2010

Preventing Security Breaches in Business

Pearl Jacobs
Sacred Heart University, jacobsp@sacredheart.edu

Linda Schain
Hofstra University

Preventing security breaches in business

Pearl Jacobs
Sacred Heart University

Linda Schain
Hofstra University

ABSTRACT

Technological advancements are constantly changing the world we live in. These advancements are not only changing how we work but also the security of our workplace. High level white collar crime is rapidly becoming a fact of corporate life. Businesses want to avoid becoming victims of these white collar criminals so they attempt to institute controls on all aspects of their operations. These controls are far from 100% effective. Businesses need to take a different approach to the prevention of white collar crime. Perhaps more effective prevention programs can be developed by exploring the various theories of crime causation and applying these theories to business practices.

Since crime is perpetrated by human beings, it is important to understand what causes individuals to engage in such behavior. This understanding would lead to more effective methods of prevention. This paper will examine several behavioral sciences theories as they relate to the development and prevention of white collar crime. It will also provide a more effective plan for preventing white collar crime.

Keywords: Industrial Psychopath, Groupthink, Information Exchange Theory

INTRODUCTION

An article in the business section of The Journal News, a local newspaper in Westchester County, New York, described some of the proactive measures businesses are taking to ensure security. The article mentioned a company that, "sells barricades that can stop a suicide bomber's truck moving at high speed before impact with a building, as well as high-strength doors and windows designed to resist explosions and bullets" (Loomis 2005:D1). The company is marketing its equipment to businesses. This article in a local newspaper and many others demonstrates the increasing concern for security in all aspects of life including business. While most businesses may not be overly concerned with physical security, they are increasingly more concerned with the security of their business records. They are constantly seeking the most sophisticated hardware devices and software programs to provide this security. Despite these efforts, security breaches continue to occur in businesses. Obviously, a breach in the security of a company's information system can have a catastrophic effect. How can businesses find or develop the best method of securing their information systems? Perhaps the answer lies in understanding theories that relate to the development of white collar crime. The application of such theories may lead to more effective prevention strategies. Thus, this paper will explore various theories as they relate to the development and prevention of white collar crime and propose a more effective prevention plan based on the theories.

PERPETRATORS OF CORPORATE CRIME

The possibility of falling victim to white collar crime is rapidly rising. To increase public awareness, the FBI website routinely lists various examples of cyber scams and other types of white collar crimes. Not much attention is given to why these crimes occur in the first place. Most individuals say it is a combination of greed and dishonesty that accounts for white collar crime. This may not be an accurate or fair explanation. Criminologists often use routine activities theory to explain white collar crime. This theory suggests that there are three factors that lead to criminal behavior. They are motivated offenders, the availability of suitable targets, and the lack of capable guardians (Cohen and Felsen, 1979). If the potential offender values the target and sees little chance of detection or punishment, the potential offender will pursue the target. Companies that don't have protection software on their systems and don't properly educate their employees to be alert for potential security breaches may fall victim to such crimes.

In order to protect assets, businesses must not only consider software and hardware solutions but they must also consider the human factor. Businesses are affected by the societal environment. If people believe that others are making money easily, they will want to as well. The prospect of easy money becomes the suitable target. People will even take risks to obtain this easy money because not to take the risk would mean they are passing up a once in a lifetime opportunity. If a company's data system seems unsecured, it becomes a suitable target lacking the guardian to protect it. The motivated offender takes advantage of that. Businesses must secure their systems and let everyone know they are doing so. Individuals should know they are being watched. The guardians are in place. When the risks are higher the temptation diminishes. Thus, protection systems should be designed with the understanding that individuals can be lured into criminal behavior if their desired target is not well guarded. They will take the risk. Businesses may reduce the tendency to take a risk if they make it clear that their information systems are in place in order to provide security for their assets. It should also be common knowledge that individuals who attempt to steal assets will be punished. The certainty of punishment is a powerful deterrent.

There is another characteristic of the criminal that we tend to ignore yet is essential to our understanding of criminal behavior. Most individuals who commit crimes are not unlike the lawful individual. That is they strive to see themselves in a positive way. How can an individual

violate the trust of their employers and still see themselves in a positive way? This is done through the process of neutralization or rationalization. The corporate criminal rationalizes that the criminal behavior engaged in is not criminal at all. The prevention of white collar crime requires that the negative aspects of the act be emphasized and any attempts at neutralization or rationalization be discouraged. Individuals must see their actions as criminal in order to deter the criminal behavior. Businesses must stress that the theft of assets is not just a violation of trust but it is a serious crime that will be prosecuted. Once again, the certainty of punishment is a strong deterrent.

Donald Cressey (1973) formulated the fraud triangle. Fraud is a form of white collar crime. Cressey noted that in addition to rationalization and opportunity, pressure is a factor in most cases of fraud. Businesses must recognize the affect that extreme pressure can have on employees and not make unrealistic demands. It is the extreme pressure caused by management's unrealistic demands that pushes some otherwise lawful individuals into crime. They view the crime not as criminal but rather necessary to secure their continued employment. It is perceived as the only way to secure their employment. Thus, it becomes an act of desperation caused by the overwhelming pressure placed upon the employee by management.

