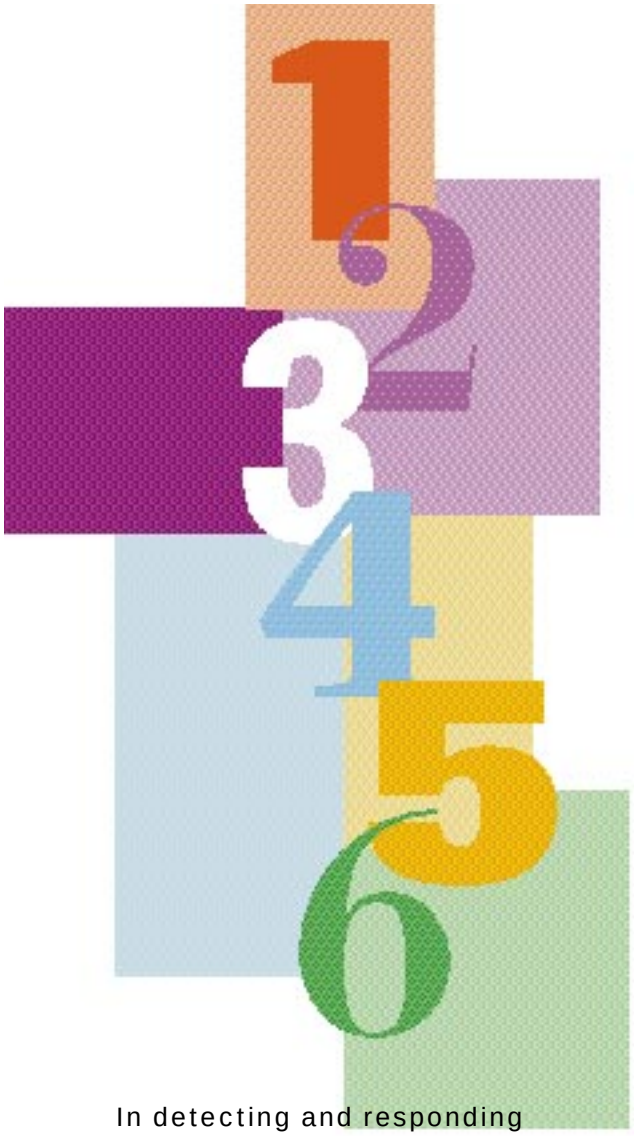


Six Steps Toward a More Secure Computing Environment

In detecting and responding to security incidents, IS professionals need to be at least as well organized as intruders into their systems. Here is a guide for getting ready.

By Jon William Toigo

In this era of open systems and enterprise networks, security intrusions are a fact of life. Concerns over the threat of unauthorized persons accessing confidential corporate data or installing malicious programs that interrupt critical business operations are well-founded. In a recent poll conducted by the Computer Security Institute (CSI) of San Francisco to which some 400 organizations responded, more than half reported unauthorized access into their systems within the last year. Responding to conditions like these, executives spend millions of dollars annually for equipment and software to secure their information assets.

More than anything else, demand for Internet access has heightened corporate risk—and, it is hoped, awareness of it. "More and more companies today connect their internal systems and networks to the Internet. Connectivity makes them vulnerable," says Bill Orvis, a member of the Computer Incident Advisory Capability (CIAC), the U.S. Department of Energy's incident response team based at Lawrence Livermore National Laboratory in Livermore, CA. "Out of 30 million machines on the Net, some are bound to be bad guys."

Orvis and other experts agree that distributed systems—particularly those whose host operating systems are some variant of Unix—are more susceptible than centralized, mainframe-based computing platforms to security breaches. "If a company is using a Unix server, threats to security increase," he says. "Unix services are made available to anyone who knocks on the door. Unix was developed in a collegiate environment where security was not considered very important."

The practical wisdom of experts involved in security incident response may be summarized tersely: Unix was designed to be open and communicative. Few system administrators properly implement what security features are available in the operating system. As a result, these systems are accessible to intruders who possess knowledge of Unix, any of a number of free Unix toolkits readily available on the Internet and the desire to break into the system.

