Lecture delivered via Vermont Interactive Television to the *Network World Deutschland Security Conference* 9 April 2003

Information Security on a Budget: Where to Invest First

By M. E. Kabay, PhD, CISSP

mkabay@norwich.edu

Professor of Computer Information Systems
Program Director, Master of Science in Information Assurance (MSIA)
Division of Business and Management
Norwich University, Northfield, VT 05663-1035

1 Introduction: why bother with information security?

The basic reasons we care about information systems security are that some of our information needs to be protected against unauthorized disclosure for legal and competitive reasons; all of the information we store and refer to must be protected against accidental or deliberate modification and must be available in a timely fashion. We must also establish and maintain the authenticity (correct attribution) of documents we create, send and receive. Finally, if poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

Another issue that is emerging in e-commerce is that good security can finally be seen as part of the market development strategy. Consumers have expressed widespread concerns over privacy and the safety of their data; companies with strong security can leverage their investment to increase the pool of willing buyers and to increase their market share. We no longer have to look at security purely as loss avoidance: in today's marketplace good security becomes a competitive advantage that can contribute directly to revenue figures and the bottom line.

Part of my job is to collect and analyze above-ground intelligence: news items from news wire services, publications such as NewsScan < http://www.newsscan.com >, reports in the Risks Forum Digest < http://catless.ncl.ac.uk/Risks/ >, BugTraq < http://online.securityfocus.com/archive/1 > and so on. My impression from all of this reading is that non-specialists believe that criminal hackers are the most important threat to information systems security. However, everything I know about information security contradicts this belief. This paper is an attempt to dispel some of the misinformation about security circulating among non-specialists and to provide practical guidelines to managers for significant improvements in securing information.

Another incorrect belief is that security is a one-time effort that can achieve successful protection and then be left alone. As all security experts today agree, security, like quality, is a process, not a static result. With the constant change in technology in today's world, it is inevitable that there will be new threats and vulnerabilities all the time.

Finally, some people believe that security must be a terribly expensive, complicated process. On the contrary, there are some major benefits available from relatively inexpensive measures such as improving corporate culture and implementing defense in depth using relatively simple techniques.

2 Fundamental Goals of Information Security

There are six different aspects of information that we want to protect:

- confidentiality,
- control,
- integrity,
- authenticity,
- availability, and finally
- usability.

These principles are called the "Parkerian Hexad" in honor of the famous information security expert Donn B. Parker, who first identified these six elements as the fundamental goals of information security back in the 1980s.

Let's look at these one by one.

2.1 Confidentiality

Security experts talk about *confidentiality*. Confidentiality refers to limits on who can get what kind of information. For example, you are surely concerned about protecting your enterprise's strategic plans from competitors.

2.2 Possession or Control

Possession or control is another kind of protection for information. If someone were to obtain an unauthorized copy of your confidential data, you'd be concerned even if you knew that the thieves had not yet read the data: they *could* access the data, and that constitutes a breach of possession or control over your information.

2.3 Integrity

Security people next consider the issue of *integrity*. Integrity refers to being correct. For example, data stored on disk are expected to be stable – they are not supposed to be changed at random by problems with the disk controllers. Similarly, application programs are supposed to record information correctly and not introduce deviations from the intended values. Any breakdown that causes unauthorized modifications is a breach of data integrity.

2.4 Authenticity

Another principle of security is *authenticity*. Authenticity means that we should label or describe information correctly. For example, storing contract data on disk that are described as coming directly from a customer when in fact the data were inserted fraudulently by a swindler would be a breach of authenticity.

2.5 Availability

The fifth principle of information security is preservation of *availability*. Availability means having timely access to information. *Timely access* refers to getting hold of the information you need when you need it. For example, a disk crash causes a breach of availability; so do denial-of-service attacks.

2.6 Utility

Finally, the sixth principle of information security is *utility*. Utility means usefulness. For example, suppose someone encrypted data on disk to prevent unauthorized access or undetected modifications – and then lost the decryption key: that would be a major breach of utility. The data would be confidential, controlled, integral, authentic, and available – they just wouldn't be *useful* in that form.

