

## **Establishing Audit Guidance for IT Security: Experience of the U.S. GAO's e\*Security Laboratory**

Information technology (IT) security requires no introduction. It is hard to pick up a newspaper anywhere in the world and not read an article on an IT security problem arising in some software, company, or government. Recently, employees at the U.S. Department of Veterans Affairs and the Department of Transportation lost their portable computers or realized they were stolen. These instances highlight the need for more IT security measures and more effective ones, with an emphasis on employee responsibility.

**IT security is a complex issue, [deleted] with many causes:**

- a dedicated external adversary;
- an outsider just trying to cause trouble;
- a dedicated internal adversary;
- an insider who does not practice good security;
- the weaknesses built into the common infrastructure (for example, the global telecommunications system);
- documented and undocumented weaknesses in software environments and products (for example, Microsoft, Oracle, or Cisco), or
- any combination of the above.

Our purpose in this paper, however, is not to present an exhaustive analysis of the threat to IT systems. Rather, we will discuss how an audit organization can answer the following three IT audit questions:

1. Does the department or agency being audited have security measures in place?
2. Are these measures effective?
3. Can the effectiveness be proven?

These questions are extremely challenging, especially as networks and systems, including individual computers and computer system environments, become more diverse, complex, and interconnected. And although these questions--as well as the findings--focus on IT systems, they are also relevant for information systems in general.

#### How the e\* Security Laboratory Audits

In the United States, the experience of the U.S. Government Accountability Office (GAO) has been that none of the networks or systems we have audited has actually been designed, engineered, and architected with IT security in mind. In addition, all the environments we have audited have evolved over time, adding networks and systems as needed. This evolution poses many challenges to the GAO in answering the three questions above.

To meet these challenges, in 1997, the GAO initiated an effort to develop the in-

house capability to conduct comprehensive technical audits of diverse, complex, and interconnected IT environments that support critical agency functions~~[deleted]~~. This effort, with an initial investment of \$250,000, established the GAO's e\*Security Laboratory, ~~[deleted]~~ but with limited capability and capacity. Through the Laboratory's IT security audits during the past 10 years, the GAO has generated ~~[deleted]~~ important findings by testing security measures, for example,

- in support of the Consolidated Financial Statements of the United States, including all of the revenue collection departments and agencies (for example, the Internal Revenue Service, the Federal Reserve Board, the Bureau of Public Debt, and the Financial Management Service), as well as other large departments, such as Defense and Veterans Affairs;
- in response to legislative mandates and requests of the Environmental Protection Agency, the Department of Energy, and the Department of State, as well as the Federal Aviation Administration; and
- in coordination with the work of the inspectors general at the National Finance Center and the Department of the Interior.

### IT Security Guidance

The GAO's only rule for IT security testing is the same as for doctors who swear the Hippocratic Oath: "Do no harm." The GAO does not test operational or production systems directly. Likewise, the GAO does not do any surprise testing; that is, the departments or agencies that GAO tests all know when GAO is going

to test, what systems are going to be tested, what tools will be used, and from what locations the tests will be coming (that is, the location on the Internet or within the department or agency). Even with all this knowledge, it should be noted that GAO's Security Laboratory team has never been stopped by any security measure. This observation reinforces the point that the tester, like the adversary, has the advantage. A dedicated adversary is hard for a defender to repel. Thus, IT security is not just a matter of technology and its configurations. Fixing a particular piece of equipment or configuration only fixes the individual piece. But having IT security measures in place—while practicing vigilance and diligence—teaches everyone who uses the system to be security conscious. This helps to fix the entire system.

For example, in an attempt to address the problem of weak passwords, a U.S. National Institute of Standards and Technology (NIST) publication has a section dedicated to passwords, including general guidance on the composition, length, lifetime, source, ownership, distribution, storage, entry, transmission, and authentication period for any and all passwords:<sup>1</sup> According to section 3.4.4, “Users that create or select their own personal password shall be instructed to use a password selected from all acceptable passwords at random, if possible, or to select one that is not related to their personal identity, history or environment.” But advising that the user is to be “instructed” to use an acceptable password “at random” does not solve the problem of weak passwords. When a user is found to

---

<sup>1</sup>FIPS-112 (<http://www.itl.nist.gov/fipspubs/fip112.htm>).

have a poor password and a new one is recommended, training and verification must be included.