Recognizing the holes in many basic systems, developers have produced a variety of add-in software and hardware. "Wrapper" software that supplements standard user permission utilities in Unix and tracks requests for services is coming into greater use. Firewalls, which shield internal networks from the Internet, are selling briskly. These tools can reduce the likelihood of a successful attack, but, says one expert who asked not to be named, "These tools are enablers, not solutions. Audit logs regularly reviewed are better than tools that are not monitored. A combination of security add-ins, active monitoring and a well-planned incident response strategy is required to provide the best solution. There is no silver bullet."

Forming an Active Strategy

The classic model for computer security has three components: protection, detection and reaction (see "Elements of Secu-

rity") Experts claim that most attention has been paid to the first component, while the other two typically receive short shrift until a security incident occurs.

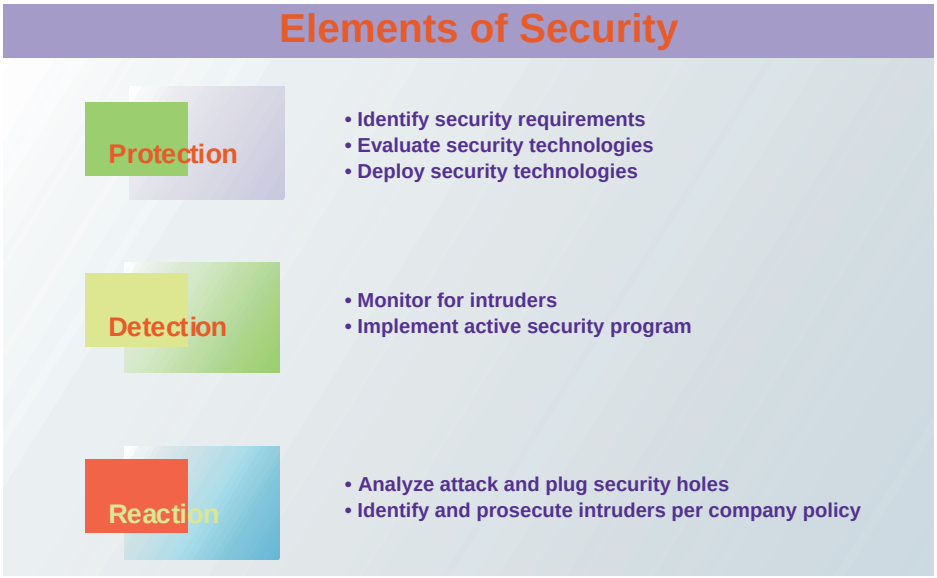
Some observers are concerned that vendors of protection products may be lulling users into a false sense of security. Commonsense thinking assumes that, for every security product brought to market, hackers will develop work-arounds.

Evidence of this claim is readily available on the Internet. CIAC does not publish information about break-in methods, but Orvis says that this information is easily available to hackers through underground bulletin boards and other sources. For example, a group called the 8LGM (eight-legged green monsters) has set up a Web page that identifies holes in commercial security products and provides steps for breaking through the security they provide. "These guys have a philosophy of full disclosure and believe that publishing break-in methods will force manufacturers to plug holes in their products," Orvis explains.

Obviously, protection is an important part of security and can prevent many security intrusions. According to Harold Highland, retired distinguished professor of computing at the State University of New York and author of several books on computer security, "Most people who violate security from inside or outside the organization are innocent wanderers. They stumble into a restricted system and look around at interesting encrypted files. Some security programs and products may keep these wanderers out or identify them so that the hole they have found in security can be plugged."

However, these security measures probably will not prevent serious hackers from accessing systems and may actually weaken security by jading system administrators about the threat. "[Wanderers] are a headache for security people," Highland says. "It's like the boy who cried wolf. The illegal entry to the system may show up on an exception report, but most security people discover quickly that these suspected hacker attacks are duds. After a while, the security people may stop reading the exception reports [generated by their own security products]."

Highland and others agree that effective security must be active. Only through active measures can hacker attacks be detected so a response can be made.



One of the first steps in preparing an active security program is determining security requirements themselves. The company must determine what is at risk and how much security it wants to deploy. The latter decision may be difficult to arrive at. Because security entails the restriction of information accessibility, it runs counter to the bases for most information systems deployed in businesses today. Once decisions are made to prevent certain types of access to certain types of resources, active security measures must be formulated. The following six steps can help an organization to establish a viable program (see "An Active Security Program").

Step 1

Establish Corporate Policy

To respond effectively to a detected attack, policies should be in place before it happens. Specifically, the company needs to articulate what measures will be taken for dealing with systems abuse by internal personnel and for coping with an external attack.

