will result in attempts to gain unauthorized access to it. As a result, the privacy of victims and constituents can be placed at risk. Additionally, the data collected - from passing the initial report around within the infrastructure to the analysis (statistically and otherwise) of the incident and related actions/information - might expose the victim/constituent. Other risks to the data and the operation of the infrastructure result from failures to ensure the authenticity of the stored and communicated data. Besides revealing the identity of a victim, the inclusion of a false identity within an incident report might result in high damages for those falsely identified.

Because constituents rely on the infrastructure to coordinate response activities, its availability is an issue in times of crisis and especially during and after attacks. This includes attacks specifically designed to limit its availability (such as sending hundreds of false/bogus reports). The community is likely to become dependant on the infrastructure and the services it provides. To be successful, the infrastructure components and the overall infrastructure must be resilient to in the face of attack and ensure that it can continue to function even in crisis situations.

In the future, more and more attacks may have a global impact on all Internet-connected sites. To ensure a global response, the infrastructure will be needed to coordinate response and carry out operational response activities. Because the response includes all measures to identify attackers and to limit the future exposure or damages, destroying the infrastructure might expose the community without any means to fight global attacks.

2.3.1.3 Current Resources for Role 1

There are a number of resources that exist today that might be considered either components of a global incident response infrastructure or resources that can be used as leverage points from which components might evolve. The following list provides an overview of the existing resources and an indication of their efforts in this area.

- Forum of Incident Response and Security Teams (FIRST): FIRST provides a forum for IRSTs from a wide variety of communities (government, military, academia, vendor community, telecommunications, banking, etc) and nations (approx. 20 nations are currently represented) to share IRST information. FIRST itself does not provide any operational element for coordination or response to IT security incidents. It does, however, provide an introduction service for new teams wishing to join the community. Coordinating response to IT security incidents and other operational activities are the responsibility of the individual member teams.

- CERT® Coordination Center (CERT/CC): CERT/CC provides a trusted point of contact for Internet IT security incidents. In addition to its incident response services, CERT/CC’s other activities that pertain to this mission includes helping the formation of new IRSTs,

coordinating the efforts of teams when responding to large-scale incidents, and performing vulnerability analysis and resolution.

- EuroCERT: EuroCERT is a service provided as part of the SIRCE (Security Incident Response Co-ordination for Europe) pilot sponsored by TERENA. This service provides an information resource for IRSTs. Initially, EuroCERT provided an incident support information resource, primarily based on information servers and mailing lists. In 1998, EuroCERT began a basic incident coordination service within Europe.

- National IRSTs: Some nations have national IRSTs that act as a central point for coordinating the response to IT security incidents in their counties. However, many of these "national" teams really focus on providing services to academic and research networks rather than the nation as a whole. There are far more nations that do not have a national resource of any kind than there are nations that do have a team.

- Other IRSTs: We estimate that there are about two hundred other IRSTs in existence today. This category includes response teams for individual universities, commercial organizations, IT product and security vendors, and others. Incident response is now becoming part of the mainstream security business. Consequently, organizations that are already concerned about security are adding incident response to their security framework. We expect the number of teams to continue to grow rapidly for many years to come.

- Critical Infrastructure Protection Groups: The emergence of national critical infrastructure protection groups is in its infancy. Currently the most well established group is the USA's National Infrastructure Protection Center (NIPC). The NIPC is brings together representatives from the law enforcement, other U.S. government agencies, state and local governments, and the private sector in a partnership to protect the USA's critical infrastructures.
  Another group is the U.S. National Security Telecommunications Advisory Committee (NSTAC), who focus on the telecommunications infrastructure in the USA.

  The mission of critical infrastructure protection groups means that they will be nationally focused and will have little or no international component to their missions.

Today, the nearest we come to a global infrastructure of incident response is a loose structure of IRSTs that voluntarily share information and collaborate if the people involved see a need or another benefit. The successes so far in this area have often resulted from the efforts of influential individuals who coordinate specific collaborations.

Some components of the global infrastructure exist, but many more are missing. As new teams do form, issues of scale make it difficult for them to become incorporated into the broader IRST community. Although the existing components are aware of each other, there is no recognized global response infrastructure for them to identify themselves with. As a result, little exists in the way of a coordinated approach to global incident response activities. FIRST is leading the efforts in the area of international collaboration; but, although many of its members respond to IT security incidents, FIRST itself lacks an operational mission.

Until there is a base set of commonly agreed-upon interactions for cooperation between teams and a recognized global infrastructure with which teams can identify, it will be hard to make progress.

2.3.2 Role 2: An Organization

This role includes missions 2, 3 and 4. As appropriate, we provide sensitive and open task lists for each in turn, followed by requirements issues and the current resources associated with this role.

2.3.2.1 Tasks for Mission 2

Sensitive Tasks

We do not anticipate any sensitive tasks associated with this mission.

Open Tasks

The majority of the work necessary for this forum be divided into three groups, which fall into the following topic areas:

1. Opening Communications Channels
2. Supporting Standards and Improvement Efforts
3. Building Awareness and Resources

1. Opening Communications Channels

- Enable authenticated interactions between all involved stakeholders to
  - Provide an open forum for discussion of the future of incident response and IT security issues
- Establish liaisons among all stakeholders independent of their specific role in order to allow the open forum to grow and to facilitate specific goals such as
  - Supporting the cooperation between law enforcement and the IRST community
  - Enabling communication with government about IRST issues
  - Enabling communication with private sectors about IRST issues
  - Lobbying governments/policy makers to ensure that there is a common understanding of all aspects that will have an impact on efficient and effective international prevention and response to security incidents
  - Lobbying the press to voice opinions related to the improvement needs of incident response and IT security and to communicate the threats to society (or part of it)

