By Michael E. Whitman

A firm can build more effective security strategies by identifying and ranking the severity of potential threats to its IS efforts.

Enemy at the Gate: Threats to Information Security

"Know the enemy, and know yourself, and in a hundred battles you will never be in peril" [5].

These prophetic words, spoken over 2,500 years ago by renowned Chinese general Sun Tzu, ring true for the battlefield warrior and information security administrator alike. Knowing the enemy faced by information security is a vital component to shaping an information security defense posture. The press routinely publishes dramatic reports of billions of dollars lost to computer theft, fraud, and abuse. The 2002 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) survey on Computer Crime and Security Survey found that 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the last 12 months. The report documented that 80% of respondents acknowledged financial losses due to computer breaches, a total of approximately $455,848,000 in financial losses, up from $377,828,700 reported in 2001. Respondents citing their Internet connections as a frequent point of attack rose from 70% in 2001 to 74% in 2002 [3].

Security researchers warn: "Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary" [4]. In order to strengthen the level of protection of information in the organization, those responsible for that information must begin with an understanding of the threats facing the information, and then must examine the vulnerabilities inherent in the systems that store, process, and transmit the information possibly subjected to those threats. The first part of this strategy is the identification of the dominant threats facing organizational information security, and the ranking of those threats in order to allow organizations to direct priorities accordingly.

Sadly, IT executives have frequently identified the security of information as an important but not critical issue [4]. IT executives reportedly dropped information security as an important issue altogether in 1995, suggesting either they felt they had sufficiently addressed the problem, or they no longer felt it was as significant as other issues [1].

Profiling the Enemy

Changes in the identification of threats, in the rollout of new technologies, and the identification of new threats may have dramatically shifted the organizational security focus. In an attempt to better understand the threats facing organizations, this study examined three questions: *What are the threats to information security? Which of these threats are the most serious? How frequently (per month) are these threats observed?*

In order to identify the threats to be assessed, the study identified a dozen categories of threats by examining previous works and publications and by interviewing three chief information security officers. These categories are:

1. Act of Human Error or Failure (accidents, employee mistakes)
2. Compromises to Intellectual Property (piracy, copyright infringement)
3. Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection)
4. Deliberate Acts of Information Extortion (blackmail of information disclosure)
5. Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)
6. Deliberate Acts of Theft (illegal confiscation of equipment or information)
7. Deliberate Software Attacks (viruses, worms, macros, denial of service)
8. Forces of Nature (fire, flood, earthquake, lightning)
9. Quality of Service Deviations from Service Providers (power and WAN service issues)
10. Technical Hardware Failures or Errors (equipment failure)
11. Technical Software Failures or Errors (bugs, code problems, unknown loopholes)
12. Technological Obsolescence (antiquated or outdated technologies)

The next step was to develop an online survey asking IT executives to rank the threats to information security; to identify the priority of expenditures to protect against these threats; and to indicate the frequency of attacks attributed to each category.

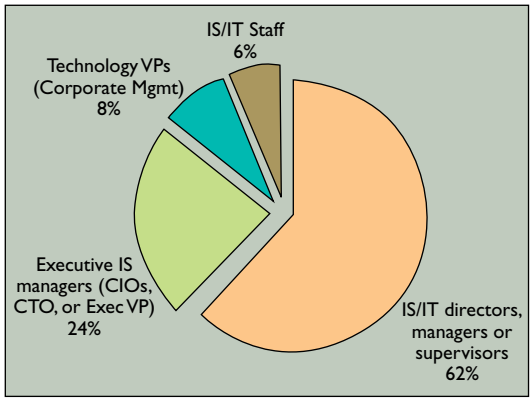

Figure 1. Respondents by position.

As expected, the respondents were predominantly IS directors, managers, or supervisors (see Figure 1). They represented a variety of organizational sizes, the majority of which were greater than 1,000 employees (see Figure 2).

When asked how their company uses the Internet, almost 95% responded they use it Internet to provide information; 81% use it to collect information; 60% to advertise; 55% to provide customer service; 46% to support internal operations; 45% to order goods and services; 38% to provide technical support; 36% to connect remote sites; 32% to extend internal networks; 27% to integrate value chain partners; and 18% to collect orders.