The audit guidance the GAO uses for IT security testing, including several different aspects, comes from many sources:

- GAO, *Federal Information System Controls Audit Manual (FISCAM)*;
- Information Systems Audit and Control Association (ISACA), COBIT®;
- U.S. Defense Information Systems Agency (DISA);
- U.S. National Security Agency (NSA);
- U.S. NIST;
- International Standards Organization (ISO) 17799; and
- vendor guidance and industry practices (for example, Oracle, Cisco, and ISS).

While the guidance may vary in particular applications or technical specificity, the desired outcome is the same: The consistent management of network and system risk, based in part on effective security measures, that is, internal controls. For example, *FISCAM* addresses six control areas:

- entitywide IT security measures (Is there an IT security architecture in place and a management program that guides it?);
- access controls (Are controls in place that manage access to individual systems and programs, and are they unique and specific to an individual

user?);

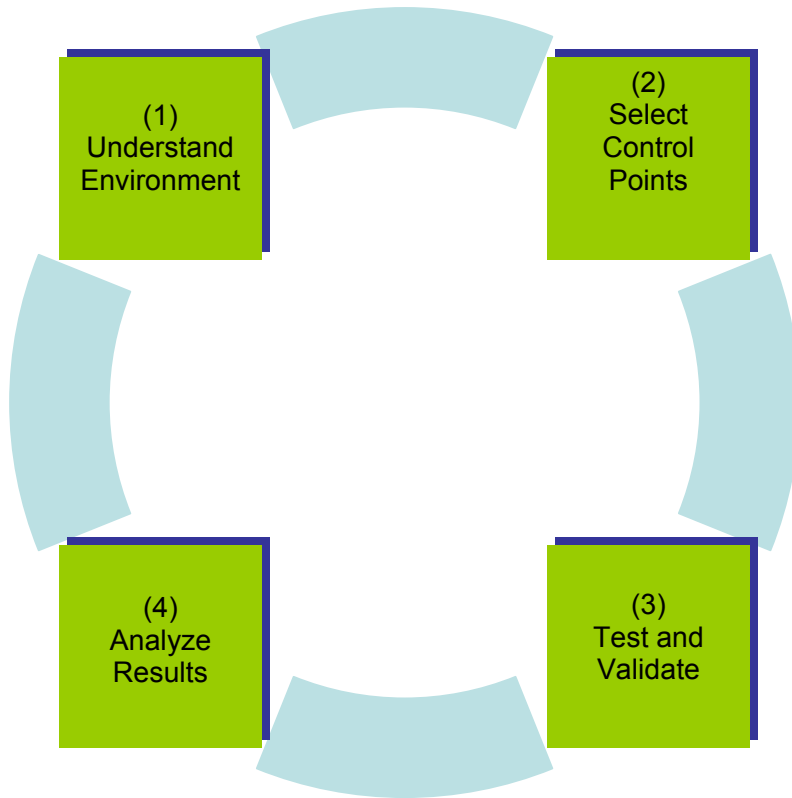
- system software (Are there effective controls in place such that there are environments separate from the production environment for designing, building, and testing new software and hardware?);
- change controls (Are there effective controls in place, so that standard configurations of systems are maintained with effective reliability?);
- service continuity (Are the systems able to recover from an interruption in either power or service, without corruption of either the system itself or the information?); and
- segregation of duties ( Are the security authorities distributed, so that no individual has more authority than he or she needs?).

### Methodology

While the specific audit questions or lines of audit questioning may vary according to the different guidance sources, the methodology cycle is similar: (1) understand the environment; (2) select control points; (3) test and validate, using automated tools where needed and selecting additional devices or systems for testing; and (4) analyze the results of the testing, in order to better understand the environment and control points. For (3), testing and validating, It should be noted here that the GAO test tools are either freely available or a commercial software. To ensure that our testing would mirror an average user, we have chosen not to use any specialized tools, available only to a specified group, such as the military. And for (4), any and all vulnerabilities must be assessed in the

context of the network and the organization's mission (see figure 1).

**Figure 1: Methodology Cycle for IT Security Audits**



At the GAO, this methodology is usually referred to as active testing. Such testing focuses on a single purpose--to collect information on systems and networks that are currently in use. Through such testing, (1) weaknesses in security measures are shown and (2) recommendations can be made that help improve the security measures of a department or agency at both the management and system levels. In particular, this includes testing a department or agency's ability to

- protect itself against intrusions (Has the department or agency configured its system to defend itself?);
- detect system compromises (Has the department or agency set up an intrusion-detection system that can issue a warning should one of the systems be compromised?); and
- ability to react (Has the department or agency designed its systems to respond to an intrusion, should one be detected).