If poor security practices allow damage to our systems, we may be subject to criminal or civil legal proceedings; if our negligence allows third parties to be harmed via our compromised systems, there may be even more severe legal problems.

3 Threats to Information Security

It is very difficult to estimate precisely what causes damage to information systems. Managers should be skeptical of any statistics about information security if they show very precise numbers. The problem is twofold: people don't recognize crimes or damage, and when they do they usually don't report them anywhere that collects statistics. Surveys that report on computer crime and other breaches of security are useful, but all of them suffer from the problems of voluntary compliance — the fundamental question of whether people who respond to questionnaires are representative of everyone in the field even though many people refuse to participate in the studies. Despite these problems, information security experts generally agree on some rough guesses about how damage occurs.

3.1 Internal dangers

Perhaps half of all the damage caused to information systems comes from authorized personnel who are either untrained or incompetent. Another quarter or so of the damage seems to come from physical factors such as fire, water, and bad power. Maybe a fifth of the damage comes from dishonest and disgruntled employees. Computer viruses cause another few percent, and maybe about 5 or 10% of the damage is caused by external attack.

3.2 External threats

The growth of Internet connectivity is altering these statistics. Many systems were once restricted to internal access, with maybe a slow modem or two for remote access by employees. Today we see production systems (those on which organizations depend day by day for continued operations) nonetheless being opened to access via TCP/IP connections from the wider Internet. Many organizations are also linking their systems tightly with those of trading partners using virtual private networks (VPNs) that increase the number of people allowed to access the systems.

Who are the people attacking computer systems? There seem to the two major classes: amateurs and professionals. Amateurs include poorly-supervised children, rebellious and badly-socialized adolescents, and psychologically disturbed or ideologically warped adults. Some amateurs cloak their destructive badly-protected computer systems in the language of social responsibility; they claim to

have the best interests of their victims of heart. Their actions belie their words, however: well-meaning people do not place obscenities and insults on other people's property as these cybervandals do on many a Web site.

Hobbyist attacks have recently become a major problem with the widespread availability of tools for distributed denial-of-service attacks (DDoS). Using these tools, even children can locate vulnerable sites on the Internet, implant special "zombie" software, and then later activate the zombie programs to send streams of spurious requests to one or more selected victims. Under siege from dozens or even hundreds of zombie programs, many such victims are swamped by the volume of traffic and see their response time for real customers and visitors increasing unacceptably.

Professionals are harder to characterize, since there are probably fewer of them and they may be harder to catch; however, some criminal hackers are earning a living with their skills. Some professionals use public and illegal sources of information to help unscrupulous private investigators. Some computer criminals steal credit card numbers and sell them to the criminal underground or participate in theft of services from telephone and mobile-phone companies. An unknown number may be involved in industrial espionage.

The use of Microsoft Office products has greatly increased the vulnerability of users because of Microsoft's decision to include a powerful scripting language at the heart of its word-processing, spreadsheet, presentation, database and e-mail products. E-mail can therefore carry documents that include the equivalent of programs— macro viruses that can not only harm documents but also call system routines and therefore wreak havoc with the operating system, memory and files. Other contributors to trouble include scripting languages used on Web sites (e.g., ActiveX, Java, Javascript) and even the fundamental formatting language of the Web, the HyperText Markup Language (HTML). All of these tools have been misused to harm users.

Some criminal hackers have set up shop as security consultants and offer penetration analysis and consulting services for their clients. There is a serious question about the trustworthiness of people who used to break or skirt the law and now claim that they no longer do so; some security experts argue that leopards have indelible spots, whereas others are willing to believe that there is such a thing as an ex-hacker. I strongly urge managers considering hiring such people to ensure that their contracts include severe penalty clauses if any of their employees are found to be breaching client confidentiality in the course of their duties.

