The Enemy at the Gates II: The Enemy Within

Michael E. Whitman, Herbert J. Mattord, *Kennesaw State University*

Abstract – The effort to secure cyberspace continues unabated. Yet, losses continue to mount. If we are to gain ground in this effort, we must understand our adversaries and the mechanisms they use to inflict losses. When we know the threats facing our information assets and the potential losses the assets face, we can begin to build more effective defenses using well defined risk management methodologies. This paper examines top computer executives' perspectives on current threats to information security, and compares those threats to a previous study from 2002.

Index terms – Information Security, Information Security Threats, Risk Management

I. INTRODUCTION

It is generally accepted that if an organization wishes to prevent losses to information assets, they must protect them. There are many reports from around the world of losses from hacking, malware and theft. As of September 30, 2009, there were an estimated 1.734 billion Internet users, approximately 25.6% of the world's population [1]. Literally interpreted that means that there could be 1.734 billion potential hackers and/or information abusers. There are an enormous number of systems connected to the Internet and exposed to potential compromise. Each of these represents possible losses and, once compromised, possible platforms for indirect attacks. This risk does not go unnoticed. The Metagroup reports that data security/protection is a leading issue with offshore outsourcing [2]. Educause reports that security is near the top of the list of issues facing higher education [3]. The verdict is in; security is a problem. Knowing one's enemy is the first step toward a solution to that problem.

A. The Wisdom of Sun Tzu

"Know the enemy, and know yourself; in a hundred battles you will never be in peril" [4]. Frequently quoted in modern times, this simple statement has been used to explain and teach information security by extending it to be an analogy for risk management [5]. Knowing oneself is akin to identifying, categorizing, classifying and prioritizing information assets within an organization. This is critical to understanding an organization's security posture. Once you know what needs protection and how you are currently protecting it, you can determine if your current defense is adequate. One element of this process is to look at what you are protecting it from. Thus, the second half of Sun Tzu's quotation "know your enemy" means you must understand the threats that menace an organization's information assets. And, if threats exist, it is essential to understand how they might present themselves as attacks.

The process begins with finding out what threats exist. According to a Rees and Allen study "respondents reported substantial difficulty in identifying threats and estimating loss, indicating that much can be done to improve the current state of practice" [6]. This indicates that, regardless of studies or publicity about cyber security, some organizations need help in this identification process.

II. PREVIOUS STUDIES

One of the most recognized studies of the threats and attacks on information assets is the Computer Security Institute's Computer Crime and Security Survey (see www.gocsi.com), conducted annually since 1996. And, even though there are questions about the rigor of this study, it has tracked some trends for over a decade, revealing the emergence and decline of issues in information security. In 2009, the CSI study identified their top 12 threats/attacks as follows [7]:

1. Malware infection
2. Laptop/mobile hardware theft/loss
3. Being fraudulently represented as sender of phishing message
4. Insider abuse of Internet access or email
5. Denial of service
6. Bots within the organization
7. Financial fraud
8. Password sniffing
9. Unauthorized access or privilege escalation by insider
10. Web site defacement
11. System penetration by outsider
12. Exploit of client Web browser

In 2002, a study was undertaken to identify dominant threats to organizational information as identified by industry professionals. This study [8] was published in the August 2003 edition of the Communications of the ACM and examined two questions:

a) What are the most serious threats to information security?

ISBN 1-933510-96-X/$15.00

b) Which threats result in the highest attack-driven expenditures?

That study compiled over 200 individual threats by reviewing relevant literature and by interviewing information security professionals. Through an iterative process the individual threats were consolidated into 12 categories of threats to information security:

1. Compromises to Intellectual Property – software piracy or other copyright infringement
2. Deviations in Quality of Service from Service Providers – fluctuations in power, data, and other services
3. Espionage or Trespass – unauthorized access and/or data collection
4. Forces of nature – fire, flood, earthquake, lightning, etc.
5. Human Error or Failure – accidents, employee mistakes, failure to follow policy
6. Information Extortion – blackmail threat of information disclosure
7. Sabotage or Vandalism – damage to or destruction of systems or information
8. Software Attacks – malware: viruses, worms, macros, denial-of-services or script injections
9. Technical Hardware Failures or Errors – hardware equipment failure
10. Technical Software Failures or Errors – bugs, code problems, loopholes, backdoors
11. Technological Obsolescence – antiquated or outdated technologies
12. Theft – illegal confiscation of equipment or information

The study was then sent to over 1000 Chief Computing Officers selected at random from the Directory of Top Computing Executives, asking them to rate and rank the threats as presented, identify their top expenditures for those threats, and provide insight as to the technologies deployed against those threats.

