Avoiding the Trial-By-Fire Approach to Security Incidents

By Moira West-Brown
Computer Emergency Response Team (CERT®) Coordination Center, Software Engineering Institute

Being proactive about security is critical to mitigating your security risk. However, having good security measures in place will not prevent you from suffering computer security incidents. So it is also important to be prepared and proactive about detecting and responding to such incidents when they do arise. This article explores the range of options that exist in organizations today for detecting and responding to security incidents.

Some Just Get Burned

Experience shows that most organizations do not think about how to respond to a computer security incident until after they have been hit significantly. They have not assessed the business risk of not having formal incident-detection and response mechanisms in place. More often than not, organizations receive reports informing them that they are involved in an incident originating from some other party rather than identifying the incident themselves. This is called the trial-by-fire approach.

The problem stems from a lack of organizations recognizing their need for a comprehensive security infrastructure. It is not until after an ill-prepared organization has suffered a significant security incident that business risk and impact are realized. The management may perceive that network and host security is something that the system and network administrators handle as a part of their day-to-day activities. Or they may think that security is handled by the organization's firewall.

Sadly this perception is often incorrect on both counts. The staff priorities are primarily focused on maintaining basic support and operation of the vast amount of computing equipment in place. Firewalls may prevent some attacks, but cannot prevent all attack types; and, if not correctly configured and monitored, they may still leave the organization open to a range of others. This approach, or lack of one, results in significant problems such as:

- Not knowing if or for how long a network or systems have been compromised.
- Not knowing what information is at risk, has been taken, or has been modified by intruders.
- Not understanding methods perpetrator(s) use to gain access to systems.
- Not understanding what steps can be taken to stop the intrusion activity and secure the systems and network.
- Not identifying in advance any possible adverse effects incident response actions may have on the company's ability to conduct business.
- Not knowing who has authority to make decisions related to containing the activity, contacting the legal department, law enforcement, etc.
- Delays in identifying and contacting the right people to notify about the activity (internally and externally).
- No recognized reporting contact in the organization known to external or internal parties.

The Volunteer Approach

Some organizations have system and network administrators who are either interested or trained in computer security. Such individuals are better prepared to address security within their domain of authority—such as the machines in one department or operating unit, or the equipment on a given network segment.

Within some organizations, various individuals may be working together to address security needs informally. This approach often stems from a group of individuals in the organization who see the need to address security even if the need is not recognized by higher level management.

However, even having capable people available does not mean that the organization is prepared to respond. Depending on the scope of the overall volunteer effort, it is likely that even with intrusion-detection software in place in parts of the organization, serious network security incidents may still go undetected. Although this approach is a marked improvement over the trial-by-fire approach, significant problems still remain, including:

- Serious intrusions may still go undetected.
- Volunteers may be able to deal with the technical issues, but may not understand or have the information available to assess the business consequences of any steps taken.
- Volunteers may not have the authority to apply the technical steps (e.g., disconnecting the organization from the Internet) or other actions they believe are necessary (e.g., reporting the activity to law enforcement or seeking the advice of legal counsel).
- Volunteers may delay seeking and obtaining management approval to respond.
- Volunteers have no bigger picture of the overall detection and response activity.
- Volunteers may know in some cases whom to contact internally, but anomalies may exist.
- Other individuals in the company who identify a possible security incident may not be aware of the informal group and may fail to report to it.
- An informal group is unlikely to have external recognition and support.

The Company-Supported Approach

Despite good intentions of technical experts or other staff members, the only effective approach to incident detection and response is to make it part of an organization-wide risk-management plan founded on the highest level of management support. Regardless of how such an approach is implemented—whether by a geographically distributed or centrally located team consisting of full- or part-time staff, or supplemented with contract support—without management support the effort will struggle to succeed. In addition to the foundation of management support, the empowered group must also be recognized internally and externally and prove its effectiveness, trustworthiness, and ability to everyone.

Management authority and recognition are the foundation for success. But

an effective detection and response service needs the trust and respect of the constituency served and others with whom the service will need to interact.