"If security violations occur from an inside source, there needs to be a policy for warning the person, then marking the person's user ID and the files that the person tried to access so that monitors will be notified immediately of any repeated violations," says Highland. "If the insider tries to hack a file or system that he clearly has no access to, it should be policy to fire him on the spot."

To deal with attacks from outside agents, Highland suggests that a worthwhile policy might be first to analyze the attack and plug the holes exploited by the hacker, then to notify the authorities. The latter step especially must be prepared for, he says. "First, you must make sure that management will support pressing charges. There is no point in notifying the district attorney and the local police if no charges will be pressed if the hacker is caught."

The decision to prosecute hacker attacks may not be a clear-cut one for businesses. Some, particularly financial firms, prefer not to publicize shortcomings in their security through a public prosecution. Says Orvis, "I think that this is a bit short-sighted on a company's part. We need to get law enforcement involved, and we need to share information between companies to identify hackers, their methods and possibly the servers where their attacks are originating."

Gene Spafford, associate professor and director of the Computer Operations, Audit and Security Technology (COAST) Laboratory at Purdue University in West Lafayette, IN, and author of the FBI's computer crime primer and books on Unix and Internet security, explains why this decision is complex. "Deciding to prosecute means that you devote time, effort and money to collecting evidence for use in court. Plus, you often need to educate law enforcement and prosecutors about computer crime. This is all expensive, without any guarantee of success. However, there are also compelling arguments in favor of prosecution. For one, prosecuting hackers will help provide protection from future attacks, as it sends a message to other hackers that action will be

taken by your company. Secondly, if enough companies get involved, take action and put some of these people behind bars, we get the point across about how much the community is willing to tolerate. That, in turn, might make law enforcement allocate more resources to developing the capability to fight computer crime. Thirdly, in a large number of cases, companies had no idea how much of their confidential data had been compromised until the hacker was apprehended. It is difficult to recover from a hacker attack without that information."

> Commonsense thinking assumes that, for every security product brought to market, hackers will develop workarounds.

At first glance, establishing a corporate policy on computer and network security may seem to be straightforward. However, formulating policies in a manner consistent with both technical and business requirements may be difficult. The security measures implemented must be balanced against the business's goal of openness, for example. Moreover, security policies may raise thorny questions for corporate culture, including the measure of trust management is willing to place in company personnel and the limits to privacy guaranteed to employees and other end users. Obviously, corporate decision-makers and technical personnel should be involved in the development of company security policy, as well as representatives of the end-user community and possibly corporate legal advisors.

Those seeking assistance in determining the components of an effective security policy may find useful a document available from the Computer Emergency Response Team (CERT). The Internet Engineering Task Force (IETF) Site Security Handbook (RFC1244), can be downloaded from the CERT FTP site free of charge. (For this and other electronic addresses, see "Sources of Security Information and Tools.")

Step 2

Collect Baseline Information

While some companies may wish to decide on a case-by-case basis whether to prosecute hackers rather than writing prosecution into policy, all companies should take proactive measures that will facilitate the detection of intrusions and the analysis of security breaches. To do so requires that system baselines be taken for use in comparisons.

"To monitor for intrusions, you need to know what are normal system events," says John O'Leary, a security consultant and trainer with CSI, based in Plano, TX. "You need to use your audit utilities over a period of time to see what files are being accessed, the routes of access, how they are accessed, by whom and how often. This data should be refreshed at least every six months." O'Leary adds that baseline data should include a system snapshot that provides checksum data for all executables.

"Checksums may not be enough any more," Spafford warns. "Hackers now have tools that can defeat simple checksum comparisons of files they may have altered. Today, you have to create an encrypted signature or message digest for a directory containing sensitive files." A message digest is the result of a program that converts file attribute data into a small output number. Tripwire, a free utility available from the COAST Laboratory Web site, can be used to build a database of message digests for use as a baseline.

Step 3

Monitor for Intrusions

The need for baseline data is clear from the techniques typically employed by hackers to access systems illegally. For example, Orvis describes a sniffer attack. "The hacker enters the system and installs a sniffer program that runs continuously to trap the first 128 bytes of every Telnet session that occurs. This data, which contains the user name and password of the session participant, is stored to a disk file—typically in a secret directory. Hackers like to use the directory name ..[Space] or ..[Tab][Tab], because the Space and Tab keys are invisible. That way, when someone tries to enter the directory using the Unix cd directory name command and types .., the hacker directory will not be accessed. Periodically, the hacker returns and collects his files. He shouldn't let the program run for very long, because the sniffer file can grow very large in a heavily trafficked system and generate telltale OUT OF DISK SPACE error messages.