III. THEN AND NOW

In 2010, the researchers decided to revisit this study, to determine the following:

a) Have the threats to information security changed in priority?
b) What risk management efforts organizations now employ?
c) What standards influence information security efforts?

As in 2002, over 1000 information security professionals were randomly selected using the most recent version of the Directory of Top Computing Executives and invited to participate in an online survey. A total of 141 responded, representing:

31.3% - IS/IT/InfoSec directors, managers or supervisors
25% - Corporate Management (VP IS, VP IT, CISO, VP InfoSec);
12.5% - Executive Management (CIO, CTO, CSO, Exec.VP);
16.7% Other IS/IT/InfoSec Managers; and
14.6% - IS/IT/InfoSec Staff.

They also represented a variety of organizational sizes (22.9% <100 employees; 12.5% 101-500; 2.1% 501-1000; 6.3% 1001- 2500; 16.7% 2501-5000 and 39.6% > 5000). They also represented a wide variety of industries as shown in Figure 1. The "other" category primarily consisted of unique organizations that combined categories (e.g. Government Healthcare).

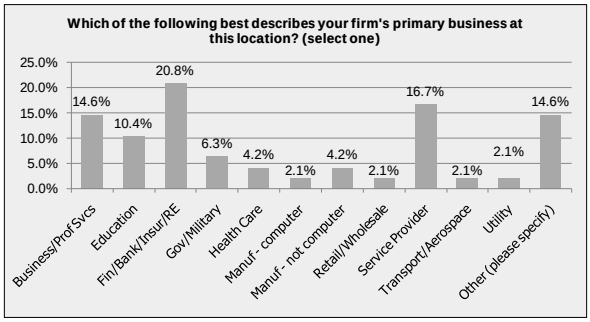

Figure 1: Respondents by Industry

A. What are organizations doing to protect themselves?

As indicated in Table 2, all respondents use passwords and virtually all use media backups and virus protection.

The top protection mechanisms identified in the 2002 survey remain the top today, with *passwords, media backup and virus protection software* topping the list. As noted in the 2002 study, "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" [8]. The drop in *employee policy education* causes some concern, as organizations may have traded off efforts in the security awareness arena for more discrete efforts such as *auditing procedures* and *published formal standards*.

Table 2: Threat Protection Mechanisms Employed in Respondents Organizations
(Multiple responses possible)

Answer Options	2010 Response	2002 Response
Use of passwords	100.0%	100.0%
Media backup	95.8%	97.9%
Virus protection software	95.8%	97.9%
Employee policy education	75.0%	89.6%
Audit procedures	72.9%	65.6%
Consistent security policy	66.7%	62.5%
Publish formal standards	60.4%	43.8%
Employee technology training	56.3%	n/a
Control of workstations	52.1%	40.6%
Ethics training	52.1%	30.2%
Encourage violations reporting	47.9%	51.0%
Monitor computer usage	41.7%	45.8%
Auto account logoff	33.3%	50.0%
No outside dialup connections	33.3%	10.4%
No outside web connections	8.3%	2.1%
No outside network connections	6.3%	4.2%
No internal Internet connections	4.2%	6.3%
Use internally developed software only	4.2%	4.2%
Use shrink-wrap software only	4.2%	9.4%

B. Know the Enemy…

The key information sought in this study is the identification and ranking of threats to information security. Table 3 presents not only the categories of threats, but their ratings and ranking as well, with the most severe threat listed as #1. This study used the same calculation methodology as the 2002 study. The ratings were calculated based on each respondent first rating each threat on a scale of very significant to not significant, converting the scores to a 5 points scale where 5 = very significant, and averaging the scores over the number of responses. The rankings were calculated asking respondents to identify the top 5 threats to their organization, then assigning 5 points for a first place vote down to 1 point for a fifth place vote, allowing the result to reflect the number of votes as well as the ranking. The combined score is the product of the two evaluations divided by 100 to standardize the results, just as was done in the previous study. The entire table is sorted by the 2010 combined evaluations resulting in a list of greatest to least threats. The right-hand column presents the overall sort from the 2002 study.

Topping the list is Espionage or Trespass, most commonly associated with hacking attempts. This is an interesting result, but not unexpected. Efforts made by organizations are doing better jobs of reducing the impact of some of the other threats, but with the increasing numbers of computers accessing the Internet, and the increase in criminal hacking, it is not unexpected that the recognition of the severity of this threat has risen.