These tests can also be used for the human, as well as the system, response. For example, having a perfect intrusion-detection system does not effectively meet the criteria for security measures. A system operator who can be notified at any time, in order to take some action, must be available. And this action taken is not complete unless and until some law enforcement agency has been contacted and a criminal investigation has been started. But the majority of organizations the GAO has tested define the action taken as purely defensive: Repel the attack and the intrusion is over. However, this defensive action does not show that the organization understands that the information being collected during an intrusion is evidence, both for the investigators as well as for the auditors. An organization can say they have defended against an attempted intrusion, but have no information to prove that the attempt took place or corrective action was taken, including putting in place security measures to avoid that type of intrusion in the future.

Tests must cover both the internal and external threats. Even though the risk of external threat is constantly increasing, the damage that can be done by an internal threat (such as a dishonest employee) is still, in our experience, of greater potential damage. This is because the insider's knowledge is so detailed and may cover

- the relative importance of the systems and networks and
- a clear understanding of the thresholds of the security measures; that is, what areas are included in the measures.

Finally, tests must include both logical and physical penetration. While most security tests look only at the IT systems and their related networks, any agency that wants to have a clear understanding of the effectiveness of its security measures should also look at the physical access controls on building information. All anyone needs to do is to look in the trash bins to see what information is being thrown away with the waste from the lunchroom.

The testing itself is divided into three levels or tiers:

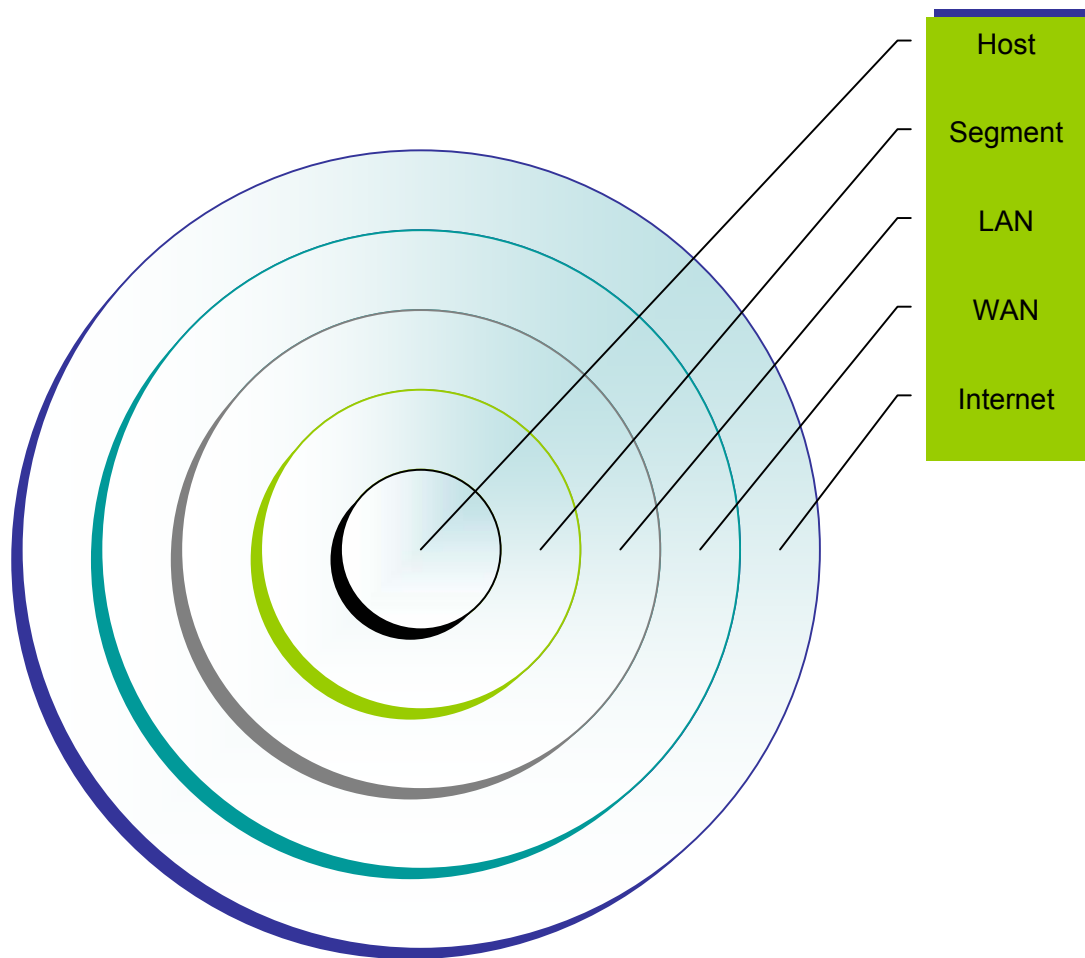
1. the main processing computer (in the United States, this is usually some large IBM or IBM-derivative mainframe computer that handles all the important information transactions for the organization);
2. the network environment, which is usually all the systems that operate the organization's intranet and serve as the bridge to the Internet; and
3. the desktop, including all the computers that are used by the individual