2. Supporting Standards and Improvement Efforts

- Enable effective cooperative work among stakeholders to
  - Influence and improve the work of international standard-setting bodies in developing guidelines and standards
  - Influence and improve the work of private sector security-related organizations in developing guidelines and standards
  - Influence and improve vendor security practices relating to both customer care and product security, including baseline security standards
  - Influence and improve ISP security practices in an effort to enhance security for their customers
  - Lobby for the recognition of established standards of the global incident response infrastructure
  - Monitor advances of standards in the area of incident response that might affect IRSTs and the global incident response infrastructure

  - Improve the general understanding on types of evidence to gather and how to gather it for law enforcement needs (should include general guidance plus specific information for different jurisdiction)
  - Influence policy at all levels to help achieve the IRST community's goals and general security improvement goals
  - Interact with the insurance organizations (through an umbrella group for insurance organizations) to help them better assess the network security issues to address when assessing risks.
  - Act as an advocacy group on issues that affect IT security at the local, national, and international levels
  - Facilitate technology transfer of improved IT security practices from the research community to other stakeholders.
- (Overlaps with Mission 4) Enable the improvement and evolution of the global incident response infrastructure by
  - Acting as an advocacy group on issues that affect incident response at the local, national, and international levels
  - Overseeing the operation of the global incident response infrastructure and IRSTs at the local, national, and international levels

3. Building Awareness and Resources

- Support the awareness-building process in regard to
  - Requirements users have in relation to vendors
  - Requirements users have in relation to incident response
  - Needs for IRST services
  - Needs for improvement within the global incident response infrastructure and its interaction with other stakeholders
  - The fact that parts of the global incident response infrastructure and IRST society might not be appropriate to commercialize
  - The fact that incidents are part of the information revolution and are not to stop in the near future
  - Risks to the society resulting from the security impact of information technology
- Provide a directory of international stakeholders, especially of
  - law enforcement groups (including international organizations) that specialize in incident response crimes/issues

2.3.3 Tasks for Mission 3

Sensitive Tasks

As previously discussed, this mission relies on access to data provided by the infrastructure components. Some of this infrastructure data may be public, but most of the information is sensitive. The tasks listed here relate to the sensitive aspects of handling unsanitized data from the infrastructure. Note that the following list includes an artificial task that allows many of the other tasks for this mission to be categorized as open tasks.

The tasks in this section have yet to be grouped into specific topic areas:

- Enable authenticated and confidential interactions with global incident response infrastructure components to

  - Receive and exchange information related to incidents, vulnerabilities, attacks, artifacts, and threats, etc.
  - Provide aggregated sensitive information about incidents, vulnerabilities, attacks, artifacts, and threats, etc.

- Enable private and effective cooperative work with global incident response infrastructure components to
  - Analyze information collected by the infrastructure and aggregate it to identify new trends and developments
  - Develop improved ways for exchanging the necessary set of information about IT security incidents and among infrastructure components
  - Develop guidelines what information should be given to whom in relation to incidents (maybe anonymized/sanitized)

- Enable appropriate and effective coordination to
  - Enforce an agreed-upon minimum reporting by infrastructure components about incidents, vulnerabilities, attacks, artifacts, and threats, etc.
  - Ensure timely reporting - especially if an assessment on a possible new attack type is requested
  - Receive feedback from law enforcement to understand the current law demands in regard to specific case studies (in various countries)

- Work on sensitive data collected from infrastructure components to produce sanitized information to
  - Support the awareness building for weaknesses, threats, incidents, and/or the commercial/financial/overall benefit of an organization having its own IRST
  - Support the promotion of the global incident response infrastructure and the work of IRSTs
  - Build case studies that highlight specific instances which need to be considered by law enforcement, law makers, or others to address new developments
  - Build case studies that highlight specific instances which need to be addressed by the global incident response infrastructure in order to improve their work
  - Undertake realistic evaluations/comparisons of security tools products

- Provide information to infrastructure components that contains more sensitive detail or more timely information than might normally be publically distributed to
  - Act as a technology watch for the overall IRST community

- Enable improvement and evolution of this mission by
  - Developing and maintaining a vision for an effective and efficient operation
  - Providing and maintaining quality management standards for public information

Open Tasks

The open tasks for mission 3 relate to the dissemination of sanitized data and analyses resulting from the sensitive tasks listed above.

The tasks in this section have yet to be grouped into specific topic areas:

- Provide information about and resulting from the global incident response infrastructure to

  - Act as a clearinghouse for information disseminated from the infrastructure
  - Promote infrastructure components by providing value-added information; for example, the services that the different teams provide and the make-up of their constituency
  - Support incident reporting to infrastructure components by explaining the regulations governing the work of the components and by providing information about issues, such as the use of encryption or the definition of computer crimes in different countries
  - Support the further distribution of IRST community announcements

- Provide public information about the sensitive information collected, sanitized, and analyzed to
  - Act as a clearing house and information center in regard to the actual state of IT security as experienced by the global incident response infrastructure
  - Support awareness building for weaknesses, threats, incidents, and/or the benefit – commercial/financial/overall - for an organization to have its own IRST (for example, with case studies)
  - Support the promotion of the global incident response infrastructure and the work of IRSTs (for example, with case studies or success stories)
  - Support the understanding and assessment of incidents, vulnerabilities, attacks, threats, etc. by providing sanitized statistics
  - Support the consideration of specific instances and evolvement of laws and standards (for example, with case studies that highlight specific instances that need to be considered to address new developments)
  - Build case studies that highlight specific instances that need to be addressed by the global incident response infrastructure to improve their work

2.3.3.1 Tasks for Mission 4

Sensitive Tasks

We do not anticipate any sensitive tasks associated with this mission.

Open Tasks

Mission 4 acts as an umbrella for many of the tasks covered in missions 1, 2 and 3. As a result, the task list below reflects a major aspect of fulfilling mission 4 – a strong voice in the broad community in regard to IRST issues and the work of the infrastructure. However, note that although tasks listed for this mission may overlap with some of those for other missions, this mission will really reflect the combined strength and voice of all the efforts and so will carry additional weight and influence in the broader community.

The tasks in this section require additional review for appropriateness and have yet to be grouped into specific topic areas.

