

Keys to Successful Incident Response Teams

Sarah Granger 2001-08-21

Keys to Successful Incident Response Teams

by *Sarah Granger*

last updated August 21, 2001

History of IRTs

Incident Response Teams (IRTs) initially evolved in response to the growing threat of viruses and hacker attempts. In late 1988, a worm infected nearly 10 percent of the computers existing on the Internet. This was the first well-publicized example of how a small program could cause such extensive damage. (Warning: here come the acronyms...) As a result, the first official Incident Response Team, Computer Emergency Response Team (CERT), was born through the Defense Advanced Research Projects Agency (DARPA). By the end of 1990, 11 teams, including CERT and the Computer Incident Advisory Committee (CIAC), created an international organization, the Forum of Incident Response and Security Teams (FIRST) to communicate and coordinate between teams.

Today's IRTs generally prepare for and respond to any network security-related incidents, which include viruses, intrusions, worms, or any other unauthorized entry into a system or modification of information on that system. It's not just the FBI who hunts down the hackers - many corporations and government agencies have their own Incident Response Teams. By the beginning of 2001, the Internet included over 110 million computers. In 2000, CERT alone received reports of over 21,000 incidents and by Q2 2001, over 15,000 for this year. As security incidents are becoming more prevalent and receiving greater media attention, many large organizations are including Incident Response Teams as part of their security strategy. This article will offer an inside look at how these teams are formed and some keys to successful operations.

Forming an IRT

There are many good reasons to form an IRT, but the most important is prevention. Furthermore, an Incident Response Team allows a quick pre-established response to an incident, thereby minimizing the potential damage. By preventing more serious incidents and reducing the harm inflicted by incidents, IRTs can save businesses and government millions, if

not billions in potential network and data recovery costs. Other good reasons for IRTs include:

- Localization for efficient responses to incidents
- Separation of security services from ISPs (honestly, how quick are most collocation facilities at communicating important data anyway?)
- Educating system administrators and staff
- Increasing general security, thereby preventing and greatly reducing the number of incidents
- Coordinating responses from a central point
- Collecting data and determining incident trends
- Saving costs at time of incident by preparing in advance
- Responding in a manner that results in the least amount of damage and
- Collaborating with other security organizations

One of the principle challenges of security personnel is to convince organizations of the value of investing in the development of a good incident response strategy, including an IRT. Although most members of the security community only see the benefits of such preventative measures, an IRT must be more cost-effective than operating without an IRT in order to sell the idea to the bean counters. Things to consider when computing costs are: staff time and energy, including outside resources (external audits, etc.), the cost of sensitive data falling into the wrong hands, potential destruction of key product data, operational & development time lost from the regular cycle, and reputation costs, especially if the parent organization has a high profile in the security environment. Sandy Sparks of CIAC equates the function of an IRT to a town's fire department. The fire department's job is to contain the blaze, put the fire out, and prevent the damage from spreading. That's a tall order, but in most cases - a necessary one.

According to experienced IRT members, the keys to success are to clearly define the mission of the IRT. For example, IRTs can exist for one or more organizations within a community, which can be organizational, network-related, and/or geographical in nature. Boundaries must be determined in order to maintain strong management support. Sparks indicated that "CIAC's primary mission is always to assist sites who have had break-ins."

One of the keys to successfully implementing an effective Incident Response Team is to clearly define its purpose, this can be done with a mission statement. The mission statement allows the members and administrators of the IRT to understand the objectives of the team, and the manner in which those objectives are to be attained. For example, CERT's mission is to:

- Provide a comprehensive view of attack methods, vulnerabilities, and the impact of attacks on information systems and networks; provide information on incidents and vulnerability trends and characteristics
- Build an infrastructure of increasingly competent security professionals who respond quickly to attacks on Internet-connected systems and are able to protect their systems against security compromises
- Provide methods to evaluate, improve, and maintain the security and survivability of network systems
- Work with vendors to improve the security of as-shipped products

If the mission is not defined in detail the IRT may not receive the necessary support of management. Furthermore, without the clear objectives and guidelines that a mission offers, the team may not have the focus and direction required to be truly effective. Management's support is imperative, and its authority over the IRT should be clearly communicated throughout the parent organization/community. If it's tough to gain that management support, Chuck Athey, computer security expert and instructor, suggests finding a champion within the organization (most likely a CIO or CSO), someone who understands the technical and legal reasons for forming an IRT, and letting that person sell the idea to upper management. "Selling the IRT as a concept requires a different type than those who make up the team." By working with the right champion, the team can not only secure support and funding, but help in educating all of upper management as well.