employees for their normal day-to-day work (for example, e-mail, schedules, worksheets, and personal records).

Because of the organization's network, no single tier is isolated from another.

Tier 1, the main processing computer, may handle the most important information. But it is not more important than any other computer or the network itself. A weakness in any interconnected system can have an impact on all the systems that it touches. Tier 2, the environment being tested, can be divided into network-based and host-based testing. The network is defined as any connection (both inbound and outbound) that goes from the world outside the organization to inside the organization and vice versa. A notional view of this can be seen in figure 2, which shows the layers of the network moving from tier 3, the individual computer (host), out to the Internet. One should remember that the information flows in both directions, with many stops along the way. For example, any time a user accesses a Web site to read the daily news, the user is going all the way from the host to the Internet and back again.

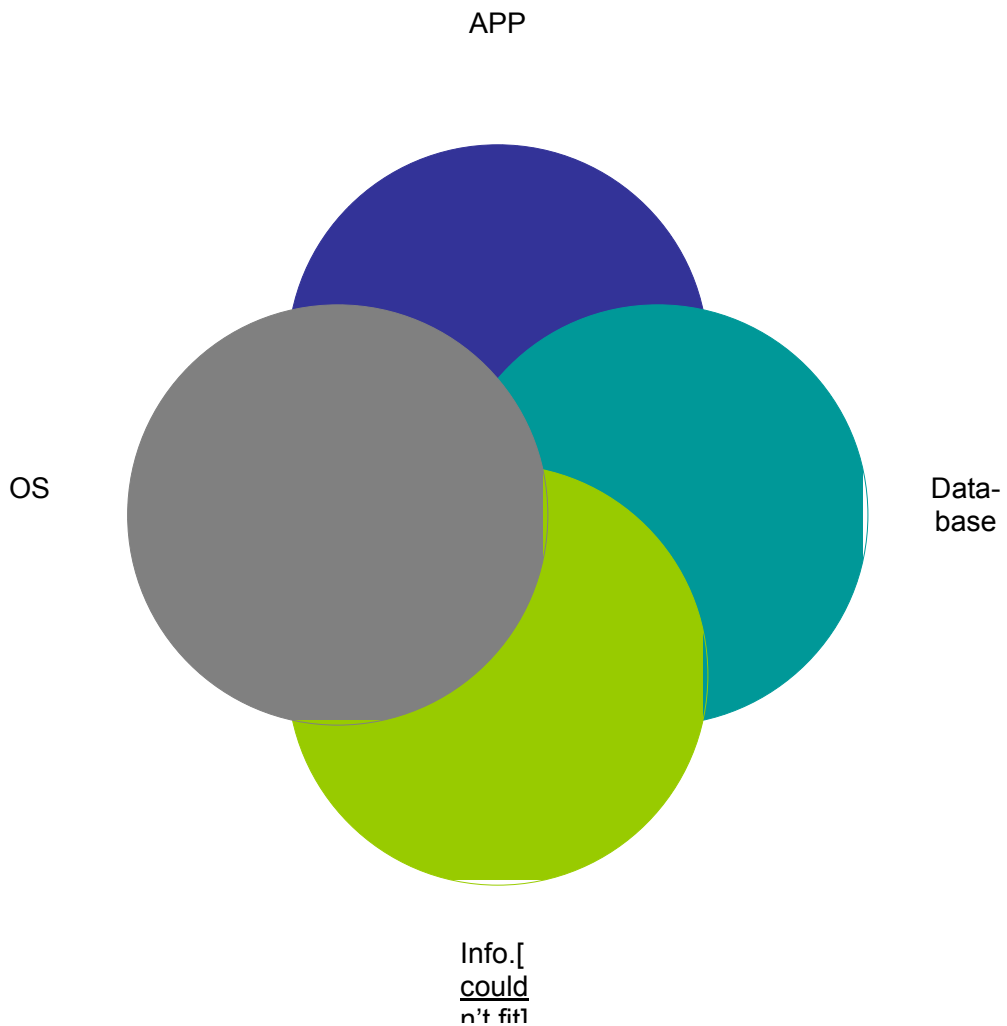
**Figure 2: Layers of the Network**



This information flow also applies to the main processing computers being used by the entire organization, as well as to the computers that are assigned to individuals, as can be seen in figure 3. Here, the application (APP) has a direct impact on the operations system (OS) and the database and the information. Likewise, the OS has a direct impact on the APP, the database, and the information. And both the database and even the information itself have a direct impact on the OS and the APP. This is because today much of the

information that flows has some associated form of internal processing or active content. Thus, just as with the network, no part of an individual computer can be ignored or assumed to be safe and secure.

**Figure 3: Impact of APP, OS, Database, and Information**



### **Findings**

As stated earlier, the GAO e\*Security Laboratory team has always been able to

successfully penetrate the departments and agencies it has tested, indicating that effective security measures are not in place. A successful penetration is here defined as being able to access the department or agency's IT system (either network or hosts) with a level of privilege that allows the creation, deletion, corruption, or modification of the information without the organization's being able to stop these actions. There are many reasons for the team's success. For example, in the area of access controls, many of the organizations tested used default, poor, or no passwords on user accounts and systems. Users gave passwords over the phone or changed them without authentication.