3.3 Attractive targets

Several factors influence the likelihood of attack. For example, a small, obscure tool-and-die company with eight employees is unlikely to be as attractive to any external attacker as a major corporation with thousands of employees and a significant share of its market. It is possible that having a public Web site makes an organization an attractive target for cybervandals. Any site proclaiming its tight security is likely to attract the attention of the amateurs who were trying to prove their prowess; for example, security firms are under constant daily attack. Some amateurs deliberately attack financial institutions and military systems to demonstrate their weakness and ostensibly to force improvements. Finally, some hackers attack sites for political purposes; recent attacks on such victims as Indian nuclear power company Web sites are said to be examples of "hactivisim." However, as mentioned above, with the widespread availability of automated attack tools, everyone has become a potential target regardless of rational measures of attractiveness.

4 Basic Protection

Many security specialists focus on significant improvement to commercial information systems by encouraging basic protection mechanisms. Experts focus on the most important security processes so that clients spend their resources where there will be the greatest return on their investment. This approach is a simple application of optimization theory, from which we know that in any field, there is likely to be a small number of factors that predominate in determining results; some people refer to the Pareto Principle, claiming that 80% of everything is the result of 20% of the causal factors.

The basic problems security specialists see in the field are

- failure to identify sensitive and critical information,
- inadequate security policies,
- poor training,
- inadequate security awareness,
- bad management,
- improper management of security technology,
- inadequate maintenance of security and operating system software,
- failure to detect security breaches and
- lack of preparation for computer emergencies.

It is possible to spend vast amounts of money on all of these issues, but even a modest expenditure of effort and funds can make major improvements in one's security posture. This section looks at some practical ways to get a lot of security for relatively little money.

4.1 Criticality

Above everything else, an organization must know which data and which systems are critical to its survival. It's not possible to manage security without knowing how long you can operate successfully without access to correct information of various types. If you have not already done so, you must convene a working group on information protection that will identify the most important types of data – and the computer software and hardware that safeguard and make those data available for use – and determine whether their critical periods of unavailability are measured in seconds, minutes, hours, days or weeks.

4.2 Sensitivity

How much do you care about whether particular data are known to other members of a work group? To everyone in a particular office? To all the employees in a division? To everyone reading a local newspaper? To viewers of national television? Your information protection working group must also identify the types of sensitivity that concern you so that resources can be applied sensibly. You don't need to protect public information with the same efforts that are necessary for highly confidential competitive information.

Similarly, you need to know the regulatory environment. In Europe, for example, the Privacy Directive has specific requirements for the protection of citizens, employees and clients; inadvertently or deliberately violating those rules may have serious consequences. Your organization must have a clear list of all the requirements that apply to all your sensitive data.

4.3 Policy, Power and Position

Many firms have no security policy all; others have policies that are so old that no one remembers their details (or sometimes even their location). Policies are an expression of an organization's values; if security is relegated to shelfware, employees will act accordingly. Too often, security is an after-thought; someone is assigned the task of managing security but lacks defined responsibilities, has no authority, and can serve solely as a figurehead. One of the most innovative measures in the industry is the recognition of information systems security as a responsibility equivalent to stewardship of financial resources or of operations. The Chief Information Security Officer (CISO) reports at the same institutional level as the CEO, CFO, and CIO. Making the information security officer report to the head of information technology is a conflict of interest; one would not want the chief auditor to report to the head of financial operations; the same principle of separation of duties should apply to security.

In many organizations, people confuse power with personal value; thus the "higher" in the hierarchy someone rises, the more access privileges they acquire. However, a CEO who insists on carrying master keys that let her into every janitor's closet would be seen as acquiring foolish and valueless access privileges. However, some CEOs insist on having access privileges to secured computer or network rooms and to the computers that run critical programs. Such access sends a very dangerous message to everyone in the organization because it encourages other employees to believe that they, too, should have unnecessary access privileges. Stopping this nonsense costs nothing, yet it can have a significant effect on the overall security of the enterprise.

