HUMAN FACTORS AND MANAGEMENT DECISIONS

Impact Failure of Safety and Security Systems

Dr. Susan M. Smith[*] and Dr. George Kelley[**]

[*] *The University of Tennessee Safety Center*
[**] *Erie Community College-City Campus, Department of Business Administration*

Keywords: Crisis management, emergency management/response, computer security, preparedness

Abstract

The success of all security and safety measures involve managing the trade-offs between implementing the procedures and the inconvenience it causes the organization. Numerous security specialists consider the human factor to be the weakest link in managing security. Correctly determining the degree of inconvenience managers, workers, and customers are willing to accept and choosing an option that falls within this acceptance level will be a major factor in determining how well many security and safety procedures are implemented and followed. Many contemporary approaches to improved security stress planning, avoiding geographic concentration, diversifying communications/network systems, and installing high tech security equipment. This paper will discuss how these technological approaches to improved security and increase anti-terrorism measures can break down at the point of management implementation unless the importance of human factors is considered. Terrorists, hackers and con artists are attacking organizations at this vulnerable threshold of effective management implementation. Examples of how company management and court decisions to suppress or conceal research data identifying vulnerable security technologies has hindered correction of security problems will be discussed. Management strategies recommended to increase compliance and reduce security breaches are also identified.

Introduction

On Saturday, January 25, 2003, a "worm" later named "Slammer" (worms propagate by attacking a system while computer viruses spread through the exchange of files) crippled tens of thousands of computers worldwide. Within 10 minutes, the worm had spread to 67,000 computers worldwide. It clogged the Internet, slowing down ecommerce and email. The worm even disabled the Bank of America's cash machines.[1]

The irony of this attack (and similar attacks like "Code Red" and "Nimda") is that the worm took advantage of a known problem in Microsoft software. Microsoft had recognized the problem in July 2002, and had made available patches to fix the problem in its SQL Server 2000 software. SQL Server 2000 is a database product used mainly by large businesses, universities, and governments.[2]

Yet, six months later, many system administrators had failed to install the patches. The result: Internet congestion that increased download times by 50%, crashing networks, and rendering some web sites (and cash machines) completely unavailable for 24 hours. Emergency

[1] Levy, Steven. (2003) "Secrecy Rarely Works." *Newsweek.* 3/24. P. 39. ISSN 0028-9604
[2] Levy, p. 39.

dispatchers in Bellevue, Washington were reduced to taking notes with pen and paper when their computer network slowed drastically. "Slammer" even delayed flights.

Bruce Schneier, chief technology officer at Counterpane Internet Security, said the attack proves that relying on patches is flawed, "not because it's not effective, but because many [system administrators] don't install them."[3]

This is the fatal flaw of all security measures: there is a trade-off between implementing the procedure and the inconvenience it causes the organization. It's the degree of inconvenience managers, workers, and customers are willing to accept that will determine how much of the security procedures are implemented and followed.

In this case, the Microsoft SQL Server 2000 patch to fix the vulnerability made inconvenient demands on system administrators that many were unwilling to accept. Installing the patch takes valuable time. The patch itself could disrupt other systems and applications on the organization's network. So installing the patch would require system administrators and their staffs to test the patch out before fully installing it on the organization's network. All of this effort requires a knowledgeable system administrator and a savvy staff. Many organizations lack these resources. And many organizations feel they can't afford the inconvenience of shutting down their network for testing and installing software patches. Complicating this process is the trend of many companies to diversity their networks which adds an additional burden to an already complex process. So the result is many system administers ignored the problem—until Saturday, January 25, 2003—when their network crashed.

The larger issue is what is the vulnerability of business, university, and government computer systems to terrorist attacks. If a worm exploiting a known software flaw can cause this kind of havoc, what would a professionally designed terrorist worm do to all these vulnerable computer systems?

"Slammer" was able to scan 3.6 billion of the world's approximately 4 billion Internet addresses to find potential targets. "Slammer" doubled in size every 8.5 seconds during the first minute according to research published by the Cooperative Association for Internet Data Analysis (CAIDA). In 2001, the "Code Red" virus took 37 minutes (or 250 times as long) to double. This means that response times to react to computer viruses and worms are shrinking dramatically.[4]

In its 2001 survey of computer crime, the Computer Security Institute reported that 85% of the responding organizations had detected computer security breaches in the preceding 12 months. Additionally, 64% of the responding organizations reported they had experienced financial losses due to those computer breaches.[5]

"Technologies like authentication devices (for proving identity), access control (for managing access to files and system resources), and intrusion detection systems (the electronic equivalent of burglar alarms) are necessary to a corporate security program. Yet it's typical for a company to spend more on coffee than on deploying countermeasures to protect the organization against security attacks."[6]

[3] Mitnick, Kevin D. (2002) *The Art of Deception: Controlling the Human Element of Security.* P. 7. New York: Wiley. ISBN 0-471-23712-4.