"If the hacker is able to get the root password, he can take over root command functions and replace the list users (ls) program with a hacker version that will permit undetected access. He may also replace the ps program so that processes he initiates will not be displayed when the system administrator uses the ps command. In short, he creates a back door to the system so he can come and go at will."

In the above scenario, comparing new programs to a baseline program could detect the alterations made by the hacker. However, determining that the hacker has attacked the system at all remains a difficult proposition.

Ideally, intrusion monitoring should be undertaken in realtime—that is, security administrators would monitor 24 hours a day all traffic in the network, all logins to hosts and all activities performed by users while logged on. However, because of the demands they make on systems and personnel resources, this type of monitoring is rarely performed.

Such realtime systems are difficult to deploy in a single host environment. Monitoring for intrusion in realtime consumes operating system resources and may slow system performance. It is rarely implemented in corporate settings except when an intrusion has been detected and the organization is engaged in active information collection. Moreover, realtime monitoring requires that knowledgeable operators be either on-site or available nearby 24 hours per day. Many companies choose not to shoulder this expense.

In a network setting, particularly a network characterized by heterogeneous system platforms, the difficulty and expense of realtime monitoring may be increased several times over. Monitoring in a networked environment may require that

technical problems, such as making the audit utilities of disparate systems communicate with each other, be surmounted. Also, a more sophisticated skill set may be required from the personnel who will monitor the network on an ongoing basis; this increases the cost of the personnel component of the strategy.

As well as being complex, realtime response is simply not a top priority for many organizations. "Most of the current technology for realtime intrusion detection is limited or introduces a lot of overhead onto the network. Users are usually worried more about the speed of their networks than their security," Spafford says. "My response is that you can make a car go 200 miles per hour if you leave off the brakes and the safety devices. But I wouldn't ride in it."

Some third-party products are beginning to become available to facilitate intruder detection. Scott Huitt, senior systems administrator for Motorola's paging products group in Boynton Beach, FL, uses Unishield from Network Information Technology of Saratoga, CA. "We have FTP drop boxes, firewalls and Web server security software, plus publicly available software for login monitoring, to establish our security," he says. "If someone tries to log on without permission, the system pages me within one minute."

Huitt manages the operation of more than 800 Sun workstations and servers at his site and is responsible for the security of company-sensitive pager design and manufacturing data. He says that he has had no major intrusions. "We do not allow outside logins, except by our users who have secure ID cards. We do have a Web server, and from time to time we will get a random hit. We wait for the user to make a second attempt to get past our security before we take any action."

Other realtime monitoring products include NetStalker from Haystack Labs of Austin, TX, and Tripwire from COAST Laboratory, which is being developed as a commercial product for release this year.

In the absence of realtime monitoring, most companies rely on either event notification software or audit logs to detect potential intruder events. "Sometimes the network administrator reviews the system logs and determines something is not kosher," says O'Leary. "This is a bit more difficult to do in a heavily networked environment, since the formats of logs and the logging mechanisms themselves may be different for each host. Plus, there may be problems with event timing or synchronicity between systems to contend with. Conversely, this scenario also makes the hacker's task more difficult. Only the most sophisticated hacker can jump from system to system. The hacker with this degree of sophistication is usually adept at covering his tracks by altering logs or disabling them."