Table 3: 2002 and 2010 Studies Compared

2010 #	Categories of Threats	2010 Scores	2002 Scores	2002 #
1	Espionage or Trespass	16.35	10.43	4
2	Software Attacks	12.24	21.79	1
3	Human Error or Failure	9.55	11.03	3
4	Theft	5.85	6.94	7
5	Compromises to Intellectual Property	5.82	4.95	9
6	Sabotage or Vandalism	3.45	9.64	5
7	Technical Software Failures or Errors	3.33	11.31	2
8	Technical Hardware Failures or Errors	2.51	9.42	6
9	Forces of Nature	2.24	6.10	8
10	Quality of Service Deviations from Service Providers	2.07	4.35	10
11	Technological Obsolescence	1.52	4.28	11
12	Information Extortion	0.48	2.25	12

Software Attacks from viruses, malware, etc., were again near the top. Identical to the results of the most recent CSI study, malware is expected to continue as a dominant threat to security efforts. Reports vary in details, but it was reported that an email security firm scanned over 413 million emails and found 52 percent were spam, three percent had a virus, and a notable number contained pornography [9]. Recently, two reports indicated that between 1 and 3 percent of Internet traffic is malicious and contained meaningless packets of information used in denial-of-service attacks [10, 11]. With the increased focus on targeted malware, the danger will rise. Targeted malware is a software attack that is specifically focused on the recipient, rather than on a general mailing, much as the mail-marketing industry has increased its focus from generic mailings, to targeted mailings, drawing information from shopper's profiles, buying habits and online searching.

The human factor remains prevalent, with Human Error or Failure rounding out the top three. In 2008 CIO magazine found that this category topped a list of security threats examined by Deloitte [12]. While the CSI study does not have an identical category, as it evaluates attacks perpetrated by threats, rather than the threats themselves, the number three and four attacks - Being fraudulently represented as sender of phishing message and Insider abuse of Internet access or email - both represent instances where a human failed to follow expected policies, procedures and practices (if indeed any were present) in the performance of their job, resulting in an attack on information.

Some threats have changed dramatically. Discounting additions, the threat *technical software failures* has shown the greatest change, falling five positions. This is perhaps due to increased rigor in software patching and updating on the part of organizations, and enhanced response to

threats by software vendors. What is not known is whether efforts to increase the quality of the actual software products deserves the credit, or whether vendors are simply gaining expertise in identifying and responding to potential or actual security vulnerabilities with available patches. *Compromises to Intellectual Property* moved up 2 positions. In spite of increased legislation regarding software piracy, organizations seem increasingly concerned with IP violations. This fact, combined with unsatisfactory levels of employee policy education, and training give rise to questions as to why organizations aren't doing more. Solutions for internal IP violations has long been recognized as possible with employee education, training and awareness programs, effective policy and enforced compliance.

C. Threat Expenditures

One question asked of the respondents was to identify their top threat-driven expenditures. Each respondent was asked to identify the top 5 threats facing their organizations based on actual expenditures. The ranking presented in Table 4 was calculated based on those responses. The results reveal the threats for which the organization is currently dedicating resources. For comparison, the rankings from the 2002 study are also presented.

Note that organizations are collectively expending resources appropriately; those organizations responding to the survey report that they are spending the most to protect against the most severe threats. Less encouraging is the high severity of *human error or failure* when compared to the relatively low expenditure for that category. Employee training, both security and job-related, would go a long way toward minimizing the impact of this category. This is also one of the few categories of threats that is entirely within the organization's control.

When we compare the ranking of threats to the ranking of expenditures, we can see that organizations are focusing the bulk of their efforts on the dominant threats. As is evidenced by Table 5, there is a strong similarity in the rankings of items in these two lists.

Table 4: Ranking of Threats by Expenditure

Money and Effort Spent to Defend Against or React to the Threat	Overall Ranking	Overall Ranking
1. Espionage or Trespass	1	6
2. Software Attacks	2	1
3. Theft	4	7
4. Quality of Service Deviations by Service Providers	5	5
5. Forces of Nature	6	10
6. Sabotage or Vandalism	7	8
7. Technological Obsolescence	8	9
8. Technical Software Failures or Errors	9	3
9. Technical Hardware Failures or Errors	10	4
10. Compromises to Intellectual Property	11	11
11. Human Error or Failure	12	2
12. Information Extortion	14	12

Table 5: Comparison of 2010 Ranking of Threats: Expenditure vs. Perceived Severity

