

***Assessment of Information Security***  
***spending and costs of failure***

**Xin Luo**

Department of Mgmt and Information Systems  
Mississippi State University  
xl96@msstate.edu

**Merrill Warkentin**

Department of Mgmt and Information Systems  
Mississippi State University  
mwarkentin@acm.org

**Abstract**

This article reviews the current state of security spending and costs of failure in information technology. Our assessment indicates that companies with insufficient IT security spending would face a risky scenario through which their overall profitability and efficiency might suffer. We have also identified a variety of critical issues that companies are likely to encounter and neglect, such as providing relevant employee training to improve security protection, internal security threats, and insurance for cyber-crime and online outages.

**Keywords:** *information technology, security, spending, cost, budget*

**Introduction**

Information technology (IT) security is becoming a more important function of information systems management, as more companies have embarked on the globally connected Internet to enhance interactivity and collaboration between employees (internally) and with external constituents, such as vendors, distributors, customers, and regulators. Many companies now perceive IT security as not only a required protective shell encompassing databases, but also as a critical asset to be carefully managed. It is estimated that business-to-business (B2B) and business-to-consumer (B2C) e-commerce revenue will reach \$5.9 trillion and \$663 billion dollars by 2005, respectively. [Datamonitor, 2000] However, without a proper IT security strategy, supported by the requisite budgetary commitment, the promise of the electronic revolution will not become

reality. Although most global companies recognize the importance of information security to their survival, much of their business-critical information, processes, and systems are still not adequately protected.

Currently, more than 50% of businesses worldwide spend 5% or less of their overall information technology budget on security. The 2-3% of the overall IT budget that companies allocate for security on average will not sufficiently protect the rapidly changing and increasingly complex technology architectures. Spending 2% or 3% on security affords most companies only basic security protections, such as anti-virus applications, firewalls, VPNs, and basic intrusion detection systems. Minimal spending on these security basics does not ensure efficient and effective security, only continued expenditures to maintain the basic systems; meanwhile, the number and destructive power of security threats continue to grow dramatically.

Insufficient IT security budgets will push companies to a perilous and vulnerable edge, which will inevitably force them to tolerate significant risks that could lead to critical data loss or corruption, system malfunctions or shutdown, and ultimately productivity losses and pressures on profit margins. According to the latest 2003 Computer Crime and Security Survey conducted by Computer Security Institute [Computer Security Institute, 2003], the total annual losses reported by 530 U.S. participants (primarily large corporations and government agencies) were \$201,797,340 and the risk of cyber attacks continues to be high. The recent MS Blaster worm costs approximately \$475,000 (includes hard, soft, and productivity costs) per company to remediate wounds. [Security Stats.com, 2003] This worm entered company networks most often through infected computers, then VPNs, and finally through weakly-configured firewalls or routers. According to a recent report conducted by TruSecure/ICSA Labs, some large companies reported losses as high as \$4,228,000 from the worm breach. [Security Stats.com, 2003]

Furthermore, the Internet Fraud Complaint Center has found that instances of Internet fraud increased drastically in 2002 as compared to 2001, and losses reported by victims totaled \$54 million versus \$17 million the year before. Non-tech manufacturers are more likely to be risk-tolerant than high-profile companies such as banks, financial trading institutions, large hosting services, and defense contractors. [Giga Information Group, 2002] These high-profile organizations are highly risk-intolerant or even zero-tolerant for risk because their customers are keenly concerned about their important confidential information. The overall trend, however, is that more companies are becoming less risk tolerant, leading more companies to increase IT security expenditures.

### **Costs of Security Failures**

Financial losses are virtually certain when security protections fail. Worldwide financial costs of cyber attacks are estimated to have increased from \$US 3.3 billion in 1997 to \$12

billion in 2003, [Tkaczyk, 2003] as the worldwide impact of cyber attacks has increased steadily. Table 1 shows the total financial impact of the most known malicious codes found in recent years: [Computer Economics]

<b>Table 1: Financial Impact of Malicious Code (\$ US Billions)</b>	
Explorer 1999	\$1.02
Melissa 1999	\$1.10
Love Bug 2000	\$8.75
SirCam 2001	\$1.15
Code Red(s) 2001	\$2.62
Nimda 2001	\$0.64
SQL Slammer 2003	\$1.25
Blaster & SoBig.F 2003	\$2.00

Source: Computer Economics

Spending on security is expected to soar over the next year and beyond in the wake of the recent outbreak of the Sobig.F computer virus, which exploits weakness in Microsoft software and radically clogged the internet by sending emails to everyone listed in an infected computer's address book. In general, the biggest threat to effective security is the increasing level of sophistication of the malicious codes attacking information systems. Additionally, a recent IDC study has found that increased use of the Internet and reaction to corporate security breaches are leading the list of reasons for companies to boost their security. [Gaudin, 2002] Particularly, high-profile companies are lowering their risk tolerance and increasing security budgets. We have found that financial services companies are spending approximately 6% of their IT budgets on security and 47% of them have hired extra security staff compared with 2001, despite the slowdown in the economy. [Deloitte Touche Tohmatsu, 2003] KPMG, for instance, is preparing for increased security related spending from between 2% and 4% of IT budgets to between 5 and 10 % in the next three years.

