Computer Abuse by Trusted Employees

Sandra J. Blanke
University of Dallas, 7460 Warren Pkwy, Suite 100, Frisco, TX 75034
Phone: 817-456-4101
sblanke@gsm.udallas.edu

Brett J. L. Landry
University of Dallas, 7460 Warren Pkwy, Suite 100, Frisco, TX 75034
Phone: 972-636-8633
blandry@gsm.udallas.edu

ABSTRACT

Computer abuse continues to be a problem for organizations both small and large. More than half of the computer abuse losses were due to trusted employees and other authorized users. Computer Security Policies (CSPs) are often incomplete and not implemented correctly within organizations. General Deterrence Theory (GDT) provides a sound research theory for utilizing CSPs as a security countermeasure based on prevention, deterrence, detection, and prosecution for employee computer abuse. This research explores a computer security incident at a small commercial real estate firm. When one employee is terminated, another employee that happens to be a relative feels compelled to help the terminated employee by providing physical weekend access to the firm and electronic access to the firms' computer system. The terminated employee takes advantage of the situation and the relatives' generosity, resulting in a breach of available system information, removal of confidential contact information from the firm, and may possibly have made changes to the data in the system breaching the integrity of the firms' information. After the incident the owner takes some very necessary next steps. The owner reviews the existing computer security policy and has the policy rewritten and re-implemented within the organization.

INTRODUCTION

Computer Abuse continues to be a problem for organizations both small and large. Mujtaba, Griffin, and Oskal (2004) indicated that American businesses will lose $63 billion each year due to employees' computer abuse on the Internet. The terms computer abuse, computer crime, computer misuse, Internet abuse, and unauthorized use are noted in the literature and refer to inappropriate, unethical, and illegal activities involving computer systems (Gordon et al., 2006; Parker, 1998; Siau, Nah, & Teng, 2002; Straub, 1986). Aytes and Connolly (2004) acknowledged that despite the rapid technological advances in computer hardware and software,

computer abuse by employees continues to be a significant source of direct expense and productivity loss.

GENERAL DETERRENCE THEORY

An early study on computer abuse by Straub (1986) was focused on deterrent countermeasures in computer security and utilized the General Deterrence Theory (GDT). Straub and Nance (1990) reported that while many business organizations have tried to implement the solutions indicated by GDT, the frequency and volume of computer abuse are expected to continue increasing as highly sophisticated employees engage in computer abuse. The foundation for GDT is the criminological theory of general deterrence (Straub, 1990). GDT focuses on disincentives or sanctions against committing a deviant act. In IS, security officers use deterrents to monitor and enforce policy, distribute information about Computer Security Policies (CSPs), detection of computer abuse and prosecution as required (Straub).

COMPUTER ABUSE

In a study of 494 IT professionals, 46% reported having a computer abuse incident within the past 12 months (Richardson, 2007). The average annual computer abuse incident loss was $350,424 as compared to $168,000 for the previous year. Additionally, respondents reported 64% of the computer abuse losses were due to employees, and others classified as insiders to the business environment (Richardson).

According to Gordon, Loeb, Lucyshyn, and Richardson (2006), 52% of the 616 U.S. computer security practitioners' surveyed by the Computer Security Institute, reported they have had computer abuse incidents as recently as within the last 12 months. Straub (1986) reported computers for all their "intricacy, mystique and power, computer systems are subject to abuse as human systems, and failing to perform in the manner intended, can endanger the very business they were designed to serve" (p. 1). Some individuals use technology for good causes while others use it ineffectively and in nonproductive or reckless ways (Mujtaba et al., 2004). The computer generally accepted as a positive technology is being used to commit traditional crimes such as fraud, gambling, and to destroy or gain unauthorized access to data.

Computer Security Policy Awareness

According to Aytes and Connolly (2004) as well as Gordon et al. (2006), although businesses have attempted to deal with employee computer abuse with Computer Security Policy Awareness (CSPA), the problem of employee computer abuse still exists. Bosworth and Kabay (2002) stated that, "security policies are the basis for security awareness, training, and education" (p. 28). As stated by Harris (2003), the purpose of the CSPA is that "each employee needs to know what they can or cannot do. Expected responsibilities and acceptable behaviors need to be clarified and noncompliance repercussions that could range from a warning to dismissal need to be explained" (p. 94). According to Lee and Lee (2002), CSPA is meant to deter computer abuse

by defining acceptable, unacceptable, and illegal behavior. Additionally, Lee and Lee noted that additional empirical studies are needed to better understand the importance of CSPA when investigating the intention to commit computer abuse.

According to Bosworth and Kabay (2002), CSP are the basis for security awareness, training, and education. Whitman (2004), reported a good security policy should "outline individual responsibilities, define authorized and unauthorized uses of the systems, provide venues for employee reporting of identified or suspected threats to the system, define penalties for violation, and provide a mechanism for updating the policy" (p. 52).