[4] Levy, p. 39.

[5] Schweitzer, Douglas. (2003). "How to Toughen the Weakest Link in the Security Chain." *Computerworld.* 13/1 P. 71. ISSN 0955-0649.

[6] Mitnick, Kevin D. (2002) *The Art of Deception: Controlling the Human Element of Security.* P. 7. New York: Wiley. ISBN 0-471-23712-4.

Thesis

Security is always a question of balance. If an organization has too little security it's vulnerable. But too much security gets in the way of the organization's business. Many people in the security business regard the human factor as the weakest link in security solutions.[7] Too much security becomes a burden for the workers, a burden they will eventually find ways to ignore or circumvent which leads to the organization becoming vulnerable just when it thinks it's protected. Structuring security procedures is more of an art than a science.

Sources of Information

Two Bell Labs researchers, Steve Bellovin and Steven Cheswick, first coined the term "candy security." Like M&M candy, they described most computer security as "a hard crunchy shell with a soft chewy center."[8] The outer shell, called a firewall, is not adequate protection for a computer network because once it has been breached, the "soft chewy" security of the internal computer systems are exposed to the intruder.

How easy is it to breach a network's firewall?

On January 21 2003, Kevin D. Mitnick, legendary computer hacker, was released from the conditions of supervised release which prohibited him from using a computer and from acting as consultant or advisor in computer-related matters. Mitnick admitted to breaking into hundreds of computer networks. He later cooperated with authorities—even testifying before the U. S. Senate Committee on Governmental Affairs—on the need for legislation to ensure the security of the government's information systems. His favorite technique was to go "dumpster diving." Mitnick would dig through the trash outside the organization's building and find treasures like internal company telephone directories, computer manuals, employee lists, discarded printouts, memos, letters, reports; in short, valuable information that gave Mitnick ammunition to penetrate the organization's security system.[9]

It's interesting to note that as long as you're not trespassing, going through someone's trash is perfectly legal.

Many organizations think their systems are secure because they password protect everything. Nothing could be further from the truth. An analysis by the Oppenheimer Funds' Vice President of Network Security and Disaster Recovery showed that a standard software package that ran a password attack on the organization's network could effectively overwhelm the existing security procedures. The most common approach to password attack is to use a "dictionary" attack which searches for commonly used passwords by trying all of the words in an English dictionary supplemented by name lists, place lists, etc. The simulated attack managed to crack the passwords of 800 employees—within three minutes![10] Employees have to be trained to choose passwords that can't be easily cracked.

According to a survey conducted by the FBI and reported by the Associated Press in April 2002, 9 out of 10 large corporations and government agencies have been attacked by computer intruders. The survey also reports that only a third of the organizations publicly acknowledged any attacks. Clearly, most organizations felt that it was in their best interests not to alarm customers by making public disclosures. And they may have felt that admitting to breaches in their network security would invite more attacks by intruders who sensed their vulnerability.

[7] Siponen, Mikko T. (2000) "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice." *Information Management & Computer Security* 8/5 P.197-209. ISSN 0968-5227.
[8] Mitnick, p. 111.
[9] Mitnick, p. 137.
[10] Schweitzer, p. 78.

It's easy to project that the size and scope of the problem is greater than the survey results given the organizational reluctance to admit to breaches in security.

Findings and Discussion

"During the past thirty years, 80 percent of terrorist attacks on American targets have been directed at corporations.[11] As Raymond Aron points out, when government fails to cope with a problem, the private sector inevitably steps in.[12] In 1999, the United States had an expenditure on private security of $50 billion. That is larger than the defense budget of every other NATO nation. U.S. private security companies outspend U.S. public police agencies by 73% and employ more than two and a half times as many personnel. With attacks by "Slammer" and "Code Red" and other worms, corporations will increasingly turn to private security companies to protect their information assets and computer networks. In fact, government agencies may be forced to employ private security companies to protect them, too. The trend in the United States is toward "privatization" and slow government bureaucracies are no match for insidious computer viruses and worms.

Raymond Aron also points out that future wars will be different.[13] Clearly, taking out an opponent's computer network and information infrastructure will be a top priority in any military operation. At the same time, terrorists who are trying to cripple the communications, decision making structures, and information assets of an organization or country will target computer networks.