THE SOCIAL ENGINEER

How can people who have never committed a criminal act in their lives and don't perceive themselves as under extreme pressure be drawn into serious criminal behavior? Some social scientists use the term social engineering to explain this (Ramamoorti, 2008). It refers to the manipulation of people through deception. The social engineer is an individual capable of convincing people of anything. He is then able to take advantage of people in order to get information. He can do this without the use of technology. The social engineer knows that it is easier to compromise people than to compromise security systems. Simply building a better security network will not guarantee protection. People are the weakest component of any security system. Thus, employees must be able to recognize the characteristics of the social engineer in order to avoid victimization.

INDUSTRIAL PSYCHOPATHS AND PERSUASION

A pleasant personality is an asset in business. It is easier to persuade people if one possesses a pleasant, nice, agreeable personality. The industrial psychopath, however, uses his pleasant personality to commit crimes. The industrial psychopath uses persuasion to achieve illegitimate gains (Barbiak, 2000). This individual makes his way up the corporate ladder taking what he wants from the business through a series of deceptive steps. He begins his persuasive techniques when he enters the organization. He is very pleasing and charming. Once inside the organization, he assesses those who can be useful to him and he begins to charm them. He is now in a position to manipulate people and information to achieve his illegitimate goals. Once these goals are achieved, the industrial psychopath must get rid of those no longer useful to him. He neutralizes them by challenging their competence or their integrity. The psychopath has reached the top level of the corporate hierarchy. He has achieved his goal of being in power. Since industrial psychopaths can do severe damage to a business, employers and employees must learn the characteristics of an industrial psychopath and be alert for evidence of this behavior.

AVOID GROUPTHINK WITH INFORMATION EXCHANGE THEORY

Another way to avoid victimization is to create a business environment that encourages employees to present their ideas and feel free to comment and disagree with presented ideas without fear of punishment or retaliation. Business decisions should not be made based upon

groupthink. Groupthink occurs when individuals agree with a group leader in an effort to maintain the cohesiveness of the group. Opposing opinions are quickly discounted. The solidarity of the group is viewed as more important than honest opinions. Groupthink prevents individuals from recognizing fraud and should be avoided at all costs. Individuals should be encouraged to present their own opinions even if they are contrary to the majority opinion. Janis (1972) has shown how groupthink can lead to tragedy in an effort to maintain solidarity. The Kennedy administration's support of the Bay of Pigs invasion in Cuba is a case in point. Several members of the cabinet had doubts about the plan but failed to mention them in an effort to maintain the solidarity of the group (Janis, 1972). Businesses must encourage frank and honest debate in order to monitor the control system. Dissent must not be viewed as negative.

Perhaps one way of avoiding groupthink is to apply information exchange theory (Cohen and Silver, 1989). It studies the relationship between an individual's status within a group and the ability to generate both positive and negative evaluations of problem solutions. Different ideas lead to effective problem solution. Negative evaluations are particularly important in this process because they provide the means for examining different solutions. Group members may hesitate to express negative evaluations because it can result in their loss of status within the group (Cohen and Silver, 1989). Thus, group members have a tendency to repress controversial ideas when there is a risk of status loss. Yet dissent is essential to accurate decision making. How do we encourage dissent? The answer is depersonalizing the negative evaluation. Research by Troyer and Youngreen (2009: 421) confirms that, "the presence of negative evaluation in group interaction, when focused on ideas and not individuals, does spur greater creativity in group problem solving."

In order for businesses to avoid fraud and information loss there must be an open and penalty free atmosphere for individuals to express their ideas. Depersonalization may be one way of accomplishing this. Suggesting that the solution is not a good one rather than your solution is not a good one reduces the risk of status loss and encourages the generation of ideas both positive and negative.

GROUP NORMS

The establishment of group norms that promote independent thought may avoid groupthink and generate more effective solutions to business problems. A group norm may be defined as a standard of behavior accepted by the group. It defines appropriate behavior within the group (Postmes and Spears, 2001). Group norms can promote consensus or diversity. Cialdini and Goldstein (2004) found three factors that might affect group conformity. They describe them as the accuracy goal which causes individuals to conform to the established behavior norm. The second factor is the affiliation goal which causes individuals to conform based on the need to be part of the group. The final factor is the self-enhancement goal which causes people to conform because the individual's self-concept is based on his perception of the way others see him. Businesses may avoid groupthink by promoting independence of thought as a group norm while retaining the cohesiveness of the group.