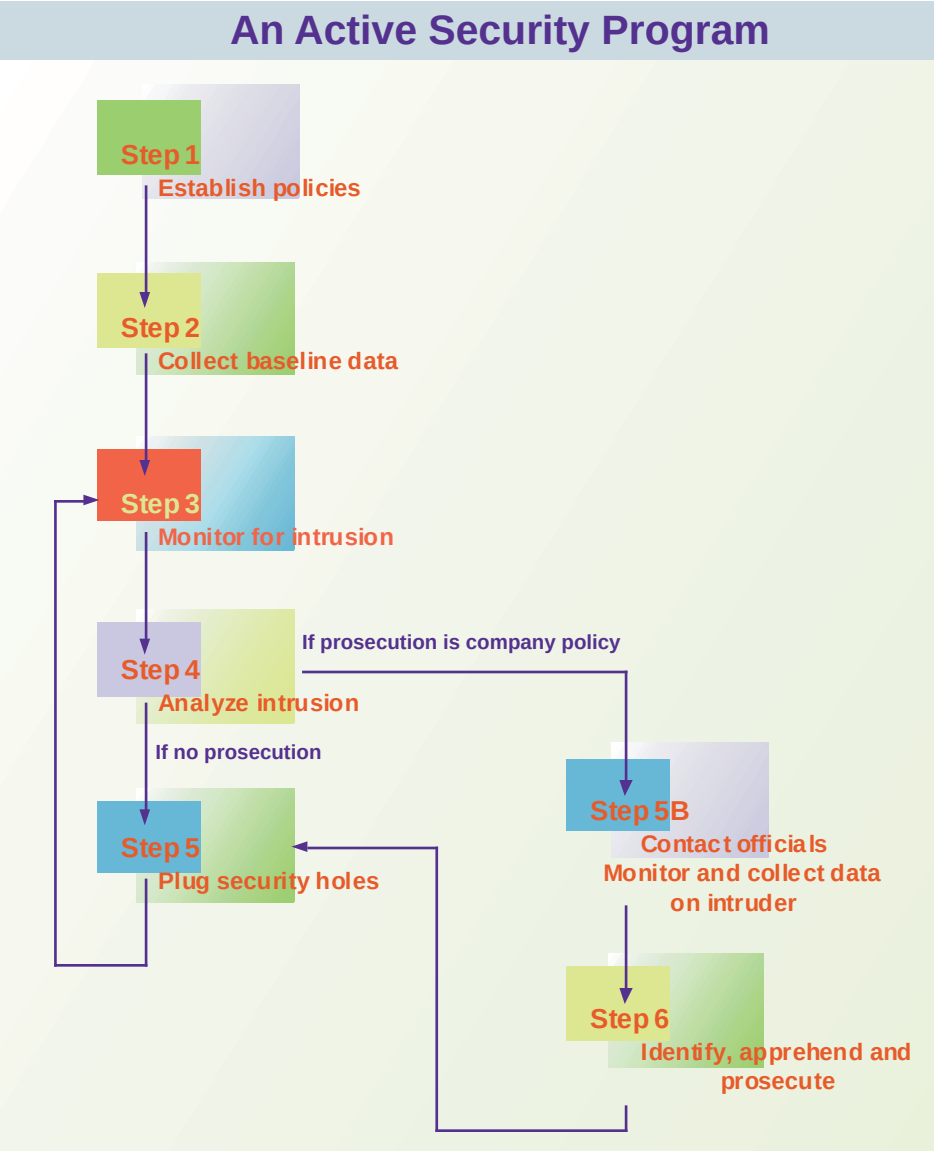
Experts report that widely available utilities often are found in the possession of arrested hackers that will enable the erasure of records in wtemp and utemp system logs. These same tools may be used to browse e-mail and perform other system attacks. They may make the quick detection of a hacker intrusion a difficult proposition.

Often, the triggers for intruder investigations are rather innocuous. End users may report that programs will no longer run—a possible sign that a hacker program is consuming memory; that disk space is becoming scarce for no apparent reason—perhaps a sniffer program is writing its files to a hidden directory; or that permissions on a confidential file have been changed. Troubleshooting to find the cause of the problem may uncover the footprints of a hacker.

Step 4

Analyze Intrusion Data

As noted above, when an intrusion is suspected, comparisons of the system's current state to a baseline state are needed to verify it. A systematic inspection of the system or subnet will be required to iden-



tify impacted files. Some companies, including Motorola, have formed incident response teams tasked with analyzing and verifying the attack. The activation of these teams is a matter of company policy and typically occurs only after all other possible explanations for a suspected intrusion have been eliminated.

"Checksum and message digest comparisons may detect files that have been altered due to hardware or software glitches, or even by end users who have modified software rather than going through formal change management procedures," Spafford says. "In fact, statistics indicate that detected alterations are about 12 times more likely to be caused by these events than by intrusion events."