One month after the September 11 attacks on the World Trade Center, Morgan Stanley sold its nearly completed office tower in mid-town Manhattan. It also moved several thousand of its employees out of New York City in an effort to lessen the concentration—and vulnerability—of their business and personnel.[14] The chief lesson of September 11 for many companies was they had made themselves vulnerable by contracting with a single telecommunications provider. To reduce costs, many companies made the decision not to diversify their communications structure, but to concentrate it with a single provider for a lower price. In the aftermath of September 11 these companies learned they had committed a classic blunder: they chose a "single point of failure" option. When their phones and computers went out, they had no alternative communications.

But, as organizations, both governmental and private, diversify their communications and their computer networks, set up alternative work sites from their traditional business sites, to geographically decentralize the organization's vital assets, use multiple power grids and different communication switches, the increasing complexity offers opportunities to break the security weakened by the trend away from concentration of assets.

The irony is that by diversifying in the hopes that damage from terrorist attacks will be minimized, organizations are creating conditions where their security can be diminished. More sites mean more to protect. Different communication and network systems means more complexity and confusion providing opportunities for breaching security. As La Rochefoucauld said, "Countless acts that seem ridiculous have hidden reasons that are exceedingly wise and sound."

[11] Blythe, Bruce T. (2002) *Blindsided: A Manger's Guide to Catastrophic Incidents in the Workplace.* P. xi. New York: Penguin. ISBN 1-59184-007.

[12] Aron, Raymond. (2002) The Dawn of Universal History: Selected Essays from a Witness of the Twentieth Century P. 111. New York: Basic Books. ISBN 2-00-200440-5.

[13] Aron, p. 222.

[14] Laye, John. (2002) Avoiding Disaster: How to Keep Your Business Going When Catastrophe Strikes. P. 243. New York: Wiley. ISBN 0-471-22915-6.

"35% to 50% of businesses impacted by disasters do not survive. In recent cases the corporate names have continued, but the leadership departed and the companies were considerable downsized."[15] The experience with "Slammer" shows that future "catastrophes" will likely involve computer worms and viruses with the power to disrupt or disable hundreds of thousands computer networks. The inconvenience of updating security software coupled with the increasing "overhead" for security in general sets a condition for many organizations that leads to eroding protection. But, for many companies, a crashed network for a long period of time will put them out of business. The stakes for business survival have been increased dramatically.[16]

Strategies for Survival

Factors that make organizations more vulnerable to breaches in security are:

- Large number of employees
- Multiple facilities
- Information on employee whereabouts left in voice mail messages
- Phone extension information made available
- Lack of security training
- Lack of data classification system
- No incident reporting/response plan in place
- Multiple networks
- Not installing security patches

Warning signs of an attempted security breach:

- Refusal to give a callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

Common Targets

TARGET TYPE	EXAMPLES
Unaware of value of information	Receptionists, telephone operator, security guards, administrative assistants
Special privileges	Help desk or technical support, system administrators, computer operators, telephone system administrators
Manufacturer/vendor	Computer hardware, software manufacturers, voice mail systems vendors
Specific departments	Accounting, human resources[17]

As technological advancements in security progress, the failure of employees not to adhere to the organization's security policies will continue to be the fatal flaw in protecting the

[15] Laye, p. 50.
[16] Hawkins, Steve. (2000) "Disaster Recovery Planning: A Strategy for Data Security." *Information Management & Computer Security* 8/5 P. 222-230. ISSN 0968-5227.
[17] Mitnick, p. 333.

organization. Human factors in decision making (like not implementing security patch upgrades), inadequate information security awareness, education and training, ignoring burdensome security procedures, taking "shortcuts," and underfunding security in general will lead to the next round of security breaches.[18]

Simple yet effective steps include upgrading to the newest operating system once a quarter: just this basic step would result in a 25-fold reduction of risk of a security breach.

Human factors come into play directly when dealing with email. Email messages can include file attachments that hackers can use to send inflected files. With a clever subject line (like the "I LOVE YOU" virus) recipients can be enticed to open inflected files. This is exactly what happened with the AnnaKournikova worm, the Melissa virus, and the Naked Wife Trojan horse. The National Infrastructure Protection Agency[19] offers the following advice to mitigate these types of threats: [20]

1. Close the preview pane of your email program
2. Disable the JavaScript and ActiveX features of your Web browser.
3. Maintain the most current version of an antivirus program
4. Save attachments to a disk before opening.
5. Do not open email attachments from strangers.
6. Be suspicious unexpected email from someone you know.
7. Verify suspicious email.