Similarly, some upper managers systematically flout security rules. The CFO and the CIO may promulgate policies requiring everyone (else) to wear identity badges but then refuse to wear their own badges. Naturally, other employees will see *not* wearing badges as a sign of high status. Pretty soon, the entire system of identification and authorization will break down as increasing numbers of employees emulate their superiors and refuse to cooperate with sound security policies. Again, stopping this destructive nonsense costs nothing but can have a major effect on promoting security compliance.

4.4 Training & Awareness

Some organizations make new employees go through training in their first weeks on the job. Unfortunately, fewer organizations bother to continue the process of training. Even if technology were not constantly changing, it would make sense to refresh the memory of employees on critical issues such as security. In addition to formal courses, employees should be stimulated to consider security an intrinsic component of their work. Like quality, security is a process, not an end-point.

We know that many intrusions or abuses of secured systems are accomplished by so-called social engineering: employees are too often willing to give away valuable information to strangers in response to a personable voice and friendly tone. It is lack of awareness that allows criminals to take advantage of innocent and overly trusting people. Security awareness programs should involve committed, repeated germane examples in of security violations in organizational newsletters or bulletins, and occasional security drills that can be turned into an enjoyable exercise in perspicacity and intelligent response.

Although it is true that formal courses can cost thousands of euros per employee per year, there are alternatives. For example, there are many Web sites offering useful information that can serve to advance security awareness and expertise at no cost other than the labor cost of salaries and

infrastructure. Textbooks can be a highly cost-effective tool; one can buy a few copies of valuable texts for the corporate library and have them circulating to many hundreds of employees over the course of a year at minor costs per employee. Videofilms (more usually available now on CD-ROM and DVD) are also highly cost-effective awareness and training tools because they can be used repeatedly by so many employees over the long term. Even bringing instructors into an enterprise to teach can be surprisingly economical if they charge a flat fee regardless of the number of employees.

4.5 Hiring, Management & Firing

Although management issues such as hiring and firing are not as exciting as criminal hackers and industrial spies, it remains true that an organization's security is in a hands of its employees. This area of security management costs relatively little to enforce yet can prevent major headaches.

All applicants for positions with responsibilities for or even contact with corporate information systems should have their backgrounds thoroughly verified. A relatively low-level clerk, for example, might spend an hour or two looking into the accuracy of all the elements of work history listed on a curriculum vitae. Did the person really work there? Is the title correct? Is the description of the person's responsibilities accurate? Did the person truly graduate with a specific degree from a named educational institution? Did the person actually successfully complete a training course or achieve a named certification? These checks need not even be completed at the time of hiring as long as the employment contract stipulates that any inaccuracies or misleading information may be grounds for dismissal. The total costs of such verification are minor compared with other security measures.

Managers should remain sensitive to changes in behavior in their employees; the classic sign of crooked employees is exaggerated fear of being absent from the systems they are diddling. All employees should be required to take their vacations; one wants to see that systems continue functioning normally in the absence of any specific person. The expenses associated with vacations are already factored into budgets; thus the marginal cost of enforcing them should be zero. If the marginal costs are *not* zero, then the organization is allowing excessive dependence on individual employees and is putting itself at increased risk of damages should such a linchpin employee be run over by a bus, decide to leave, or decide to embezzle millions of euros.

When employees, contractors or subcontractors are fired, it is essential that information security staff protect corporate resources against future unauthorized access by these ex-employees. Such procedures must be applied uniformly and require only an hour or so of time by managers and security personnel. How much does it cost for the 60 seconds required to inactivate a user ID? For the 30 minutes to accompany a fired employee to his or her desk and supervise as the person removes personnel effects and returns such corporate property as personal computers, smart cards and identification badges? The payback by avoiding future trouble for such minor expenses is potentially enormous.