- (Overlaps with Mission 2) Enable improvement and evolution of the global incident response infrastructure by
  - Acting as an advocacy group on issues that have an impact on incident response at the local, national, and international levels
  - Overseeing the operation of the global incident response infrastructure

- Enable open and effective cooperative work between IRSTs to understand the legal situation that might affect the ability of IRSTs to perform their work and meet their agreements (examples include differences in the laws of various countries and non-disclosure agreements)

- Enable improvement and evolution of the IRST community by
  - Advocating the minimum level of authority and position in organizational structure for IRSTs to be effective
  - Developing and maintaining a vision for an effective and efficient IRST community, including the global incident response infrastructure
  - Developing and recommending guidelines, standards, policies, and procedures for the work of IRSTs, including prototypes for infrastructure components, interactions within the infrastructure and without (like law enforcement), consideration of national specifics, etc. (in cooperation with the global incident response infrastructure)
  - Building working groups on specific topics of common interest for IRSTs – common terminology, classification schemes for attacks and vulnerabilities, etc. (in cooperation with the global incident response infrastructure)
  - Collecting information about knowledge available in different teams and conditions under which this knowledge might be available to others
  - Acting as technology watch for the overall IRST community
  - Monitoring advances of standards in the area of incident response that might have an impact on IRSTs
  - Identifying future needs of IRSTs to be able to facilitate the IRST business
  - Developing tools to help the IRSTs to perform their work
  - Providing a sponsorship program to allow other interested parties to contribute to incident response
  - Building awareness that incidents are part of the information revolution and will not stop in the near future
  - Building awareness about risks to the society resulting from the security impacts of information technology
  - Acting as an advocacy group on issues that affect incident response at the local, national, and international level
  - Tracking the development of other "players" whose activities might affect the CSIRT community
  - Establishing/facilitating liaisons with those whose activities affect the CSIRT community
  - Coordinating with others whose activities affect the CSIRT community to achieve mutual goals or to educate them on CSIRT issues and influence them to help achieve the CSIRT community's goals and general security improvement goals
  - Lobbying with the press to voice opinions related to incident response and the IRST community

- Enable improvement of the operation of IRSTs by
  - Providing in-depth training for "learning by doing" for new teams
  - Providing education/training for IRSTs
  - Providing training material for IRSTs to use for internal training and/or external training
  - Helping new IRSTs become integrated within the IRST community
  - Helping IRSTs in becoming operational
  - Funding research that may improve the state of the IRST community or that may result in improved security (that is, fewer incidents)

  - Providing an arbitration service to resolve conflicts between different teams
  - Advocating the minimum level of authority and position in organizational structure for IRSTs to be effective
  - Promoting the need for client-confidentially clauses to apply to IRST organizations
  - Building awareness about requirements that users have in relation to vendors
  - Promoting/building awareness of the need for IRST services
  - Promoting/building awareness of the need for interaction among IRSTs
  - Building awareness that parts of the IRST business might not be appropriate to commercialize
  - Promoting the need for and effectiveness of incident response
  - Collecting user feedback about different teams and follow up with the team to ensure that the conflict/misunderstanding is resolved
  - "Translating" between different cultures as cultural differences might affect the way, incident response is viewed

- Provide an open forum for IRSTs to
  - Participate in informal discussions of topics that are of interest and not sensitive in nature
  - Participate in discussions of interest for a subset of IRSTs of similar types (geographic and team/service type) to share experiences and discuss common problems and issues
  - Establish virtual chapters for special interest groups and virtual communities as appropriate (A community of national teams may want to talk; a community of university teams might want to talk; and a geographically-close group of different teams may also want to talk. Forums need to take into account the fact that similar-types of teams that wish to communicate may not be geographically close.)
  - Discuss the future of incident response and IT security issues

- Provide guidelines, recommend standards, policies, and procedures that establish and support the operation of IRSTs
  - Develop a press policy in relation to information not owned by the local team but by the IRST community
  - Provide quality management standards for public information
  - Guidelines for establishing and operating an IRST
  - Setting quality assurance guidelines for IRST customers
  - Develop prototypes for IRSTs
  - Develop standard operating procedures for all activities related to incident response and the related interaction among IRST members
  - Set professional standards/qualifications for IRST staff
  - Provide certified education for new teams
  - Provide guidelines on what evidence to gather and how to gather it for law enforcement needs (would need to be something general plus specific information for different jurisdictions)

- Establish recognition of incident response efforts and IRSTs based on agreed-upon quality measurements
  - Membership in one or more IRST umbrella organizations or being certified in some way might become a business differentiator
  - Compliance testing of IRSTs and staff in regard to established standards
  - Certification of "good" IRSTs that meet or exceed the set standards
  - Awards for IRST and IRST staff excellence

    - An award program to recognize improved incident response effort by service providers, etc.

- Establish incident response as a profession
    - Advocate the importance and need for expert/professional IRST staff
    - Solicit information for and generate IRST salary and funding surveys
    - Provide funding for scholarships in IR training and IT security training
    - Cooperate with others who provide additional education suitable for the area of incident response
    - Awareness building to integrate incident response into curriculum

- Provide information services for the public
    - Keep track of what teams exist where, and the constituencies that they serve
    - Provide directory of international stakeholders
    - Provide a directory of law enforcement groups (including international organizations) that specialize in incident response crimes/issues
    - Provide information about IRSTs and their services, such as conferences, training programs, sponsorship
    - Release information to the press about the state of incident response; guidelines
    - Provide information services to distribute announcements of the IRST community
    - Maintain a directory of IRSTs
    - Maintain a directory of information sources in relation to IRSTs
    - Maintain a value-added collection of information from other IRSTs
    - Maintain a value-added collection of information available for IRSTs; for example, the legal requirements in regard to incident response that might exist in other countries and/or organizations
    - Provide case studies in each area to show what models are possible and in what situations
    - Provide value-added information, such as the services provided by the different teams and the characteristics of their constituency, including regulations governing their work

2.3.3.2 Requirements Issues for Role 2

The requirements issues associated with this role can be considered as the combined set of requirements for each of the missions that it fulfills. However, as some of the more stringent requirements pertain only to a subset of the tasks, it is worthwhile to review the requirements for each mission.