Teams established to address incident detection and response for organizations are known as computer security incident response teams (CSIRTs). Forming, staffing, and operating a CSIRT is not easy. However, if appropriately set up and empowered within an organization, a CSIRT can begin to gain the trust and respect necessary to address incident detection and response from a company-wide perspective.

CSIRTs vary in structure, staffing, and the range of services provided based on the situation or need that they are trying to fulfill. Consider the need for a CSIRT in your own organization, whether it is company wide or just for your business unit or department. A recently published handbook is available at www.sei.cmu.edu/publications/documents/98.reports/98hb001/98hb001abstract.html to help an organization determine the scope and range of services for a CSIRT and provide guidance in forming operational policies and procedures.

Advocating the Company-Supported Approach

Making the transition from a trial-by-fire or volunteer response effort to a company-supported one is not easy. The most important and often the most difficult challenge is convincing management of their need for an effective and empowered CSIRT as part of an overall risk-management approach.

Waiting for a serious security incident to occur within your organization to convince management of the need is not a productive approach. Nor will it necessarily be successful. Even after suffering a serious computer-security incident comprimising hundreds of systems, some organizations still do not recognize the need for a formal incident-response capability.

I remember one case in which I contacted a multinational company to provide information indicating that an intruder was gaining access to the company's corporate network through the Internet. As a result of the report, the company began to look at its systems and found that they had been seriously compromised for more than six months. The company was able to identify many systems and internal networks that were compromised by the activity along with the sensitive information available on those systems. But it had no idea of the intruder's motives or the extent of the data that the intruder had copied or amended. A significant period of time elapsed and further compromises occurred before the organization established a CSIRT.

"It is only a matter of time before insurance companies begin to request more information about network security and to raise the cost of general insurance coverage for companies that are ill prepared to detect and respond to computer security incidents."

Another organization that was compromised by an intrusion reinstalled all of its systems from known good backups—losing two weeks of production effort in the process—as they could not be certain what data might have been tampered with by the intruder. In this case, malicious modifications to the application under development could have resulted in loss of life if the application had failed during use. The organization involved promptly established a company-supported CSIRT.

One of the most important factors to document is the associated business risk or loss of any incident. This information must be presented in a form that will help management understand that the problem is a business one and not a technical one. I recall one case in which technical staff had great difficulty in gaining management attention regarding ongoing intrusions. It was not until the intrusion data was presented by describing the mission of each system in question rather than providing its host name and operating system version that management paid attention. Volunteers should attempt to document and present to management the impact of known intrusions and recorded losses.

The Insurance Influence

I learned of one situation recently in which a security officer compromised the home system of a manager as a last resort to gain management recognition of the company's security risk. For the majority of us, such extreme measures are far too dangerous. In such cases, financial pressure from another source may be a last resort to gain management's attention. Pressure from insurance companies (seeking to limit exposure of losses resulting from network security incidents) will provide a financial incentive for organizations to improve security measures to keep insurance premiums affordable.

I was involved in a recent insurance application where an insurance company requested information on what policies an organization had in place for virus prevention and control of defamatory or libelous information on public Web sites and mailing lists. Conspicuous by their absence were questions seeking an understanding of how well prepared the organization was to prevent, detect, and respond to computer security incidents—even if only from the perspective of preventing viruses or defamatory or libelous information being published on a public forum.

It will not be long before insurance companies are asking the right questions in this area. In fact some already are, but their motives are slightly different. Just recently some insurance companies have begun to offer policies that provide organizations with financial protection for third-party damages resulting from network security breaches. A prerequisite for such coverage is an associated network security risk assessment.

It is only a matter of time before insurance companies begin to request more information about network security and to raise the cost of general insurance coverage for companies that are ill prepared to detect and respond to computer security incidents. Eventually, trial-by-fire or financial incentives will force organizations to realize the need for a CSIRT.

Be Prepared

It is still not uncommon to find callers to the CERT Coordination Center hotline who do not know what steps to take to report an incident within their own organizations. Although many callers know their vendor and maybe even the organization's Internet service provider,

very few know to whom they should report a computer security incident. Being prepared and knowing what to do in advance can help to further mitigate the damage. That is why it is very important that an organization advertise its CSIRT both internally and externally. As with emergency services, it is important to find out how to contact a CSIRT before it is needed in an emergency. It is also important to know in advance whom the service can help and what information is needed to ensure that the CSIRT can provide the service requested.