In addition to financial losses, companies also pay close attention to customers and focus their security efforts on trying to retain customers, as the expected increase of security partly comes from the pressure from companies' customers. During the global outbreak of the recent Sobig.F virus, many companies realized that under-investment in IT security led to vulnerabilities that triggered systems breakdowns and threatened profits. For example, companies like Barclays Bank, one of Britain's biggest investors in IT, reported a 900% increase in the number of customers requesting protection for their e-mail accounts; the total number of queries was in the thousands. [Sabbagh, 2003] Customer concerns are now driving IT security expenditures.

Systems integration efforts have caused companies to invest more in creating a common security infrastructure across their organizational structures. Access control, authorization and auditing, and identity management are the top spending priorities. Most companies are well aware of the importance of information security. According to the 2003 CSI/FBI survey, virtually all organizations are armed with anti-virus software (99%) and firewalls (98%) against cyber attacks. [Computer Security Institute, 2003] However, most companies have not yet effectively deployed more advanced defensive security applications beyond basic anti-virus software and firewalls. Most companies are deploying security spending on basic information technology and business continuity systems instead of investing in employee training, vulnerability analysis, and other measures to enhance and solidify protection. Failing to implement a security awareness campaign with sufficient relevant security training can cost huge sums in the long run and, more importantly, can cause potential security problem for companies, because the lack of user education indicates that companies may not be taking the full advantage of their existing expensive security systems. Numerous reports indicate that the greatest threat to most organizations is the internal threat of existing employees, who introduce security weaknesses as a result of poor awareness of security vulnerabilities, sloppy data entry, ineffective systems analysis and programming, avoidance of internal controls, and other practices. Accidental and inadvertent actions are usually a much greater source of security weaknesses than malicious and deliberate acts of sabotage.

When determining which security solutions to purchase and implement, most companies are aimlessly investing in security technology without carefully analyzing the return on investment. This indicates that companies might be squandering their money on unnecessary and needless technology, which might instead be spent on employee education. Since most system breaches caused by hackers stem from known system vulnerabilities, employees can be educated to better understand the value of accessible data and information so as to further enrich the efficiency and effectiveness of security identification and protection.

### **Government Regulations and Insurance**

In addition to security hardware and software applications, federal and state regulation can be an indirect incentive for companies to increase spending on information security. Legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Financial Modernization Act of 1999, and the Sarbanes-Oxley Act of 2002 has forced companies to spend more in order to comply. HIPAA sets up national standards to ascertain privacy in electronic healthcare transaction; Sarbanes-Oxley will become a Securities and Exchange Commission rule that requires managers have internal control over areas including transactions, electronic information, and communications; The Gramm-Leach-Bliley Act regulates how U.S. banking, securities, and insurance industries can share information and provide various financial

services to customers. [Dubie, 2003] These regulations will pressure companies to increase spending on IT security maintenance. For example, it is estimated that implementing IT security solutions to ensure minimum compliance with HIPPA regulations could cost hospitals up to US\$ 22.5 over five years. [American Hospital Association, 2001]

As mentioned above, security threats are becoming more sophisticated and have not declined. What's more, malicious code attacks cost companies considerable time and money to remedy every year. Losses from computer crime are expected to soar 25% to \$2.8 billion in the USA this year and successful web-site attacks nearly doubled to 600 a day. [Money, 2003]

On the other hand, insurance companies are encouraged to provide more cyber-risk insurance policies to integrate with the National Strategy to Secure Cyberspace plan from the U.S. federal government. In order to vouch for financial safeguards, many companies are driven to spend extra money purchasing cyber hacking-related coverage policy, which is also called network risk insurance and is expected to escalate from a \$100 million market today to \$900 million by 2005. [Money, 2003] Currently, separate cyber-policies cost between approximately \$10,000 and \$30,000 a year for \$1 million of coverage, depending on the intricacy and density of a company's online activities. In addition to the premium, companies also have to have their networks assessed and therefore undergo an independent and expensive audit of their online security to be eligible for cyber-risk coverage. Such a security audit can cost between \$5,000 and \$30,000. [Johnson, 2001]

As technology grows more complicated, hacker insurance will be ubiquitous in a few years as a fixed cost for companies to reduce cyber risk. Nevertheless, despite the cyber risk coverage, companies are still exposed to certain level of financial and physical risks since insurance coverage has limitations and may not cover increasingly sophisticated malicious codes or other new threats that have yet to emerge. Cyber-policies will likely be purchased to augment general liability policies (that costs \$5,000 per \$1 million of coverage) if damages from cyber vandalism keep growing at the current pace.