The requirements for mission 2 and 4 are very similar in scope and nature:

Mission 2
Exchange, coordination, and leadership
- Information flow
- Coordination of events
- Facilitating the development of standards, policies, and agreements

Coverage
- Liaisons to each player on national and global levels

To ensure its success, the forum must establish liaisons to all stakeholders on the national and global level to ensure transfer of the available information among all parties.

Sensitivity and security
- Authenticity
- Limited confidentiality for working groups
- Privacy for confidential surveys, delphi studies, etc.

The sensitivity and security demands are lower for this mission than for any component of the global incident response infrastructure. Much of the information shared in this forum will not be sensitive and is destined for (semi-)public consumption. However, authenticity is an essential requirement, as any compromise might but the whole forum at risk.

Confidentiality and privacy issues mainly come into play for some working groups that require it. However, the greatest need for addressing these issues is likely to be associated with confidential surveys or delphi studies carried out by the forum.
*

Mission 4
Exchange, coordination and leadership
- Information flow
- Coordination of events
- Coordination of training and education
- Facilitating support of standards, policies, and agreements related to IRSTs and especially supporting the establishing and enlargement of the global incident response infrastructure

In addition to requirements introduced for mission 2, the following additional requirements need to be considered here. Because training and other forms of education fall under this mission, additional coordination requirements will be necessary. In particular, the establishment and maintenance of support for standards, policies and agreements related to IRSTs needs to be coordinated and managed. This relates to (and especially supports) the establishment and growth of the global incident response infrastructure.

Coverage
- Liaisons to each player on national and global level
- Membership of major part of individuals serving within IRSTs
- Membership of major part of IRSTs
- Recognition by society at large as representative

To ensure the community coverage necessary to support all the tasks in mission 4, and to ensure that the organization has credibility and gains acceptance, the bulk of its constituency must consist of the individuals serving within IRSTs as well the IRSTs themselves. To enable the professional organization to take on its mission, it will also need to be recognized by the society at large as an advocate for and representative of the global IRST community.

* Specific questionnaires are given to experts or the public to gain the community's assessments, which are expected to be very near to the reality. This even holds up for future developments. Usually there is a second round in which all participants review the results and have an opportunity to modify the assessment they initially gave.

Sensitivity and security
- Authenticity
- Limited confidentiality for working groups
- Privacy for confidential surveys, delphi studies, etc.

Mission 3
With respect to the open tasks, the requirements issues for this mission are similar to those for missions 2 and 4. However, with respect to the sensitive tasks, the requirements issues are similar to those for the global incident response infrastructure. This is a natural consequence of the direct relationship between missions 1 and 3. Any difference in the requirements issues for this mission are clarified below:

Exchange, coordination, and leadership
- Information flow
- Audit by trusted parties (required to ensure that confidentiality and privacy requirements are met)
- Facilitating support for the analysis of any suspected or actual compromise of other requirements to ensure the ongoing support of mission 3

Coverage
- Establish liaisons to organizations involved in improving IT security
- Ensure acceptance by each player on the local, national, and global levels as clearinghouse for information related to incident response-that is not otherwise accessible outside of the global incident response infrastructure
- Establish and maintain recognition by society at large as information (and resource) center for information about global incident response and the incidents handled by the infrastructure

The information assembled can be of benefit only if it is disseminated and used in the broader community. To support this effort, information and technology transfer is critical to the success of this mission.

Sensitivity and security
- Attack
- Privacy
- Confidentiality
- Authenticity of information services (highly important as they are publicly available and any introduced failure might reflect badly on the overall ability to ensure other requirements)

Survivability
- Attack

2.3.3.3 Current Resources for Role 2

Mission 2
There are a large number of discussion forums in existence today that cover small portions of this mission. The following list provides an overview of the existing resources and an indication of their efforts in this area:

- Forum of Incident Response and Security Teams (FIRST): FIRST provides forum for incident response and security teams, practitioners and experts from law enforcement interested in the FIRST community.

- Other IRST Forums: European IRSTs have been holding open meetings for a number of years to discuss the need for and ongoing progress of IRSTs in Europe.

- Task forces or working groups in forums such as those connected with TERENA (Trans-European Research and Education Networking Association) that support the development of incident response efforts and security improvement as part of coordinating transnational networks (The TERENA Task Force "CERTs in Europe 1995" - http://www.eurocert.net/history/cert-task-force-report.html);

  Similarly, the Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG) is chartered to create the AP regional forum to promote the exchange of ideas and expertise on Internet security incident handling and to foster closer collaboration among the IRSTs in the Asia Pacific region.

- Security Organizations:
  A variety of security organizations provide no incident response services, but do either support the discussion of IT security incidents or attempt to gain a more detailed picture of risk exposure and actual loss resulting from incidents.. Many are focus their efforts on a particular area such as telecommunications or banking. These include:
  International Information Integrity Institute (I-4)
  The International Security Forum – (ISF) [Formerly the European Security Forum]
  The National Security Institute (NSI)
  The Communications Fraud Control Association (CFCA)
  European Institute for Computer Anti-Virus Research (EICAR)
  The Information Systems Security Association (ISSA)
  The SANS (Systems and Network Security) Institute

- Law Enforcement:
  The International Organization on Computer Evidence (IOCE): Provides an international forum for law enforcement agencies to exchange information concerning computer crime investigation and related forensic issues.
  High Technology Crime Investigation Association, Inc (HTCIA)

- International Policy Efforts:
  Group of Eight Advanced Industrial States (G8)
  Organization of Petroleum Exporting Countries (OPEC)
  Organization for Economic Cooperation and Development (OECD)

- Standards Groups: Groups that address IT security or other related standards (both international and proprietary) include
  Internet Engineering Task Force (IETF)
  The International Organization for Standardization (ISO)
  The Institute of Electrical and Electronics Engineers (IEEE)
  World Wide Web Consortium (W3)
  The Open Group

- Other Organizations: A large number of other organizations exist that address IT security issues at some level, but security is not the organization's central focus – USENIX is a good example.