4.6 System Administration

This is not a place to discuss technical aspects of security in detail. Managers should fulfill their legal and professional obligations by supporting technical staff at least for basic system hygiene: establishing a sound security architecture; staying up to date in the versions of security software and operating systems; monitoring intrusions using widely available auditing and intrusion-detection software; and establishing computer emergency response teams so that the organization can intelligently respond to accidents and attacks.

One of the least expensive security measures available to anyone is anti-virus software. The consequences of virus and worm infection can be devastating, and so making sure that every workstation in the organization is fully protected can prevent disasters that would cost hundreds of thousands of euros. Be sure that all such anti-virus products are configured to update themselves completely automatically. Put a note on your administrative calendar to be sure that the update licenses are renewed before they expire. Such protection is very high on the list of cost-effective, inexpensive security measures in today's interconnected computing environment.

4.6.1 Establish Effective Security Configuration

Proper configuration of security devices costs very little, yet without it, huge investments in hardware can be completely useless.

Any system with links to the Internet should have a properly-configured firewall to implement security policies governing access to corporate data. A firewall is a device that filters packets to and from the Internet, allowing control over what kinds of commands can be carried out on corporate systems by remote users.

Many firewalls are improperly configured; many Internet-visible systems are often undocumented and therefore poorly protected.

Software firewalls are also available for individual computers and should be installed on all laptop computers in particular. All employees connecting a corporate laptop computer to a hotel-room cable modem must have a firewall in place to prevent other people on the same network from penetrating their files. These firewalls can also be a useful way of alerting top management to the reality of security breaches on the Internet: just set their alert functions to maximum and watch the warnings pop up every few seconds. They'll beg you to turn off the warnings, but the message will definitely get through: the Internet is a dangerous place if you're not protected.

Another frequent problem in network design is that there are no internal barriers to access; firewalls should be placed strategically within an organization to reduce violations of security policies by employees and to limit the damage that can be caused if the external firewalls are breached.

Finally, be sure that configurations are modified to suit new requirements of your network topology and changes in your security posture.

With the growing frequency of Internet-wide distributed denial-of-service attacks, organizations with critical e-commerce applications will find that investing in dynamic anti-DDoS technology placed in front of the firewall to deflect attacks can be a cost-effective method of preventing disastrous downtime.

4.6.2 Maintain Software

Perhaps the single most important problem we face in managing security is that system personnel fail to keep their software up to date. Almost all the intrusions carried out by criminal hackers take advantage of known vulnerabilities.

Every system manager must subscribe to the alert services from their vendors and from the Computer Emergency Response Team Coordination Center (CERT-CC at < http://www.cert.org >) and must implement all security patches as soon as possible. Another invaluable source of information is the Common Vulnerabilities and Exposures (CVE) database best accessed online through the free ICAT Metabase < http://icat.nist.gov/icat.cfm > run by the US government; this service is free and it allows a system manager to search for known vulnerabilities and patches specific for a particular operating system and version.

Failing to heed the free warnings from CERT-CC and one's own vendors is simply asking for trouble. In my opinion as a non-lawyer, there is no excuse to fall behind in keeping up to data on patches. Such failure to keep current constitutes negligence.

There is, however, a practical concern about installing patches, especially in large networks: there is considerable effort required for manual installation of software on thousands of desktop systems or servers. To save money, big organizations will find it helpful to invest in configuration management software that can, for example, generate a disk image of the authorized configuration and install it (after testing) on all connected workstations overnight.

4.6.3 Detect Security Breaches

One of the changes in the security paradigm over the last few years has been a realization that we will not succeed in achieving perfect security. Our perimeters will be breached; authorized personnel will make mistakes; there will occasionally be problems stemming from dishonesty or from revenge. It is therefore appropriate for us to detect such breaches and be prepared to respond intelligently to them.