Organizations failed to educate users on what to look for and what to do when a security problem arises, and they allowed untrained or uncertified people to secure systems. In the area of media storage, most organizations did not even think of portable media as a security risk. However, portable media are at an ever-increasing risk, both to loss or theft. When the storage capacity of portable media is considered, the vulnerability posed is clear. For example, if we assume, for purposes of this illustration, that the average government document is equivalent to 360,000 characters and each character is 1 byte, then the following is true:

- 1 high-density disk = 1.44 M characters = 4 books;
- computer memory = 256 M characters = ~712 books;
- 1 ZIP™ drive = 250 M characters = ~694 books;
- 1 hard drive 15 G bytes = 15 B characters = ~41666 books; and
- 1 CD-ROM 600 M characters = ~1667 books.

The relationship between a small USB drive and the corresponding amount of cases of paper is shown in figure 4.

Figure 4: Relationship between USB Drive and Cases of Paper

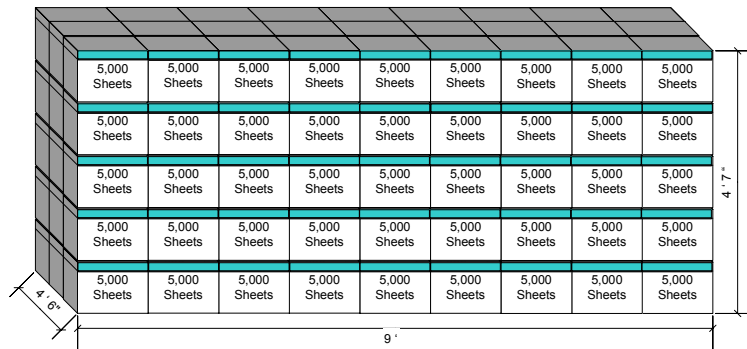
### USB Drive

**Capacity:** Up to 2G or about 675,000 pages  
**Weight:** 1 ounce  
**Portability:** Fits on your keychain



### Cases of Paper

**Capacity:** 135 cases X 5,000 = 675,000 pages  
**Weight:** About 3,375 lbs or 54,000 ounces  
**Portability:** Fits in a tractor trailer



It should be noted that this relationship does not take into account the search capabilities available for computers; these capabilities are not available for paper.

For those organizations that actually do their own security testing, the GAO has found that they usually hire a consultant to perform a vulnerability analysis. The consultant provides a detailed analysis showing 5 to 50 vulnerabilities for every system (We can only assume that 5 to 50 is a number the consultants have decided shows they have done work, but does not worry the client so that the consultant does not get hired again). The organization sends the vulnerability report to the system administrators, with a strong suggestion that the problems should be fixed right away. What usually happens next is that the system

administrators are overwhelmed by the number of tasks and the hours and days required. They do things they know how to do; thus, a lack of knowledge slows progress. And then they are faced with the demands of their regular work, and the boss says “Let’s just get this one project done and then you can go back to the security project.”