Although at first glance there appears to be a large number of organizations working in this area, much of the current effort is being undertaken in isolation and there is limited cooperation and coordination taking place. Various factors result in lack of cooperation and communications. The major two are that

1. In some cases the organizations (particularly some of the security organizations listed) are in direct competition with each other and are resistant to collaboration.
2. Many of the forums are closed, and membership restrictions inhibit external collaboration.

The lack of communication and coordination among the various stakeholder communities is the most significant issue preventing this mission from being achieved. Moreover, no single group has the charter to lead this mission and act as an umbrella organization to instigate communication and discussion among these groups in the area of IRST and IT security issues.

Mission 3

Most of the current work associated with this mission is in the area of statistics on IT security incident computer crimes. Most of the effort today that involves identification and analysis of threat information is being done by IRSTs and vendor organizations and falls under mission 1. Little threat analysis work in the 3-12 month time scale is being publicly undertaken at all. The following list provides an overview of the existing resources and an indication of their efforts in this area:

Statistical Information

- Global Statistics: The only example that we are aware of in this area is First's one-time collection of data based on the Melissa Word macro virus incident.

- IRST Statistics: Many IRSTs produce some form of statistics derived from IT security incidents that are reported to them. Given the lack of standards in the area ,it is difficult to compare the figures generated and is impossible to correlate them. AusCERT is currently conducting a consolidated statistics pilot study (http://www.auscert.org/Information/acsp/index.html) in an attempt to generate consolidated statistics in their constituency for a variety of attack types that are perceived as less serious and so are rarely reported.

- IT Security Questionnaires and Surveys: Many organizations collect data (often pre-sanitized) from a variety of sources and produce computer crime and security surveys. Organizations generating this type of information in the USA include the Federal Bureau of Investigation/ Computer Security Institute (FBI/CSI) and Ernst and Young. Similar efforts in other countries are underway in Australia: The Office of Strategic Crime Assessments and the Victorian State Police. However, some of the data samples are very small (in the hundreds).

Long-term Analysis: Little work has been accomplished so far in this area, mostly because there is limited data available. The work that has been performed has been conducted in the academic and research communities; for example, John Howard's PhD thesis, *An Analysis Of Security Incidents On The Internet*, based on CERT/CC incident data.

Because a number of stakeholders are very interested in IT security incident and computer crime statistics, significant effort is underway in this area. However, this work is being undertaken in isolation and is fraught with inconsistencies. The inconsistencies are primarily caused by a lack of agreed-upon standards for what constitutes an IT security incident or crime and a lack of understanding of whether reports are duplicated across studies. The efforts also lack a global perspective and are being undertaken with very small data samples relative to the global scale. Increasing the sample size is not easy given the current collection methods, and potential participants need to be convinced as to the importance of their contributions.

The data to fulfill this mission should be provided by the global incident response infrastructure and then analyzed and further disseminated under a neutral and independent organization. Then, depending on how the information is provided (from what infrastructure components and how heavily it is sanitized), security of the data and/or its origin becomes the main operational issue.

Mission 4
Many organizations in existence today promote IT security either as the main focus or a sub-focus of their charter. We have already listed many such organizations under the previously covered missions. In this section, we will duplicate organizations that have been listed previously only if they serve an additional purpose with respect to this mission. The following list provides an overview of the existing resources and an indication of their efforts in this area:

- Forum of Incident Response and Security Teams (FIRST): FIRST is fulfilling some of this mission, but its influence is limited due to lack of funding, its volunteer nature, and its lack of "clout" in the broader community (it lacks involvement with major players to promote the need for incident response). Another consequence of First's limited resources is that it has not attempted to seek acceptance as professional IRST organization.

- CERT/CC: In its efforts to help create a self-sustaining global incident response infrastructure, CERT/CC has developed a number of resources to help in the formation of IRSTs and the associated training of staff. However, at this time, many of these resources are not widely distributed.

- ISSA and others provide certification for information security professionals (CISSP); however, there is no specialty coverage for IRST issues.

- SANS provides information for security professions and resources related to incident response, such as their step by step guidelines for incident handling..

- IETF as undertaken some work in the area of IRST standards (but with little input from the IRST community).

Although many organizations exist to address some aspects of IT security issues, very little exists today that specifically addresses the needs of the IRST community.

2.3.4 Conclusion

There are a broad range of entities and organizations working in the general IT security arena. No single organization or group of organizations exist today that fulfill the vision of a global

infrastructure for incident response. Moreover, there is no current leader in this area providing the effort needed to make progress toward this vision and maintain the necessary momentum to carry this work forward. Unless there is a champion and a leader for these missions, progress will be slow (we cannot afford delays) and individuals organizations will follow directions that fulfill their own needs. Those needs are likely to be insignificant compared to the overall global need. It is imperative for the IRST community and society at large that the global need is nurtured and addressed.

To implement the vision, we need to consider how the missions can be implemented. There are two different approaches that can be taken:

Evolution of existing organizations
Establishment of new organizations

In the next section, we will discuss the possible approaches and will indicate the pros and cons associated with possible organizational models.

2.4 Organizational Models

Having identified the missions, tasks, and requirements issues associated with the key elements, we can now consider a range of possible organizational models for each of the two roles described in Section 2.2.5.

As noted in previous sections, this is a draft for discussion; we will revise and refine it after receiving feedback from stakeholders.

As we consider each model, the main issues we will discuss are

- **Funding sources.** No entity can fulfill the missions associated with either of the roles unless it has adequate and appropriate funding. The range of possible funding sources will vary depending on the role in question, the missions associated with it, the nature of the work, the players involved with undertaking the work, and the stakeholders who will benefit from it.