With the extensive use of the Internet (99%), these organizations could clearly be open to attack. With almost 95% of respondents providing information via the Internet, there could be a great exposure of information to potential crime, abuse, or misuse. With almost half of respondents indicating use of the Internet to support internal operations, there is also the risk of unauthorized disclosure or modification of information.

What are organizations doing to protect themselves? As indicated in Table 1, all respondents use passwords and virtually all use media backups and virus protection. What is not revealed is the organizations' vigilance in updating virus definitions, or the type of media backup schedule, either of which could negate any benefit derived from use of these protection mechanisms.

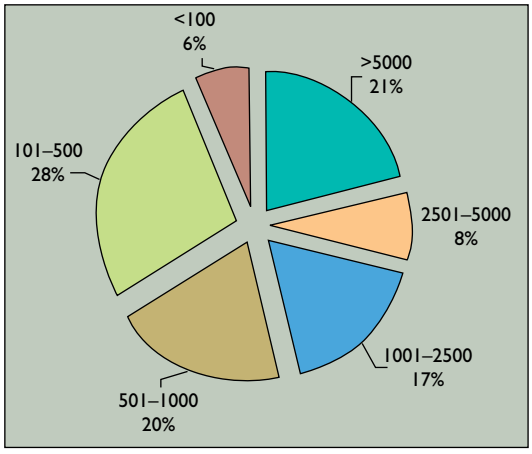

Figure 2. Respondents by organizational size.

Sadly, only about 63% indicated a consistent security policy. The security policy is the first and potentially most important layer of security available to an organization. Security policies define the security philosophy and posture the organization takes, and are the basis for all subsequent security decisions and implementations. Again, what's indistinguishable

is the effectiveness, comprehensiveness, and quality of the security policies of those indicating the presence of a policy. Equally concerning is the low response in the area of ethics training. A fundamental part of an organization's security function is the implementation of a security education, training, and awareness (SETA) program. Both the security policy and the SETA program are relatively low-cost protection mechanisms with the potential for high returns-on-investment. As technologists we often overlook the human solutions and instead opt for technology solutions, when in fact the human factors must be addressed first, with technology assisting in the enforcement of desired human behaviors.

Protection Mechanisms	
Use of passwords	100%
Media backup	97.9%
Virus protection software	97.9%
Employee education	89.6%
Audit procedures	65.6%
Consistent security policy	62.5%
Firewall	61.5%
Encourage violations reporting	51.0%
Auto account logoff	50.0%
Monitor computer usage	45.8%
Publish formal standards	43.8%
Control of workstations	40.6%
Network intrusion detection	33.3%
Host intrusion detection	31.3%
Ethics training	30.2%
No outside dialup connections	10.4%
Use shrink-wrap software only	9.4%
No internal Internet connections	6.3%
Use internally developed software only	4.2%
No outside network connections	4.2%
No outside Web connections	2.1%

(Multiple responses possible)

Table 1. Threat protection mechanisms employed in respondents' organizations.

Know the Enemy

The key information sought in this study is the identification and ranking of threats to information security. This list presents the result of the study with each category's corresponding ranking.

Threat Category	Weighted Ranking
Deliberate Software Attacks	2178
Technical Software Failures or Errors	1130
Act of Human Error or Failure	1101
Deliberate Acts of Espionage or Trespass	1044
Deliberate Acts of Sabotage or Vandalism	963
Technical Hardware Failures or Errors	942
Deliberate Acts of Theft	695
Forces of Nature	611
Compromises to Intellectual Property	495
QoS Deviations from Service Providers	434
Technological Obsolescence	428
Deliberate Acts of Information Extortion	225

The ranking is a calculation based on a combination of the respondents evaluating each category on a scale of "very significant" to "not significant" and then identifying the top five threats to their organization. With the prevalence of the malicious code attacks, it is not surprising that Deliberate Software Attacks tops the list, weighted almost twice as important as the second threat on the list. Given the cases of Nimda, Code Red, Sircam, Klez, and the SQL Slammer Worm, there is a substantial risk to organizational information and systems from malicious code. What is their primary means of access to systems? Exploitation of human failures in accidental activation of virus and worm executables, usually from email or Web site downloads. What's also interesting is that threats of Technical Software Failure or Errors ranked second, which can be viewed as both a threat and vulnerability; as malicious code and intruders exploiting problems in the software code. A direct threat to information exists when software failure causes information to be inaccurate, compromises integrity, or simply corrupts or impedes availability. Third and fourth on the list are Acts of Human Error or Failure and Deliberate Acts of Espionage or Trespass, better known as hacking.