It would seem then that concerning security measures, the GAO has only one basic finding, as mentioned earlier: “No one can stop us.” That, however, is not helpful to anyone. IT security is not perfect and can never be perfect, but what can be done to address the lack of effectiveness of security measures?

## **Recommendations**

Government organizations must first understand that they do not control everything they need to control in order to serve the public. The government, like everyone else, is connected to everything. Safety-critical systems are networked, as are emergency communications and the physical infrastructure. Software vendors are not putting security first; thus, if the government is using commercially available software, it is being developed by people the government does not know and there is, therefore, no guarantee that it is being well-engineered. There are not enough skilled system administrators, and there are insufficient background checks being performed on the ones who are in place. Finally, more and more of the systems and help desk functions are being

managed remotely, outside of the organization.

With all of these difficulties, what can a government do? First and foremost, departments and agencies must understand their risk, defined thus: The probability that an adversary will compromise critical information and the impact if the adversary is successful. Here, “adversary” refers to only one type of attack threat. It should always be remembered that carelessness is another type, as dangerous as a dedicated adversary. The risk should be seen as being both human and technological, either on purpose or by accident. If the commercial software that runs a department is flawed deliberately or by accident, the result is the same—the risk is high. The questions an organization should ask are simple:

- What is our mission?
- What or who is our adversary?
- What is the critical information?
- How long can we meet our mission without an update to this information?
- How complicated is it to build (or rebuild) this information?

Once these questions are answered, the risk can be understood and effective security measures, that is, controls, can be put in place to protect the critical information. The security measures that can be put in place to counter these problems cover four areas: management, operation environment, engineering, and legal. For the management area, the recommendations seem almost tautological, First, there must be management; this means that someone in the organization has to be in charge, not just be a position in order to pass the audit.

This person must have both authority and accountability for security. He or she must also be able to make IT security a priority for the organization, so that the security measures are not fragmented, with one group doing what they think is right and another group doing something different. If this person is not in place, then not much else has any hope of working. For the operation environment area, the solutions are all about people. The users--the owners of the information, the ones for whom the systems are built--need to know what their role is in securing the organization's information. If the users do not know their role, they cannot make their concerns known to the engineers. For the engineering area, the engineers are the stewards of the information. The stewards, like the owners, have to understand their role in IT security. Otherwise, they will only solve the problems they see and understand, not the ones that may be most important. For the legal area, the legal authority of the organization must be clearly understood. What steps can legally be taken to protect information, such as suing a vendor for bad software, counter-attacking an adversary, or establishing what constitutes adequate evidence for prosecution. While legal decisions are not simple usually, nor easy to understand, they are imperative for any effective security measures.

For all these four areas, a specific security measure from which any and all organizations would benefit is the establishment of a Computer Emergency Response Team (CERT). A CERT can help an organization ensure that it can protect its information, detect if it has been compromised, and react to any

attempt against its information. The CERT can meet these needs by

- establishing tools and procedures for protecting the information,
- building and operating vigilant and effective systems and programs for detecting unauthorized access to this information, and
- having the ability to react (both operationally and legally) to any intrusions or exposures.

To carry out these activities, a CERT can

- distribute security advisories and tools,
- monitor the organization's network and system, and
- apply direct countermeasures, as well as cooperate with international and domestic law enforcement.

Lastly, a CERT can perform vulnerability testing, which is necessary for testing IT security. These tests must not just focus on technology. They must also focus on

- an organization's public sources (for example, Web pages, newspapers, periodicals, and phonebooks);
- the people of the organization (for example, the help desk staff, the employees, any contractors, and temporary employees or interns), and
- continuity of operations through contingency planning.

While none of this ensures perfect security, the CERT forms a good basis for any

IT security measures.

### **Some final thoughts**

As we have been saying, IT security is a function of people *and* technology, not technology alone. Our testing has shown that no single security standard, vendor, or product can meet an organization's need for security measures. In addition, most security measures do not scale well; that is, something that works well in a laboratory or in a small unit does not easily meet the needs of an operation environment or large department. Likewise, security software vendors are trying, just as government is, to keep up with the newest vulnerabilities and threats of attack; thus, do not assume that a vendor solution will solve a problem forever. It literally has been the case that what worked in the morning did not work in the afternoon. And although the ability to identify and understand system vulnerabilities and attack threats is increasing, the attacks are becoming even faster, as (1) the speed of the networks increases and (2) the software is becoming, unfortunately, more and more complex and vulnerable. Finally, always remember that if a system has not been tested, then it has not been evaluated, and its security is unknown.

Assumptions about security are always dangerous.