IRT Components

Major components of the IRT include staff, technical equipment, policy, procedures, and community contacts. The energy of the IRT should be roughly split in half between training/prevention (proactive activities) and response (reactive events.) Once the IRT is deemed a necessary expense and its scope defined, people from all different areas must be brought into the loop.

Define a Contact Person

The first important step is to define one point of contact for all incidents. This person communicates to the outside world, coordinates and disseminates information throughout the team and to the parent organization. It is key that there be only one point of contact. This

lowers the margin of error considerably. It also provides better protection against unauthenticated calls. That person should be not only the point of contact for phone calls, but for e-mail, and that person should log all contacts and track by ID numbers. The IRT staff will be consistently placed under high stress, so team member roles should be rotated (and ample caffeine supplied), specifically concerning those on-call.

Key team departments generally include the CIO, Network and System Administrators, HR, Legal, Public Affairs, and Physical Security. Upper management must be kept informed, and the team should also have administrative and clerical assistance. This is all to ensure smooth communication of incidents and proper damage control. All sources consulted in the research for this article emphasized the importance in choosing the right people for the permanent IRT staff. Central team members need not merely have sound technical skills (operating system administration, network administration, and programming experience), but also good communications skills and integrity. Staff members should continually communicate with other IRTs to stay up-to-date. News groups and mailing lists, such as those hosted by Security Focus (shameless plug), are important resources. "The best thing people involved in incident response teams should do," Athey notes, "is get together and talk, keep up to date in information, and share."

One fun thing about being involved with an IRT can be the technology. It's a great place to play with the latest hardware, OS revisions, vendor packages and 3rd party software because all of these need to be checked for holes, viruses, and Trojan horses. Team members must be in the loop as to the newest holes. Most products have them, so it's important to be on the lookout.

Develop Incident Response Policies

Developing appropriate policies can be a royal pain, but it is essential to get this out of the way. Policies must be developed before the IRT is officially announced and functioning in order to promote efficient handling of attacks and potential attacks. The policies should be a part of the communication between the technical team members and upper management, and these policies should be recommended as general security policies to the parent organization/community.

One of the biggest policy issues is the question of how much information to give out to others (community, suspects, law enforcement, other IRTs) about attacks. In general, it's a good idea to default to a "no release without permission" policy in cases where it's not required to report the incidents to law enforcement authorities. Seeking permission from vendors and organization

members in advance of incidents can expedite the response process.

In addition to general and IRT security policies, it's a good idea to develop working procedures and/or an operations manual. According to Australia's Security Emergency Response Team (SERT), procedures to cover should include handling vulnerabilities, creating advisories, handling difficult contacts, handling unauthenticated callers, information disclosure, coordinating with other IRTs, systems management, backup strategy, disaster recovery, and off-site operations. For the more serious IRTs, role-playing provides an excellent method for developing procedures, like in military exercises.

The IRT will function in a number of ways, including training, prevention, and response. In all cases, it is important to collect good community, law enforcement, and vendor contacts. This helps the incident response process move more quickly and smoothly.

Once an IRT is formed and functional, it should be announced to the community through the usual paths: press releases, web site, conference participation, news groups, email lists, and through FIRST. This will allow members of the community to participate actively by submitting information and incident reports to the IRT. Timing is crucial - any announcement of an IRT will make the parent organization and the IRT into a target; therefore, careful planning is key.

Incident Prevention and Education

Although they are called incident response teams, a big part of the IRT's role is in incident prevention. Incident prevention includes, first and foremost, the education of technical IRT members and communication within the security community. IRT members must be up-to-date on the latest bug reports, advisories, and virus warnings. Attending conferences, workshop presentations, training courses, journal articles, and books provide a strong foundation.

For further information and training, CERT offers courses and provides introductory and advanced training courses for technical staff and the management of computer security incident response teams, as does the System Administration Network and Security (SANS) Institute. (Also see resources listed at the end of this article.) Other options for learning and making contacts are conferences and related events.