These results were compared to the 2002 CSI/FBI Annual Computer Crime and Security Survey [3], which ranked the following items as significant threats (in order of significance) with 2001 ranking in parentheses:

1. Virus (1)
2. Insider abuse of Net access (2)
3. Laptop (3)
4. Denial of Service (6)
5. Unauthorized access by insiders (4)
6. System penetration (5)
7. Theft of proprietary info (7)
8. Financial fraud (9)
9. Telecom fraud (10)
10. Sabotage (8)
11. Telecom eavesdropping (11)
12. Active wiretap (12)

Both studies found malicious code the number-one threat. Not surprising, the CSI/FBI study found it the dominating threat for the past several years. The second threat category in the CSI/FBI study was Insider abuse of Net access. Interestingly enough this is more a function of security policy, ethics training, and

human failure than of technology. In order for a response to qualify for this category, first an organization had to establish a security policy, then train the employees on what they could and could not use their Internet access for, then the individuals had to fail to follow the established policy. Whether those responding to this question actually met all three requirements is open to speculation. Similar in scope is the CSI/FBI's unauthorized access by insiders. Here, however, there may be technology issues present. Was this a failure of individuals to follow policy? Or was it the failure or absence of a control mechanism to regulate user access?

The next area of interest was the frequency of attacks identified by respondents. Unfortunately, for every attack detected many more go undetected. Table 2 presents the responses to the inquiries on the number of attacks per month. Of particular interest is the emergence of Deliberate Acts of Information Extortion, the intentional illegal acquisition of information from an organization, with the intent to blackmail the organization with the threat of publication, dissemination, or use. While not a largely indicated threat, the mere presence designates an increase in the malicious nature of intruders. In general, almost all of the respondents indicated some form of attack, whether internal or external.

Number of Attacks per Month	>100	51–100	10–50	< 10	None	No Answer
1. Act of Human Error or Failure	5.2%	2.1%	14.6%	41.7%	24.0%	12.5%
2. Compromises to Intellectual Property	1.0%	2.1%	3.1%	25.0%	61.5%	7.3%
3. Deliberate Acts of Espionage or Trespass	4.2%	3.1%	3.1%	20.8%	68.8%	
4. Deliberate Acts of Information Extortion			1.0%	8.3%	90.6%	
5. Deliberate Acts of Sabotage or Vandalism	1.0%		3.1%	31.3%	64.6%	
6. Deliberate Acts of Theft			7.3%	38.5%	54.2%	
7. Deliberate Software Attacks	11.5%	9.4%	14.6%	47.9%	16.7%	
8. Forces of Nature	1.0%		2.1%	34.4%	62.5%	
9. Quality of Service Deviations from Service Providers		1.0%	8.3%	43.8%	46.9%	
10. Technical Hardware Failures or Errors		3.1%	11.5%	51.0%	34.4%	
11. Technical Software Failures or Errors		5.2%	18.8%	45.8%	30.2%	
12. Technological Obsolescence		1.0%	15.6%	21.9%	60.4%	1.0%
Average Responses:	**4.0%**	**3.4%**	**8.6%**	**34.2%**	**51.2%**	**6.9%**

Table 2. Numbers of attacks per month as reported by respondents.

As is evident from the findings, the threat is real, the stakes are high, and the systems protecting the target information are difficult to protect. Just as Loch, Carr, and Warkentin found in a similar study over 10 years ago, "results suggest that management needs to (1) become more informed of the potential for security breaches … (2) increase their awareness in key areas, … and (3) recognize that their overall level of concern for security may underestimate the potential risk inherent in the highly connected environment in which they operate" [2].

How to Put this Information to Use

Now that an organization knows what the threats are, how can its security administrators and technology managers put this information to use? One of the most direct uses of this information is in the identification and application of controls. The methodology to develop and implement a "control matrix" is simple. Making it work is the real challenge.

Identify and prioritize threats to the organization's information assets. Beginning with the information provided, the security administrators should prioritize those categories of threats that represent the greatest danger to the organization. How the organization defines danger is up to them. Danger could be determined based on the probability of an attack coupled with the potential loss value in financial terms, in critical information, or in potential embarrassment. The criteria used to rank the threats are part of the customization of the process to the organization's needs.