- **Authority and balance of power.** Although the nature of the both roles' work will require them to conduct business in different ways, they have some striking similarities. In order to be successful, both roles must provide an environment that supports the handling of sensitive issues and effective communication on a local, national, and global level. As a result, organizational models must take into consideration the issues of influence, competition, and trust that might affect the overall balance of power.

- **Issues of scale.** Both roles address global issues; consequentially, it will be necessary to consider global models to fulfill them. So we must consider models that support the participation of many different parties located in different time zones, originating in different cultures and countries, and governed by different regulations. However, it is not reasonable to expect that an implementation of either role will happen on a global scale overnight. Rather, implementation will evolve over time as the number of nations that become involved increases and as general interest in IT security and IRST issues grow.

- **Organizational requirements**. As appropriate, we will cover additional issues or requirements that may have an impact on success when setting up or implementing a given model to fulfill a role.

2.4.1 Role 1: Models

In this section, we outline three possible models for implementing a global infrastructure for incident response:

1. A Global Coordination Center
2. International Time Zone Coordination Centers
3. National Coordination Centers

A brief overview of each model follows, along with a discussion of the issues outlined above, as appropriate.

2.4.1.1 A Global Coordination Center

A natural model to consider is the establishment of a single center to coordinate global response to IT security incidents. At least a two-level hierarchy would be established, with the global coordination center at the top level and the rest of the infrastructure at one or more lower levels.

While conceptually this sounds like a clean and simple approach, it is fraught with practical and political issues. We will only discuss the main "show-stopper" issue. Experience has shown that it is insufficient to designate a component of the incident response infrastructure and expect it to succeed. To be successful, a component must gain constituency, recognition, and trust. It is unlikely that any one organization (of any form) could be established that could gain the global recognition and trust of every nation in the world. As a result, a single organization providing a truly global coordination service is not a viable option.

2.4.1.2 International Time Zone Coordination Centers

Another frequently discussed model is the establishment of a number of international coordination centers (ICCs) located in different time zones around the world to coordinate response to IT security incidents around the globe. If the ICCs were run by a single organization, the result would be the same as the global coordination center described above. So this model needs to be viewed from a different perspective. The ICCs would act as peers and coordinate their efforts, but each would be separately operated and run. This would also result in at least a two-level hierarchy being established, with the international coordination centers at the top level and the rest of the infrastructure at one or more lower levels.

The community has some practical experience in establishing, funding, and operating such centers both in the USA (the CERT/CC's coordination role) and in Europe (EuroCERT's coordination role). The discussion of the issues below are based on lessons learned from those experiences. The role is one of "coordination" in response to incidents and events and not one of operationally "handling" incident and events.

It is important to note that national teams have resisted the suggestion that a coordination team for a continent might take over the "operational" mission for a region. They believe that the operations should stay within the team, close to the constituency, where the funding is and where the language, culture, and laws are understood. . However, in some instances national funding bodies have given funding to EuroCERT instead of to the national team, falsely believing the international coordination entity would be a substitute for any national incident handling effort.

The impetus for a European coordination center resulted from the recognition that limited coordination among European teams was taking place and also from a general feeling that a coordination center located in Europe (rather than the USA) was needed for practical reasons (such as time zone, culture, and knowledge of the operating environments of the European teams). After a number of meetings by teams in the region, a project was initiated to establish a European CERT Coordination Service.

Experience has shown that although it is possible to provide an operational IR service on a national or international basis, provision of a multinational or global operational service has so far been unsuccessful. The reasons for this include the following:

- **Funding**. Nations fail to recognize the need to fund a national service and an international one. The funding source of an IRST has a big influence on how that IRST will be perceived and trusted both nationally and internationally.

- **Authority and balance of power**. Nations want to be responsible for their own needs and do not necessarily want a coordination center for the continent becoming privy to their data. Additionally, hostility between nations in the same geographical region will inhibit or prohibit cooperation. The role of a continental coordination center brings responsibility, prestige, and recognition. As a result, many countries may want to take on the role, making it hard to reach agreement. As previously discussed, trust and respect must be earned; they cannot be designated or delegated. There must be consensus and buy-in on the location and host of the continental coordination center. It is not something that could be moved from country to country on a rotating basis.

  For the reasons described above, even if sufficient ICCs did exist to provide global coverage, they would not hand off responsibility for activities within in their own constituency to another ICC. Effective collaborations between ICCs could not be enforced, and recommended guidelines could be set for inter-ICC collaboration. But as with any IRST, if the ICCs themselves do not have mutual trust and respect, interactions will suffer.

- **Issues of scale**. Organizations have yet to address the practicalities of scale when trying to dig through a huge volume of data resulting from a global influx of information. When providing coverage for more than one country, cultural and language issues come into play (this can even be an issue even within a single country). In the incident response field, it is vital to ensure that all parties involved understand what is being communicated. It is unreasonable to expect that each ICC would hand off coordination responsibility for activities relating to its constituency to another ICC. As a result, to be effective, each ICC would need to provide a basic level of services on a 24/7 basis. There are a number of practical issues that must be addressed when dealing with multiple time zones (such as shifts and coverage). It is hard to transition work from one time zone to another as the day passes around the world. And the transitions result in loss of continuity and in loss of productivity due to ramp-up during the hand off.

Although many coordination centers exist, truly multinational ones struggle to address the practical issues of providing operational service to a global community. We do not consider this to be a viable approach to address global incident response needs. However, if some nations can reach agreement and establish one or more international coordination centers, then these can participate as components in a global incident response infrastructure.

2.4.1.3 National Coordination Centers

The number of national teams is continuing to increase, and many other existing and newly forming teams have constituencies that fall within national boundaries. National boundaries provide a demarcation for policies, procedures, and jurisdiction for information exchange; thus, they provide an excellent opportunity for coordinating on a national level.