The least responsive approach to detecting problems is to examine log files or audit trails. The disadvantage of this approach is that one detects problems long after they have occurred. A better tool — one that complements a good audit trail — is a modern intrusion-detection system (IDS). These software tools identify unusual patterns of system use. Depending on their sensitivity, they can flag anomalous behavior by internal personnel (e.g., having an accountant login to the financial system at three in the morning) as well as spotting intruders by recognizing attack profiles. Such software can be programmed to alert system management to a potential problem using a variety of tools; e.g., alarms, e-mail, pagers and even telephone calls. In the long run, a good, well-tuned IDS can save an organization far more than its installation cost and license fees the first time it detects an intrusion early enough to stop a destructive attacker.

4.6.4 Respond Intelligently

There is no point in detecting a problem if we don't have a response in hand. A computer emergency response team (an internal CERT — distinct from the CERT-CC) should be in place before there is a direct need for it; an emergency is hardly the time during which to define and refine procedures. The CERT should include legal staff with expertise event damaging the evidence that law enforcement will require for effective prosecution of the malefactors. Emergency response involves more than a technical battening down of the electronic hatches; organizations should prepare for liaison with law enforcement authorities and have a well-organized public relations plan to keep employees, stockholders, and the public accurately informed of events when conditions allow such disclosure.

The work that goes into preparing and honing the CERT is directly usable in a related area – the disaster recovery plan (DRP). DRPs extend beyond the computer intrusion to look at all kinds of disasters – fire, flood, earthquake, chemical and biological weapons, and so on. The DRP incorporates business continuity planning (BCP) as an extension of the immediate response to disaster; effective DRP and BCP can make the difference between continued survival of an enterprise and its demise.

Some organizations include mechanisms for entrapping external attackers in simulated areas with supposedly sensitive information; these so-called honeypots give the CERT and law enforcement experts more time to locate the intruders and plan for their arrest. All of these plans have to be sought through and tested many times for they are used. Ideally, the CERT will be part of the corporate disaster recovery team because so much of their work will overlap. However, many aspects of the CERT plans must remain secret to maintain effectiveness against internal attackers.

Unfortunately, there is no way around the expense involved in all CERTs and disaster recovery teams. These are not low-cost activities; they involve thousands of hours of work by the most knowledgeable and experienced employees in the enterprise. On the bright side, many organizations have found unexpected side-benefits from DRP and BCP such as increased internal communications, increased team-spirit, improvements in business processes, and new friendships that improve productivity and atmosphere.

4.7 Use Independent Security Evaluations

Many organizations recognize the benefits of using formal guidelines and methodologies from neutral third parties in establishing their security policies. Some groups have never developed policies; others have been unable to devote enough time to maintaining those policies. Sometimes the information technology staff lack expertise in information security; other times upper management have refused to support the measures known by the staff to be important for protecting corporate information assets. In all these cases, external organizations such as consultants, professional associations and certifying authorities can serve a useful purpose to alter the corporate culture and make the best use of security expertise.

As in the case of DRP and BCP, such efforts are not cheap, but they may be cost-effective measures for some organizations and can be cheaper than the consequences of remaining unprepared and disorganized.

5 Concluding Remarks

In summary, managers must understand that security cannot come by buying and installing a gadget, no matter how good. Security is a process, much like quality assurance. Security can and must be woven into the corporate culture of every organization, with due attention to the changing landscape of market advantage, threats, vulnerabilities, risks of damage and extent of damage. The most important measures may cost very little to implement and can materially improve security even more than equivalent expenditures on isolated technical components of security gear.

6 For further reading

- The German BSI (Bundesamt für Sicherheit in der Informationstechnik) has a wonderful Web site at http://www.bsi.bund.de/index.htm that includes extensive security policy documentation in German and in English.
- For a single-volume compendium of information security principles and practice, see

  Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook, 4th Edition*. Wiley (New York). ISBN 0-471-41258-9. 1200 pp. Index.
- For a comprehensive list of information security resources, see < http://www2.norwich.edu/mkabay/overviews/infosec_ed.pdf >
- Check out M. E. Kabay's INFOSEC Newsletters archived on the NetworkWorld Fusion Web site at http://www.nwfusion.com/newsletters/sec/