Threats by Expenditure	Threats by Severity
1. Espionage or Trespass	Espionage or Trespass
2. Software Attacks	Software Attacks
3. Theft	Human Error or Failure
4. Quality of Service Deviations by Service Providers	Theft
5. Forces of Nature	Compromises to Intellectual Property
6. Sabotage or Vandalism	Sabotage or Vandalism
7. Technological Obsolescence	Technical Software Failures or Errors
8. Technical Software Failures or Errors	Technical Hardware Failures or Errors
9. Technical Hardware Failures or Errors	Forces of Nature
10. Compromises to Intellectual Property	Quality of Service Deviations from Service Providers
11. Human Error or Failure	Technological Obsolescence
12. Information Extortion	Information Extortion

Of particular interest in Table 5 is the disproportionate nature of protecting against each threat category. The cost of protecting against the number 2 threat *software attacks* by purchasing anti-virus software, can be much less expensive than the cost of protecting against a lower threat: such as *sabotage or vandalism* which requires the purchase and installation of firewalls, intrusion detection software and so forth. Similarly, the cost of training internal employees and developing policy can be substantially less than that required for protecting against quality of service deviations through redundant circuits and power protection. There is a presumption that organizations would dedicate more resources to the "more

expensive to protect against" threats. However, organizations may be using their understanding of the level of severity of these threats to drive expenditures.

IV. Security Management Items of Interest

Other questions of interest asked how respondents dealt with security management issues focusing on risk management. When asked "*In your organization's risk management efforts, what basis do you use to assess threats?*" respondents indicated that the probability of occurrence and reputation loss if successful were the top two drivers of assessment, with financial loss if successful, cost to protect against, and cost to recover next in priority.

Next respondents were asked "*Does your organization use a formal risk management strategy to guide its efforts? (I.e. OCTAVE, MSRM, FAIR).*" Given trade press discussion of security management certifications and industry professionalism, the results were rather surprising. Trade press coverage and anecdotal feedback had led the researchers to expect that the bulk of the respondents would indicate that they had adapted a formal risk management. However, the study found that the vast majority of those responding did not (62.5%). Those that indicated that they did use a formal methodology (6.3% did, and an additional 20.8% did but modified it) indicated methodologies that varied wildly, from the traditional NIST SP 800-30, OCTAVE and COBIT to a "North American Electric Reliability Corporation (NERC) formal risk assessment for critical assets".

A. Information Security Standards

Information security standards are often used to guide an organization's security efforts, including risk management. There are a number of alternatives available, but the most popular are the NIST standards, designed predominantly for government agencies, and the ISO 27000 series, designed for those organizations interested in international security management certification. When asked "*Does your organization use a formal information security standard to guide its efforts? (i.e. ISO, NIST)*", respondents indicated that 27.1% did not, 31.3% did, and an additional 37.5 percent did, but modified it. Those that did use a standard (modified or not) indicated the ISO 27000 series as their standard of preference (64%), as shown in Figure 2.

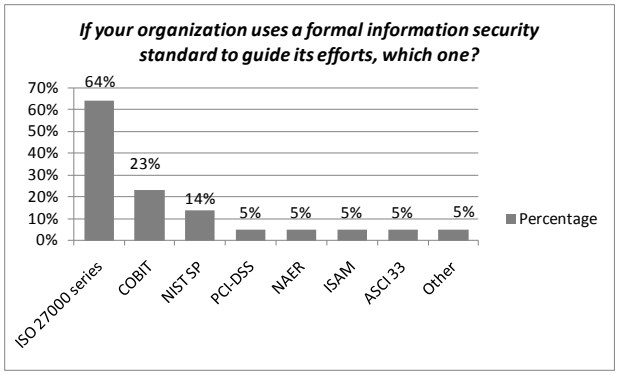

Figure 2: Employed Information Security Standards

V. How To Put This Information To Use

When an organization knows what threats are present, how can its security administrators and technology managers put this information to use? One of the most direct uses is in the identification and assessment of threats to the specific organization. While the threats and threat categories described in this study represent an overview of widespread threats, each organization must evaluate and assess the threats facing it. This is done through a formal and precise risk management program. While the details of risk management programs will differ, most involve four basic steps:

1. *Identify and prioritize threats to the organization's information assets.* Prioritize those categories of threats that represent the greatest danger to the organization. Defining danger may be based on the probability of an attack coupled with potential losses.
2. *Identify and prioritize the information assets.* Identify assets that collect, store or use information in the organization. Prioritizes these assets based on organizational needs using the number or severity of known vulnerabilities, exposure to threats, cost or difficulty of replacement of the asset, content of critical information or the most applicable criteria.
3. *Compare the prioritized threats to the prioritized assets.* Determine if assets are currently at risk. If an asset is not at risk, then that threat/asset pair can be disregarded. If it is, then the vulnerabilities associated with the threat/asset pair must be examined.
4. *Evaluate the sufficiency of existing controls/safeguards and remediate as needed.* What, if any, new controls and safeguards must be obtained to reach an acceptable level of risk.