As reported by Harris (2003), the purpose of the CSPA is that each employee needs to know what they can or cannot do according to CSP. Most organizations of at least moderate size now have some type of security policy in place to protect information resources (Lee and Lee, 2002). CSPA programs are expected to reduce computer abuse (Lee & Lee). According to Rose and Tom (1989) as well as Parker (1998), CSPA programs have been ineffective in practice since employees perceive CSPA as difficult to learn, inconvenient, and restricting their freedom.

Ineffective Policies

Mirchandani and Motwani (2003), reported in a survey of 192 manager responses from 66 companies, "the most widely used measure-having a written company policy barring Internet abuse … is also considered one of the least effective" (p. 55). According to Aytes and Connolly (2004) as well as Gordon et al. (2006), while some businesses have attempted to deal with employees' computer abuse with CSPA, the problem of employees' computer abuse still exists. Both Aytes and Connolly indicated additional research is needed on CSPA.

Petruich and Motuk (2004) state the ability of an employee to "understand the business computer security policy is paramount to ensuring that the policies are followed. It is better to provide the information proactively to the employee rather than spend time and thus capital recovering from a severe violation" (p. 48).

In a study of 219 technology managers in a large organization in the UK, the results indicated there is no statistically significant relationship between the adoption of CSP and the accompanying levels of computer abuse (Doherty & Fulford, 2005). Additionally, Doherty and Fulford stated "given that nearly all the respondents in our study claimed to be actively disseminating their policies, questions must be raised about the effectiveness of their dissemination strategies, in light of the consistently high levels of security breach witnessed" (p. 34). Hone and Eloff (2002) stated "a common failure of information security policies is that they fail to impact users on the ground" (p. 15). According to Orshesky (2003), CSPA "needs to reinforce the security message and explain why security is our issue … people need to be able to recognize a security incident or violation and know what to do about it" (p. 46). Foltz et al. (2005), survey results suggested that 76% of respondents had not read the computer policies. All of these point to the results of ineffective policies on a firm's information system.

Security Countermeasures

Parker (1998) as well as Straub and Welke (1998) recommend business environments implement security countermeasures to control IS computer abuse. These security countermeasures should include a combination of procedural controls (security policy statements, acceptable usage guidelines, security awareness education and training, as well as technology controls such as biometric devices, filtering, and technical controls.

According to Dhillon and Backhouse (2000), with many organizations facing pressure of organizational cost containment and external competition, many companies are rushing headlong into adopting technology without carefully planning and understanding potential security issues. Other organizations are realizing that they do not have the expertise in managing their technology and have turned to Managed Service Providers (MSP) to maintain IT resources. The MSP is a firm that manages its clients' IT support and security needs, by deploying its personnel or though Internet Monitoring.

The next section explains an actual computer security incident researched in a small firm where the CSP addressed only the need for changing passwords. The names of the individuals are disguised at the request of the company.

Computer Abuse Post Termination Incident

The organization studied was a small commercial real estate corporation with less than 20 employees. There is no IT expertise within the corporation so they contracted a MSP for their IT resources. When an employee (Bob) was given two weeks notice by the owner of the company (Terry), Bob immediately became visibly upset and announced he was leaving and did not want or need the two weeks notice. Since this is a small company Terry had limited experience with terminating employees and had never anticipated this reaction by Bob.

Terry called in the lead accountant of the firm (Sarah), explained what had just happened, and instructed her to call their MSP. In this small business employees have many job responsibilities and Sarah (the accountant) long ago had been assigned as the primary contact for the MSP. Sarah, Terry, and the MSP discussed the situation and they all agreed the best approach was to just change the password on the email account and leave the email ID in place. Sarah and Terry did not want to delete the email account as important emails would still be coming to Bob from important clients. Terry and Sarah would assign someone else in the business to Bob's real estate accounts the following Monday morning. Later on that evening Bob realized his contact information was all at the office. He really did want to get some of his contact information and his personal items. The next day Bob contacted Sarah and explained he only needed his personal contact list and personal items from his office. Bob asked Sarah to meet him at the office and she agreed.

In this small commercial real estate firm they hire relatives. Sarah is Bob's mother. Sarah agreed to meet Bob at the office for his personal items. When at the office Sarah provided

Bob the new password and then attended to some of her work responsibilities. Bob worked in what was his office packing the personal items and using his computer. It is estimated that Bob was in his former office about two hours.

On Monday morning when employees arrived at the office one of the employees (Katie) was assigned the task of going into Bob's email account to read the emails and notify his clients that he was no longer with the firm. When Katie signed onto Bob's email account there were no emails, no contact list, nothing in the sent folder, nothing in the trash folder, and only a few emails from Sunday in the inbox. Immediately Katie knew this situation was not normal and set out to find Sarah. Katie explained there were no emails and nothing on the computer. Sarah immediately realized that she had made a critical mistake by letting Bob come to the office and access his email account over the weekend. How could Bob do this? Bob only said he wanted his personal contact information and a few person items from his office. Sarah knew this was her fault and that she needed to apologize and explain to Terry what had happened. Sarah never thought her son would do this and she never thought Bob would put her job and her reputation at risk. As Sarah explained the situation Terry listened. Together they called the MSP and explained what they thought had happened. The MSP again changed the email password and let Terry, Sarah and Katie know they would need to perform a tape restore. This would mean the system would be restored as of Friday night. The only emails they could not retrieve were the messages that came in on Saturday or Sunday. Sarah, Katie and Terry felt this would cause only minimal issues with only a few lost emails.