Identify and prioritize the information assets. Administrators should detail all assets that collect, process, store, or use information in the organization. These will most likely not be all IT assets, and should include various "people" areas as well. How the organization prioritizes these assets could be based on the number or severity of known vulnerabilities, exposure to threats, cost or difficulty of replacement of the asset, content of critical information, or a host of other criteria. Should more than one criterion be used in evaluating the asset, a weighted means could be developed to quantify the ranking.

Create a matrix listing the threats, in priority, along one axis, and the assets, in priority along the other. The resulting grid provides a convenient method of examining the "exposure" of assets, allowing a simplistic vulnerability assessment. Table 3 presents a sample of the resulting framework.

Fill in each intersection with the current controls. The intersection of the threat to asset pair represents an area that should be addressed by more than one control. Controls in this situation are defined as those

	Asset 1	Asset 2	...	...	...	...	...	...	...	...	...	Asset n
Threat 1												
Threat 2												
...												
...												
...												
...												
...												
...												
...												
...												
...												
Threat n												
Priority of Controls	1		2		3		4		5		6	
These bands of controls should be continued through all threat: asset pairs.												

Table 3. Sample control matrix (incomplete).

measures that protect this asset from this threat, or allow the organization to recover this asset if attacked by this threat. If a particular asset is not at risk from a paired threat, simply cross out that cell. At a minimum each threat:asset pair should contain one policy-related control, one education- and training-related control, and one technology-related control. When all controls in place have been entered, an organization can (beginning with the upper-left corner of the matrix) begin prioritizing the implementation of additional controls until such time as multiple controls have been assigned, implemented, and tested to protect each asset.

Upon completion of this task, not only have the administrators gone through an internal self-assessment of vulnerabilities, they also have ensured the organization has "defense in depth" providing protection and recovery capabilities for all priority information assets.

Policy and the SETA Program

The information gathered through the aforementioned exercise should not be used in isolation. Nor should it be the first exercise in security profile development. Security advocates emphasize that any security profile begins with valid security policy [4, 6]. This policy is then translated into action through an effective security plan focusing on the prevention, detection, and correction of threats. While the development of such a policy—or more accurately, series of policies—is so important as to go beyond the scope of this discussion, it is vital an organization begin with the methodical development of such policy.

An additional activity that should be developed early is the design and implementation of an employee security education, training, and awareness program. These programs seek to educate employees on the importance of security, and its implementation within the organization. The accompanying awareness program seeks to keep security on the minds of employees as they deal with vital information on a daily basis.

Lessons Learned

The lessons learned from this study are simple. Now, more than ever before, the information contained in the organization is at risk. There are a large number of threats to this information, representing diverse and complex challenges to protect the information, personnel, and systems that process, transport, and store it. This requires a wide array of protection mechanisms and strategies to be thorough. An important component of this protection is the understanding of the enemy.

This study sought to provide additional insight into this understanding, as well as a method for assessing protection mechanisms, ensuring a comprehensive security profile, with defense in depth. Organizations that employ these techniques can expect to better understand their security profile, and more easily identify weaknesses in it. This information, coupled with solid policy planning, and SETA development should allow an organization to better focus its security efforts, thus increasing its probability of protecting the information and reducing its vulnerability to attack. C

References

1. Brancheau, J.C., Janz, B.D., and Weatherbe, J.C. Key issues in information systems management: 1994–95 SIM Delphi results. *MIS Q 20*. 2 (1996), 225–242.
2. Loch, K.D., Carr, H.H., and Warkentin, M.E. Threats to information systems: Today's reality, yesterday's understanding. *MIS Q. 16*, 2 (1992), 173–186.
3. Power, R. 2002 CSI/FBI computer crime and security survey. *Computer Security Issues & Trends 8*, 1 (2002), 1–24.
4. Straub, D.W. and Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Q. 22*, 4 (1998), 441–469.
5. Tzu, S. *The Art of War: Translation by Samuel B. Griffith.* Oxford University Press, Oxford, U.K., 1988.
6. Wood, C.C. Integrated approach includes information security. *Security 37*, 2 (2000), 43–44.

Michael E. Whitman (mwhitman@kennesaw.edu) is an associate professor of IS in the Computer Science and Information Systems Department of Kennesaw State University, Kennesaw, GA.