### **Security Challenged by Insiders**

In general, the safeguards in place today are primarily implemented to keep outsiders from intruding the internal information systems and accessing confidential business information. However, spending millions of dollars adopting security practices does not guarantee security effectiveness because many threats are internal. In addition to the accidental damage discussed above, which can be ameliorated by training, there are disloyal employees that may sabotage their employers. According to a recent CSI-FBI survey, 80 percent of the computer crime cases involve insider attacks, which are just as costly as outside attacks or even more damaging. [Computer Security Institute, 2003]

Additionally, the 2000 Information Security Survey conducted by *Information Security* magazine shows that the number of victims of insider attacks (such as theft and the intentional destruction of computer equipment and information) doubled last year, as 58% of the 1,897 respondents said that insiders had abused computer access controls and 41% reported that insiders had electronically destroyed or distributed confidential company information. [Enos, 2000]

An organization's vulnerability to insiders can trigger considerably serious aftermath. In one relevant insider cyber crime case, Timothy Lloyd, a former chief computer network program designer of Omega Engineering Corp, was convicted of unleashing a logic bomb on the company's computer systems after he realized that he was about to be fired. The bomb systematically deleted all of the company's contracts as well as proprietary software used by the company's manufacturing tools. The damage, followed by loss of productivity, cost Omega Engineering \$12 million and competitive position in the electronic manufacturing market to fathom that security is everybody's business. [Enos, 2000] In another public case, a firm's board of directors fired a CEO, who subsequently stole trade secrets from the corporate network files before leaving his position. The costs of such activity are immeasurable.

## **Summary**

The costs to companies arising from IT security vulnerabilities is likely to rise as a result of the increasing sophistication, complexity, and frequency of security threats. Not only are there more external threats, such as hackers and malicious codes, there are increased vulnerabilities from internal sources, both accidental and deliberate. Firms must proactively increase their IT security budget on the appropriate measures, including increased employee training, vulnerability assessment, and compliance with new regulations. This increased level of spending has become a "basic cost of business" in financial services and other industries, and will likely become required as well in many other industries, as the costs of failure to do so increase. The outlook for increased hiring of IT security specialists (the lone bright point in IT hiring in 2003) is one ramification of this trend; the dramatic increase in stock prices of IT security specialist firms is another. Ultimately, each firm must determine the most appropriate level of expenditure and the proper targets of IT security investment based on a careful analysis of vulnerabilities, costs of controls, and a return on investment approach to analysis. Many firms must increase their level of sophistication in this arena, and the role of the Chief Security Officer (CSO) may be expected to continue to grow. Every survey of top issues for IT managers now includes strategic focus on security management, and this trend is likely to strengthen in the coming years.

## References

- American Hospital Association (AHA), (2001)  
<http://www.aha.org/ar/Comment/PrivacyDetailB0330.asp>, 03/30/2001.
- Computer Security Institute, 2003 CSI/FBI Computer Crime and Security Survey,  
<http://www.gocsi.com>.
- Datamonitor, (2000) "eSecurity – removing the roadblock to eBusiness,"  
<http://www.datamonitor.com/viewnewsstory.asp?id=1375>.
- Deloitte Touche Tohmatsu, (2003) Global Security Survey 2003,  
<http://www.deloitte.com/dtt/cda/doc/content/Global%20Security%20Survey%202003.pdf>, 05/20/2003.
- Dubie, Dennis. (2003) "Corporate security spending not in line with real-world requirements," *Network World*, 05/05/2003.
- Enos, Lori. (2000) "Cyber crime Outpacing Security Spending", E-Commerce Times, 10/6/2000,
- Gaudin, Sharon. "Security Spending Bucks Downward Trend,"  
[http://itmanagement.earthweb.com/it\\_res/article.php/1552231](http://itmanagement.earthweb.com/it_res/article.php/1552231), 12/4/2002.
- Giga Information Group. (2002) News Release, 09/24/2002.
- Johnson, Julie. (2001) "Insurers hedging cyber-crime risk," *Crain's Chicago Business*, Col 24, Issue 50, 12/10/2001.
- Money* (anonymous), (2003) "Insurers require special policies to cover computer crime," *Money*, pg. 02b, 2003,  
<http://www.gigaweb.com/aboutgiga/0,2351,pressreleases,00.html?strPubID=MPR-032002-00004>,
- Sabbagh, Dan. (2003) "Internet security spending to soar," *The Times*, 08/27/2003.
- Security Stats.com, Computer Security Spending Statistics,  
<http://www.securitystats.com/sspend.html>.
- Tkaczyk, Christopher.(2003) "Crushing bugs," *Fortune (Europe)*, Vol. 148, Issue 5, p20, 9/15/2003.