Another protective measure is to download an antivirus test from the European Institute for Anti Virus Research (EICAR) at Eicar.com. The file can't spread or cause any damage, but it can tell you if your antivirus protections are working.[21]

Many organizations rely on "The FUD Factor" approach to security. The use "Fear, Uncertainty, and Doubt" to intimidate their workers into following security procedures. "Do this or your data will be lost forever!" uses fear as a short-term motivator, but many workers get cynical with type of approach and return to their previous behaviors with security "shortcuts."[22] Other organizations try to hide their vulnerabilities behind court decisions that prohibit their suppliers from fixing known security problems. Should the approach be to report flaws in security systems or bury them in hopes they won't be exploited? Security by obscurity is a bad idea.[23]

Strategies to improve overall security include better training of employees, to encourage them to verify the identities of non-organizational contacts, increasing budgets for security software upgrades and patches, and to bolster security at the likely points of attack.[24]

[18] Siponen, Mikko T.

[19] Schweitzer, p. 76.

[20] Levy, 39.

[21] Tuesday, Vince. (2001) "Human Factor Derails Best-Laid Security Plans." *Computerworld.* 11/4 P. 36. ISSN 0955-0649.

[22] Hawkins, Steve. (2000) "Awareness and Challenges of Internet Security. *Information Management & Computer Security* 8/3 P. 131-143. ISSN 0968-5227.

[23] Siponen, Mikko T. (2000) "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice." *Information Management & Computer Security* 8/5 P.197-209. ISSN 0968-5227.

[24] Vermeulen, Clive. (2002) "The Information Security Management Toolbox—Taking the Pain out of Security Management." *Information Management & Computer Security* 10/3 P. 119-125. ISSN 0968-5227.

Biographical Notes

Dr. Susan M. Smith is Director of The University of Tennessee Safety Center and an Associate Professor at the Department of Health and Exercise Science in Knoxville, Tennessee. She teaches graduate courses in emergency management, accident prevention and environmental health. Dr. Smith's research includes: emergency evacuation and warning systems affecting special populations; and the evaluation of effective management strategies to achieve disaster mitigation.

Dr. George Kelley is Professor of Business Administration at Erie Community College-City Campus in Buffalo, New York. Currently, Dr. Kelley is part of a research training team working with General Motors to train GM employees and UAW workers in the Paid Educational Leave (PEL) program. He has also worked as a consultant for Occidental Chemical and several government agencies. Dr. Kelley's research interests focus on practical strategies to improve management effectiveness.

Sources

Aron, Raymond. (2002) The Dawn of Universal History: Selected Essays from a Witness of the Twentieth Century. New York: Basic Books. ISBN 2-00-200440-5.

Blythe, Bruce T. (2002) Blindsided: A Manger's Guide to Catastrophic Incidents in the Workplace. P. xi. New York: Penguin. ISBN 1-59184-007.

Hawkins, Steve. (2000) "Awareness and Challenges of Internet Security. Information Management & Computer Security 8/3 P. 131-143. ISSN 0968-5227.

Hawkins, Steve. (2000) "Disaster Recovery Planning: A Strategy for Data Security." Information Management & Computer Security 8/5 P. 222-230. ISSN 0968-5227.

La Rochefoucauld, Francois. (1665) Maxims. New York: Penguin. ISBN 0-14-044095-X.

Laye, John. (2002) Avoiding Disaster: How to Keep Your Business Going When Catastrophe Strikes. P. 243. New York: Wiley. ISBN 0-471-22915-6.

Levy, Steven. (2003) "Secrecy Rarely Works." Newsweek. 3/24. P. 39. ISSN 0028-9604.

Mandel, Robert. (2002) Armies Without States: The Privatization of Security. Boulder, Colorado: Lynne Rienner Publishers. ISBN 2-00-105942-6.

Mitnick, Kevin D. (2002) The Art of Deception: Controlling the Human Element of Security. P. 7. New York: Wiley. ISBN 0-471-23712-4.

Schweitzer, Douglas. (2003). "How to Toughen the Weakest Link in the Security Chain." Computerworld. 13/1 P. 71-78. ISSN 0955-0649.

Siponen, Mikko T. (2000) "Critical Analysis of Different Approaches to Minimizing User-Related Faults in Information Systems Security: Implications for Research and Practice." Information Management & Computer Security 8/5 P.197-209. ISSN 0968-5227.

Tuesday, Vince. (2001) "Human Factor Derails Best-Laid Security Plans." Computerworld. 11/4 P. 36-41. ISSN 0955-0649.

Vermeulen, Clive. (2002) "The Information Security Management Toolbox—Taking the Pain out of Security Management." Information Management & Computer Security 10/3 P. 119-125. ISSN 0968-5227.