This approach is based on having every nation establish a national coordination center. This model is not as clean an approach as the first two and has its own limitations (described below), but it has more potential to achieve global coverage. Although these components need only provide a coordination effort, the centers might also undertake an operational incident-handling role, depending on the size of the nations involved.

One limitation of this approach is that there are teams (other than international coordination centers) that provide services to constituencies that cross national boundaries (IRSTs for multinational corporations). For this and other reasons, it makes sense to consider additional

coordination boundaries to support such cases; coordinating centers might exist for teams with similar needs, such as those within the banking or telecomm communities. This would result in at least a three-level hierarchy. This hierarchy could be made flexible enough to enable teams, as appropriate, to be served directly by a coordination center without the need for national coordination. Issues to be addressed within this model include the following:

- **Funding sources**. Funding will come from different sources and will be dependent on the function provided by the team, the constituency served, and the team's position in the hierarchy. Participating teams will need to seek their own funding sources to support them as an infrastructure component.

  There is potential for funding from role 2 to provide support for infrastructure components to conduct sensitive/closed discussions. From an operational perspective, it would be possible to seek funding for groups of infrastructure components to collaborate and to provide funding for national/multinational organizations to develop tools and services to support the infrastructure (but not to run it).

- **Authority and balance of power**. Determining how to appropriately position a given team in the hierarchy can be addressed by a combination of approaches. In some cases, this will occur bottom-up because there will be components that do not wish to provide the funding to perform a coordination role. Some teams that gain the trust and respect of others may naturally find themselves being recognized in a coordination role. In other cases, the level in the hierarchy will result from existing organizational structures. However, recognition of national teams themselves will result not only from national designation, but also from international recognition. Until base standards are recognized in this area, the situation will remain complex and problematic. Many existing "national" teams are not truly national because their constituencies do not officially extend to a nation but, instead, to national academic and research networks.

  A neutral arbitration service will be necessary for the discussion and resolution of dispute between IRSTs at all levels. We suggest that this service be provided by the professional society component of role 2.

- **Issues of scale**. For large-scale events that affect a significant number of sites across the world, this approach can become complex without a single team taking on the coordination effort for the event. Agreeing to allocate the coordination role "on the fly" would not be productive or efficient. It might be appropriate to identify and recognize a number of teams that are willing and able to take on such a role in advance.

- **Organizational requirements**. With such a large number of nations around the globe, a higher tier of coordinating teams will need to exist for this approach to work effectively. This higher tier is likely to evolve from a limited number of ICCs becoming established for small groups of cooperating nations, and other coordination centers representing specific interest groups and industries. In reality we will have a web of IRSTs that have the flexibility of coordination on a number of levels.

Although this approach is not ideal, it may be the only possible approach that can be implemented on a global scale. There needs to be a way of reaching agreement on some of the issues described above before this could be implemented. A major hurdle that the infrastructure will need to overcome is the minimum level of standards that all participating can agree to from the outset.

2.4.2 Role 2: Models

As previously discussed in Section 2.2.5, we envision a single international organization with national subsidiaries or chapters to undertake role 2. However, the number of missions and associated tasks that constitute this role make its initial start-up a daunting prospect. Rather than attempting to establish an organization that would immediately fulfill this role, we envision an initial implementation of the role that addresses only one mission or a subset of it. Then as more funding becomes available and as recognition increases, the organization can begin to add further missions and tasks until it has fully developed into an organization to fulfill the overall role. Below we consider each mission associated with role 2 and identify the organizational issues that need to be addressed.

The overall approach of developing an organization to fulfill role 2 should take into account how one mission depends on another, the tasks in each that support other missions, and the natural growth and progression of these issues. We'd appreciate feedback on what the broader community believes are the priorities across the missions served by this role and the relative priorities of the tasks within each mission.

In reality, the fulfillment of this role is likely to depend on the availability of funding and on the ways we can use existing resources. In addition, it will take a great deal of effort and dedication on the part of a small number of individuals to build the necessary support and momentum needed to make progress.

2.4.2.1 An Open Forum

Issues that must be addressed in relation to an open forum are the following.

- **Funding sources**. Funding should be sought from as many sources as possible and should not be limited to any one source. It can take the form of membership fees, sponsorship, grants, donations, and in-kind services (an organization might offer to host and underwrite working group discussions).

- **Authority and balance of power**. The participation of the major stakeholders for this mission is paramount to its success. Although the IRST community will be at the heart of this forum, if it is to succeed, no single stakeholder can be allowed to dominate it. One method that can be used to achieve this is to offer voting rights to individuals, enabling them to select the organization's leadership. Another is to ensure that funding sources are equally distributed between government and private sources.

  Balance of power can also be distributed on a global scale by operating the organization on local, national, and international levels. There are many different open forums in existence today that address similar organizational issues. These forums should be reviewed to see how they address the balance of power on a global scale.

- **Issues of scale**. Although the open forum must meet global needs, it will need to operate locally and nationally also to ensure success. In fact, this forum should encourage as much participation (both in breadth and numbers) as possible to ensure it is a strong global voice. The forum should include national societies that, in turn, foster local interest groups. Some

of the interest groups may also be on a global scale, addressing the needs of given community, such as telecommunications.

- **Organizational requirements**. The success of this organization depends on its ability to coordinate activities and initiate discussions. Providing these services requires a funded secretariat. And before it can begin to function, this organization must have adequate initial funding to operate this secretariat.

  Support for local and national efforts will be critical to ensuring progress and broader adoption of standards. The approach should encourage the formation of suggestions and recommendations at local and national levels and seek national adoption before attempting to reach international consensus. Wherever possible, the organization should strive for consensus on a common standards base. However, there will be cases where local and national differences, such as legal jurisdictions, prevent agreement on every aspect. So standards development and advocacy must be undertaken in parallel to help form consensus and minimize the need for exceptions. This forum will not influence policy overnight but this will develop over time as the forum grows, establishes a network of contacts, and gains broader recognition.