The Data Loss

There are major impacts of Bob's action in terms of the three main principles in security regarding Confidentiality, Integrity, and Availability (CIA). The company focused on the latter, availability. The missing email constituted a loss of availability. The email was restored and most of the information was recovered. In terms of data loss this is minimal, but there is a good chance that key correspondence was lost. The real problem is that confidential information in terms of emails and client contacts have been stolen by Bob. There is a very real possibility that Bob may have taken other key documents; contracts, trade secrets, logos, non-disclosure agreements, leases, etc.

Additionally, did Bob go and change any other data while he was logged in? If so, the firm has lost the integrity of their system. From Sarah's perspective, email was lost so she contacted the MSP and told them that a terminated employee logged in with a legitimate password and deleted email. The MSP then reset Bob's password and restored the email. The MSP did not examine data integrity because they were not asked to and the reality is that it would be cumbersome and most likely a billable expense to search the servers for files that had changed on Saturday morning.

Lastly, the firm has a disloyal employee that has compromised the organization by allowing her son to gain access to the systems after he was terminated. What other activities could Sarah be involved in? Will she allow Bob back in? Will Terry be able to trust Sarah in the

future? Should Sarah be allowed to stay at the firm or be asked to leave? All of these were concerns that had to be addressed by the firm.

In this specific incident, Terry realized the existing high level CSP needed to be enhanced. He assigned a different employee to work with the MSP to enhance and introduce the revised CSP in the firm. The owner is now fully supportive of the CSP and provides on the job time for computer security training and awareness. The MSP was also given some additional responsibilities for tracking usage, reporting, and security of the system. The former trusted employee after a short time was deemed a risk and terminated by the owner.

CONCLUSION

This case provides support to the literature that reports, while many companies have CSPs many are incomplete. GDT is important to this research as it provides the guidelines for creating complete CSPs. CSPs may be used as a security countermeasure when they define the authorized and unauthorized uses of the systems. CSPs based on GDT work to prevent computer abuse, deter computer abuse, detect computer abuse, and prosecute for computer abuse as necessary. In this case, management has accepted the responsibility of updating their CSPs based on the guidelines in the literature and fully implementing the CSP with a complete and ongoing security awareness program. The owner of the firm has provided the authors of this case permission to share this security incident in other that other businesses may learn from this case and not experience a similar trusted employee security incident.

REFERENCES

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing, 16*(3), 22-40.

Bosworth, S., & Kabay, M. (2002). *Computer security handbook* (4th ed.). New York: John Wiley & Sons Inc.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Doherty, N., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Foltz, C., Cronan, T., & Jones, T. (2005). Have you met your organization's computer usage policy? *Industrial Management + Data Systems, 105*(1/2), 137-146.

Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. (2006). CSI/FBI computer crime and security survey. Retrieved July 20, 2006, from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml

Harris, S. (2003). *All in one CISSP exam guide* (3rd ed.). New York: McGraw Hill.

Hone, K., & Eloff, J. (2002). Information security policy: What makes an effective information security policy. *Network Security, 20*(6), 14-16.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security, 10*(2), 57-63.

Mirchandani, D., & Motwani, J. (2003). Reducing internet abuse in the workplace. *S.A.M. Advanced Management Journal, 68*(1), 22-26.

Mujtaba, B., Griffin, C., & Oskal, C. (2004). Emerging ethical issues in technology and countermeasures for management and leadership consideration in the twenty first century's competitive environment of global interdependence. *Journal of Applied Management and Entrepreneurship, 9*(3), 34-55.

Orshesky, C. (2003). Beyond technology – the human factor in business systems. *The Journal of Business Strategy, 24*(4), 43-47.

Parker, D. (1998). *Fighting computer abuse – A new framework for protecting information.* New York: John Wiley & Sons.

Rose, K., & Tom, R. (1989). Computer security. Who's minding the store. *Academy of Management Executive, 3*(1), 63-66.

Richardson, R. (2007). CSI computer crime and security survey. Retrieved May 6, 2007, from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml.

Siau, K., Nan, F., & Teng, L. (2002). Acceptable internet use policy. *Communications of the ACM, 45*(1), 75-79.

Straub, D. W. (1986). Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment. *Dissertation Abstracts International, 48*(04), 813. (UMI No. 8710538)

Straub, D., & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly 22*(4), 441-469.

Whitman, M. (2004). In defense of the realm: Understanding threats to information security. *International Journal of Information Management, 24*, 3-4.