Prevention also means detecting, assessing, and terminating vulnerabilities. Holes that are discovered must be patched accordingly. Firewalls, packet filters, non-replaceable

authentication tools, such as S-key, and data encryption keeps information secure while assessment tools watch for unusual activities. Redundant servers, on and off-site backups, provide reliable methods for restoring networks in the case of major incidents. IRTs must also conduct regular network security audits, including checking of all log files. Related physical security includes safes, shredders, badges, and other methods of physical identification.

IRTs must also prepare for incidents that are anticipated beforehand. Preparation for such incidents can be extensive and resource-intensive. Preparation for incidents such as the "Code Red" virus, for example, can place tremendous strain on the IRTs of large organizations like Visa and Cisco, if only because the potential losses posed by such a threat are huge. Proper allocation of appropriate staff and network resources requires experience and planning. However, the importance of proper prevention and preparation cannot be overstated.

Incident Response

Here's the exciting part - tracking and catching the hackers. Actually, it should be noted that IRTs do not investigate individuals. This is the function of law enforcement agencies. IRTs merely collect and analyze data about the incidents. And in most cases, incidents covered by industry IRTs are similar to the incidents that all computer users encounter, such as viruses, break ins, denial of service attacks, etc.

The first step in the incident response procedure is to identify and confirm incidents. There's always the boy who cries "wolf". It's easy to mistake a file replacement error as a hacker attempt. Having the experts on the IRT assess incident reports closely will determine their relevance. Australia's SERT recommends determining the following basic facts when a vulnerability is reported:

1. Is this vulnerability easy to reproduce?
2. Does this vulnerability affect different versions of this software?
3. What previous level of access is required to exploit this vulnerability?
4. Does this vulnerability grant privileged access?
5. Does this vulnerability affect other vendor versions?
6. Is this vulnerability being actively exploited?
7. Can this vulnerability or others be further exploited to gain privileged access?
8. How many systems within the organization and the Internet are affected?

This is where the value of employees is shown - it is essential to have experienced people to make sure evidence is not destroyed, which means these people must not only be technically superior but also knowledgeable about the organization or business functions, so they can put themselves in the mindset of potential hackers and seek potential motivations for break-ins. During major incidents, Gary Robinson, head of Visa's IRT, recommends daily briefings to keep everyone in the loop.

All of the resources gathered in creation of the IRT may be needed here, including community contacts, policies, technology, and staff. Robinson said, regarding one incident, "we had ten people in a room twenty-four hours a day for two weeks just to analyze logs." Seizing evidence & maintaining appropriate logs, keeping/maintaining relevant attack info is incredibly important. The point of contact will keep a database of incidents, which should generate statistics, such as number of incidents (open & closed), number and type of queries received, time incidents require before closure, trends, etc.

The tricky part is determining who to notify, and when. This includes everyone in the organization or designated IRT community: staff (trusted & technical experts - ops & programming, communicators), administrative support, management, customers, service providers, legal authorities, and the community network (experts, other IRTs, vendors, etc.). Privacy in this area is a sticky topic. Many incidents are not reported to CERT or the FBI; however, especially by larger corporations, because it is in their best interest to appear secure to customers. For example, consider the bank that's been attacked five times in the past year. They could lose a great deal of business through the press alone.

After a decision is made, responses must be processed. Preparation of press statements and other follow-up procedures occurs. Advisories should be created at this time. If law enforcement is involved, the legal process begins and all evidence will be required. Supposedly, collaboration of intelligence agencies is improving, so the future may hold more convictions.

The bottom line is that general awareness is increasing, and as a result, organizations are becoming more tuned into security needs. Building and deploying IRTs is the next logical step for organizations that have not yet done so, and along the way, FIRST and its member organizations, like CIAC, are there to help everyone recover from security incidents and disasters. "Success is making our customers happy, providing them with whatever it is they need to get on with their business," says Sparks.

References: Hafner, Katie & Markoff, John Cyberpunk: Outlaws and Hackers on the Computer Frontier, New York: Simon & Schuster, 1991, p. 321.

Relevant Links

[ARIS](#)

SecurityFocus

[SecurityFocus Incidents Mailing List](#)

SecurityFocus

[Computer Incident Advisory Center \(CIAC\)](#)

CIAC

[Forum of Incident Response and Security Teams \(FIRST\)](#)

FIRST

[Privacy Statement](#)

Copyright 2006, SecurityFocus