2.4.2.2 A Professional Society

The issues associated with this organization are similar to those for the forum, with the following exceptions:

- **Funding sources**. The stakeholders for this mission are the natural funding sources for this effort. As for the forum, funding could be accepted in a variety of forms and should be sought from as many sources as possible.

- **Authority and balance of power**. The participation of the major stakeholders for this mission is paramount to its success. The IRST community will be at the heart of this society and should hold the balance of power. However within that community it is nevertheless vital to ensure that the balance of power is distributed on a global scale by operating the organization on local, national, and international levels. There are many different international professional societies in existence today that address similar organizational issues. These should be reviewed to see how they address the balance of power on a global scale.

- **Organizational requirements**. In addition to the requirements listed for the forum, the professional society should establish a core effort and establish credibility before reaching out to other communities. As this society becomes established, it will naturally begin to build links elsewhere. Having developed those links, it can begin its efforts to influence policy.

2.4.2.3 A Capability

These are key issues to consider for the capability mission:

- **Funding sources**. The stakeholders for this mission are the natural funding sources for this effort.

- **Authority and balance of power**. This capability must have the trust and respect of the global community - and that of the infrastructure components - but must also retain neutrality. This is difficult to achieve unless this capability is assumed by a suitably qualified and respected international organization. As a result, the full mission of this capability cannot really be attained until either the forum or the professional society is established and ready to take on this mission.

- **Issues of scale**. Before it can begin operating, the capability must be ready to accept and process the great influx of sensitive data that it can expect to receive. This will require it to have an established secure environment and an internal infrastructure of tools and key management processes to accept and process data and to publish, and well-defined interfaces and processes for the receipt and authentication of incoming data.

- **Organizational requirements**. This effort is dependent on the existence and supply of information from the global incident response infrastructure. It is reasonable to expect that this effort could be initiated with a voluntary information flow from various IRSTs without agreed-upon standards being in place. But to truly fulfill its role, the capability needs structured input from as much of the infrastructure as possible. This requires a minimum level of standards and a significant number of infrastructure components to be in place.

Additionally, although every component of the infrastructure can be considered as a stakeholder for this mission, each component may not be able to supply information in the format required unless it either has funding for this purpose or the promise of a service in-kind. It is clear that there are several issues pertaining to the establishment and operation of this capability that suggest a greater likelihood of success if it is established after other missions are achieved or are close to being achieved. In addition to undertaking work of specific interest to its stakeholders, this capability should provide information to benefit the broader community. Although some organizations may be willing to provide funding for analysis and information dissemination for the greater good, others may not. It may be necessary to charge an overhead fee to ensure that broader community needs are addressed as well as specific interests of funding organizations.

2.5 Preliminary Conclusion

Our critical information infrastructures and the government and businesses operations that depend on them are at risk. We share the responsibility to improve Internet security and coordinate effective international global response to IT security incidents and events. To be successful, it is paramount that we ensure participation and cooperation among governments, law enforcement, commercial organizations, the research community, and practitioners who have experience in responding to IT security incidents.

It is inexpensive (the cost of a personal computer and Internet access), quick (less than a minute), and easy (using freely available intruder tools) for anyone to launch attacks against our critical information infrastructures. Conversely, it is expensive (international effort and funding), long-term (research, development, and deployment), and complex (technically and politically) to take the steps needed to harden the information infrastructure to make it less susceptible to attack, and to enable us to respond more effectively and efficiently when attacks do happen.

In this chapter we have presented our vision for an international infrastructure for global security incident response and have identified and discussed in detail the interdependent key elements we believe to be necessary to fulfill this vision. Significant participation, time and effort are necessary to implement the elements of this vision. Our preliminary assessment of the relative priorities needed for the roles are as follows.

2.5.1 Role 1: Priorities

Priority 1
There are two top priority issues associated with this role that must be addressed in parallel:

Infrastructure Consensus
Given the current number and diversity of IRSTs in existence today, the IRST community is on the brink of being unable to coordinate its efforts. There will undoubtedly be teams that see no need to implement any infrastructure at all as today's approach appears to be working. With the formation of many new IRSTs, the critical point will soon be reached. At that point, a natural breakdown in coordination is likely to take place and a loose form of infrastructure will result through the "old boy" network and similar methods. The resulting infrastructure is unlikely to be appropriate to fulfill our vision. So it is necessary to act quickly and reach consensus in the community on the need for a structured approach.

Continued Growth
To support the evolution of the infrastructure, we need to continue to raise international awareness and recognition of the problem. This will encourage the formation of more infrastructure components in the form of new IRSTs at all levels, and national IRSTs in particular. The forum is needed to advocate this need.

Priority 2

Infrastructure Support
To support the operation of the infrastructure, standards efforts in the area of IRST collaboration need to commence. This task is reliant on the forum's existence.

Additionally, to support the growth of the IRST community, the professional society is needed to provide training for IRST staff and to provide an IRST arbitration service.

2.5.2 Role 2: Priorities

Priority 1

Establishing the Forum
This is in direct support of the top priorities needed for role 1.

Priority 2
There are two priority issues associated with this role that must be addressed in parallel:

Expand the forum to include the professional organization
This is in direct support of the second-level priorities for role 1.

Develop a capability
This item may drop to a lower priority if the necessary growth and evolution of the infrastructure, standards, and funding are not in place to support it.

2.6 Next Steps

As we noted previously, this document is currently in draft form. Before developing this material further we are seeking feedback from the broader community and are particularly interested in hearing opinions on these:

- The overall vision
- Coverage of stakeholders
- Appropriateness of missions
- Coverage and priorities of tasks
- The relative priorities of the missions
- Coverage of requirements issues
- Coverage of current resources
- Appropriateness of organizational models

In addition, we are seeking input from the FIRST community to understand the role FIRST can play in this vision.

Subject to available funding and feedback from the FIRST community, we will then, as appropriate:

Review and revise the document based on feedback

Review FIRST as it is currently structured to assess the viability of FIRST undertaking one or more of the missions or roles. This would include identifying whether FIRST could migrate from its existing structure towards one better able to fulfill the need.