To find out if your organization has a company-supported CSIRT, ask your security officer or system/network administrator, and consult your organization's security policies and practices. Some CSIRTs are members of the Forum of Incident Response and Security Teams (FIRST). See www.first.org/ team-info for a list of FIRST members and their contact information

With millions of organizations now reliant on networks to conduct their businesses, it is a shocking fact that only a few hundred CSIRTs exist around the world today. Many of these CSIRTs continue to cite annual increases of 200 percent or 300 percent in the numbers of computer security incidents reported to them. They are struggling to keep pace with the number of incoming reports. Even with general improvements in the field of network security, a dramatic increase in the number of CSIRTs is urgently needed. More advocates are needed to help organizations understand the risks associated with the failure to detect and appropriately respond to computer security incidents.◆

About the Author

Moira J. West-Brown is a senior member of the technical staff within the CERT® Coordination Center at the Software Engineering Institute. She leads a group that aids in forming new CSIRTs world wide. Active in CSIRT internationally, she has developed a variety of materials on operational and collaborative CSIRT issues. She was elected to the Forum of Incident Response and Security Teams Steering Committee in 1995 and is currently chair. She holds a bachelor's degree in computational science from the University of Hull, United Kingdom.

Open Forum

Security Often Sacrificed for Convenience

By Shawn Hernan
Vulnerability Handling Group, CERT® Coordination Center

When given a choice between a product that is secure and one that is not, nearly everyone will say they would prefer the secure product, all else being equal. But things are not equal. Despite clients' cries for more secure products from vendors, when it comes to writing the check security often gets the short end of the stick.

The Message Clients Send

One e-mail product vendor has been among the market leaders in implementing security features into its products. This vendor, who ships both e-mail servers and e-mail clients, was among the first to add a particular kind of secure authentication to client and server. As the vendor was among the first to do so, there were concerns about interoperability. Would its e-mail client be able to work with other vendors' e-mail servers, and vice-versa? Would the secure authentication scheme prevent interoperation with other vendors' products?

Complicating matters was the fact that the e-mail protocol did not provide for explicit failure messages when an authentication attempt failed. That is, the client was unable to tell if the authentication attempt failed because the password was incorrect, or because the server did not support the same authentication scheme. Here were possible options if the client received a failure message:

- Ask the user for the password again, assuming it was incorrect the first time.
- Try a less secure but more widely implemented authentication scheme, namely plain text passwords.

In other words, the vendor was faced with a tradeoff between interoperability and security by default. The vendor chose security by default and started to ship the client. The default behavior was to stick with the secure authentication scheme, but give the end user a way to configure it so the client could use a less secure authentication scheme.

The effect of this security-conscious choice was that the client would work only with a server from the same vendor, until other vendors implemented the same authentication scheme. The vendor provided documentation with the product to allow an end user to configure the product to work with other vendors' servers. So the issues of security and interoperability were addressed, but security was primary.

Although the end user could configure the product to work with other vendor's servers, the vendor received more than 280 trouble reports from sites that thought the client was broken or that simply did not want to reconfigure the client. The customers wanted interoperability by default.

This market pressure forced the vendor to choose a different set of defaults—the product will now try less secure authentication schemes if the more secure scheme fails. Thus, if a user makes an error in typing a password, the client will try the same incorrect password using all of the authentication schemes including plain text.

This means that if the user makes a typo in entering a password, the slightly incorrect password is sent on the network in plain text. More importantly, if an intruder is able to convince a user to establish a connection to a mail server of the intruder's choice, the intruder can recover the user's password. The consequence of the customers' demands for default interoperability was that they obtained a less secure product.

Having changed the default configuration of the product, we would expect that the vendor would have received trouble reports from other customers complaining about the less secure configuration. But they received only one such report. The message sent to this vendor was loud and clear—default interoperability is more important than default security.