VI. Lessons Learned and Conclusions

Gene Spafford observed "Asking how to make system 'XYZ' secure against all threats is, at its core, a nonsensical question… The goal in the practice of security is to construct sufficient defenses against the likely threats in such way as to reduce the risk of

compromise to an acceptable level" [13]. The lessons to be learned from this study are simple. The information assets of the organization are at risk from many, diverse, and complex threats. Any response will require the selection of protection mechanisms and strategies drawn from many possibilities. An important part of selecting controls is an understanding of your adversaries. These adversaries present themselves to you in 12 categories of threats to your information security. Organizations are also dedicating increasing resources to defend information assets. Forewarned is forearmed; Just as a similar study found almost 20 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" [14]. In order to continue to prepare for the attacks from these threats, organizations now more than ever must carefully prioritize the threats facing their assets, as well as prioritize the assets themselves. In order to make sure that no asset goes unprotected, the organization is advised to compare assets to threats and identify the safeguards currently in place. The prioritization process itself is worthwhile. The ultimate benefit, however, is the peace of mind that comes from knowing that the information you protect is as secure as it can be.

VII. References

[1] Miniwatts Marketing Group. (2009). Internet Usage Statistics: The Internet Big Picture. WWW document viewed 2/5/2010 from http://www.internetworldstats.com/stats.htm.

[2] Davidson, D. (2004). Top 10 risks of offshore outsourcing. WWW Document viewed 2/10/2010 from http://searchcio.techtarget.com/news/article/0,289142,sid182_gci950602,00.html?mboxConv=searchSecurity_RegActivate_Submit&)

[3] Agee, A., Yang, C. & the 2009 EDUCAUSE Current Issues Committee. (2009). Top Ten IT Issues of 2009. WWW Document viewed 2/10/2010 from (http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume44/TopTenITIssues2009/174191).

[4] Wu, Sun Tzu & Griffith, S. (1971). The Art of War. Ozford University Press, Oxford, England.

[5] Whitman, M. & Mattord, H. (2010). Management of Information Security, 3rd ed. Delmar/Cengage/Course Technology, Boston, MA.

[6] Rees, J. & Allen, J. (2008). "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation" Journal of Organizational Computing and Electronic Commerce. Oct. Vol. 18, Iss. 4; pg. 255.

[7] CSI. (2000-2009). Table compiled from CSI and CSI/FBI studies from 2000 to 2009, downloaded from www.gocsi.com. Most recent edition, Richardson, R. CSI Computer Crime Security Survey, December 2009. WWW Document, downloaded February 2010 from www.gocsi.com.

[8] Whitman, M. E. (2003). "Enemy at the Gates: Threats to Information Security." Communications of the ACM, 46(8), pp. 91-95.

[9] Microsoft. (nd). "Intro to Criminal Hacking, Viruses and Malicious Activity" WWW Document viewed 3/25/2010 from http://www.microsoft.com/canada/smallbiz/sgc/articles/an_introduction_to_criminal_hacking_viruses_and_malicious_activities.mspx.

[10] Anonymous. (nd). "More than 2% of Internet Traffic Malicious" WWW Document viewed 2/25/2010 from http://stratusec.com/blog/tag/malicious-internet-traffic/.

[11] McMillian, R. (2008). "Up to Three Percent of Internet Traffic is Malicious" CSO. April 1. WWW Document viewed 2/25/2010 from http://www.csoonline.com/article/326013/Up_to_Three_Percent_of_Internet_Traffic_is_Malicious_Researcher_Says.

[12] Daniel, D. (2008)."Human Error Tops the List of Security Threats." CIO. WWW Document viewed 2/25/2010 from http://www.cio.com/article/179802/Human_Error_Tops_the_List_of_Security_Threats.

[13] Spafford, E. (2009). "Answering the Wrong Questions Is No Answer" Communications of the ACM. 52(6), pg. 22.

[14] Loch, K., Carr, H. & Warkentin, M. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly, 16(2), 173-186.