If an attack is verified, an incident response team (or ad hoc team comprised of systems administrators and staff) may be brought in to determine the magnitude and scope of the incident and to protect the evidence for future use in documenting the event. This team may also have responsibility for sharing information about the event with other response organizations such as the CERT Coordination Center at Carnegie Mellon University in Pittsburgh or the Forum for Incident Response Teams (FIRST).

The incident response team may wish to perform realtime monitoring of the affected system or subnet for a period of time. This way, if the hacker returns, his access method may be more readily determined. This data will help to identify the hacker or provide additional information that will be of use in plugging holes in existing security.

Step 5A

Plug Security Holes

If the intruder is identified and the company does not elect to go forward with prosecution, the active security effort may end with the repair of damaged files and the elimination of security flaws thought to have permitted the intrusion. Backups or original software distribution media may be needed to reinstall trusted applications and data. Baselines will have to be reestablished, and monitoring for intrusion should recommence.

Step 5B

Contact Officials/Monitor Intruder

If a decision is made to prosecute a hacker upon identification and apprehension, the company must notify authorities and formulate strategies for monitoring and tracing the hacker when and if he reappears. It is essential that all data pertaining to the incident be verified and documented in a manner acceptable to the courts. This documentation should include details of the originally detected intrusion event, time and resources expended in preparing a trap for the hacker, and damage to the company from the intrusion. FIRST members often are willing to advise in these mechanics of computer crime prosecutions.

> Prosecuting hackers will help provide protection from future attacks, as it sends a message to other hackers that action will be taken by your company.

Step 6

Identify, Apprehend and Prosecute

A complete incident response may include the identification, apprehension and prosecution of the hacker. In the first step, companies should not be surprised at what they find, says Orvis. "The great majority of hackers are kids. They may be trying to show off to their peers by hacking a system, changing the operating system or grabbing a souvenir. It's unnerving and it leaves you feeling violated, like someone can enter and leave your house at will. Don't be put off. No one will argue with you about wanting to prosecute the kids who broke into your house."

According to Orvis, a smaller number of hackers will be industrial spies. "These people won't spend time stealing passwords. They will target a specific machine and specific files, copy what they want and get out. You probably wouldn't find a trace of them after the initial event."

An even smaller number of hackers will enter systems to leave viruses, says Orvis. Viruses are written primarily for PCs and are generally introduced via software diskettes or bulletin board system downloads rather than by hackers.

Spafford suggests that companies realize that the preponderance of intrusions are not from hackers at all, but from disgruntled employees. "The line between internal and external attack is blurring," he says. "Internal personnel may collaborate with someone on the outside to break into systems and take what they want. Or they may purchase an Internet account and hack their office systems once they have left work for the day. They are in a good position to know where files and programs are and what security protects them."

The Bottom Line

Whether or not the hacker is apprehended, the holes in security demonstrated by unauthorized intrusion must be identified and repaired. Additionally, a company should perform post mortems and document the results for every intrusion event. Information about the procedures used to cope with the event should be gathered from response team participants, reviewed and kept for future use. These lessons can improve incident-handling procedures next time.

The CERT, CIAC, COAST and FIRST Web sites are ongoing sources of the latest accounts of hacker incidents. The methods used by the hackers to penetrate security are rarely discussed in detail at these sites. However, the security systems that hackers have penetrated may be identified, and the telltale signs of the incident may be provided in detail, so security personnel can use the information to review their own systems and networks. If your organization doesn't have a security policy and procedures in place, it surely isn't too soon to initiate them. IT

Jon William Toigo *is an independent writer and consultant specializing in business automation solutions. He can be*

Sources of Security Incident Information and Tools

CERT
Web Site
http://www.cert.org
FTP site
ftp://cert.org/pb/ietf/ssphwg/rfc1244.txt

CIAC
Web Site
http://www.ciac.llnl.gov

COAST Laboratory
Web Site
http://www.cs.purdue.edu/coast

FIRST
Web Site
http://www.first.org

Free utilities are available from the Web pages of organizations such as COAST and CIAC. On the CIAC home page, users can select the Security Tools option to obtain access to free software for a variety of computer and network platforms, including TCPWrapper, Gabriel, Netlog, Courtney, Argus, Watcher and other audit, monitoring and prophylactic utilities.

In addition to Tripwire, other utilities are available from the COAST home page by selecting the COAST Tools option. As with many free utilities, support for these may be limited. Prospective users should perhaps develop contacts with FIRST member organizations or attend sponsored events to learn about the free utilities and their effectiveness.