A MORE EFFECTIVE PLAN

There are reasonable steps that businesses can take to avoid victimization. They are as follows:

1. Make sure there are proper internal controls. Internal controls are elements that protect resources and lessen liability. They encompass business policies and staff responsibilities for securing assets and maintaining records. There should be absolute segregation of responsibilities to avoid criminal temptation. For example, the employee handling an

asset should not have the responsibility for the accounting records for that asset. The Sarbanes-Oxley Act of 2002, Section 404, states that it is management's responsibility to develop and maintain a company's internal control system. It is the auditor's responsibility to report management's claim about the efficacy of their internal control system (McConnell and Banks, 2003).

2. Employees must receive good training not merely adequate training to avoid victimization. This may require regular training sessions to keep employees up-to-date on various fraudulent schemes.
3. Employees must be properly and effectively supervised. They should be aware that their actions are being observed daily and that there work will also be reviewed while they are on vacation. It is important for employees to know that their actions are not only being observed but evaluated as well. This reduces the temptation to act inappropriately.
4. Businesses should make it known to all that perpetrators of criminal activities will be prosecuted. There will be no exceptions. This is vital. Crime is deterred in part by the knowledge that such activities will be prosecuted and that there will be no leniency or exceptions.
5. Businesses should make every effort to have and use the most current crime prevention policies, procedures, and programs. Criminal schemes are constantly evolving with the advent of new technology. Business crime prevention programs must keep current as well.
6. Every member of the organization must accept the policies in order to create a strong ethical culture. Supervisors must demonstrate their compliance in order to gain acceptance from all employees.
7. Supervisors must observe the decision making processes of their employees. In so doing, they can assess their commitment to proper business ethics.
8. Be suspicious and alert. The motivated offender is always out there.
9. Support an atmosphere that encourages individuals to identify potential risks of fraud. Employees should be made to feel that notification of potential risks is valued by the employer.
10. Encourage and support whistleblowers. These individuals serve a vital function. They are necessary and should be assisted and encouraged.

CONCLUSION

There seems to be a never ending supply of motivated offenders. We can continue to try to create crime resistant software and hardware. If the past is any indication of the future, these efforts will only be successful for a brief period. The motivated offender will eventually find a way around security systems. Understanding why individuals are drawn to white collar crime in the first place is the key to creating effective deterrents.

Businesses that place increasing pressure on employees create an atmosphere conducive to criminal activity. The employee fearing the loss of employment or status feels compelled to engage in unlawful activity. The pressure that leads the employee to crime also enables the employee to neutralize or rationalize the behavior and not view it as criminal but necessary and reasonable.

When a society values economic success more than conformity to appropriate norms of behavior, the norms lose their power to regulate behavior and the result is unethical or criminal business practices. Strain occurs when an institution fails to provide for the needs of employees. This failure results in a sense of alienation. This condition can lead to harmful and criminal acts. Strain can also occur when businesses institute policies that make success unattainable for most employees. The extreme strain that is generated leads to crime. In order to avoid recognizing that appropriate behavior norms have been violated, individuals seek to rationalize the criminal

behavior. They provide an "ends justifies the means," explanation or rationalization (Donegan and Ganon, 2008).

Technological advances constantly present new opportunities for crime. It may not be feasible nor economically expedient to try to develop crime resistant software and hardware to protect businesses. It would be much more effective to monitor the individuals employed in a business. Maintaining a business environment free of the stressors that may cause some employees to engage in criminal activity is recommended as a more successful way of preventing white collar crime.

REFERENCES

Babiak, P. (2000). "Psychopaths in the Organization." Presentation delivered at the Eleventh Annual Meeting of the American Neuropsychiatric Association, Fort Myers, FL, February 20-22.

Blickle, Gehard and Schlegel, Alexander. (2006). "Some Personality Correlates of Business White-Collar Crime." *Applied Psychology*, Vol. 55, 220-233.

Box, Ron. (2010). "Firm Up Your Data Security." *Journal of Accountancy*, Vol. 206, Issue 6, p18.

Cialdini, R.B. and Goldstein, N.J. (2004). " Social Influence: Compliance and Conformity." *Annual Review of Psychology*, Vol. 55, 591-621.

Cohen, I. and Felsen, M. (1979). "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review*, Vol. 44, 588-608.

Cohen, B.P. and Silver, S. D. (1989). "Group Structure and Information Exchange: Introduction to a Theory." In J. Berger, M. Zelditch Jr. and B. Anderson (Eds.), *Sociological Theories in Progress: New Foundations* (pp. 160-181). Newbury Park, CA: Sage.

Cressey, Donald. (1973). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Montclair, N.J.: Patterson Smith, 1973.

Donegan James, J. and Ganon, Michele W. (2008). "Strain, Differential Association, and Coercion: Insights From the Criminology Literature on Causes of Accountant's Misconduct." *Accounting and the Public Interest*, Vol. 8, 1-20.

Dorminey, Jack W., Fleming, Arron Scott, Kranacher, Mary-Jo, and Riley, Jr. , Richard A. (2010). "Beyond The Fraud Triangle." *The CPA Journal*, July, 17-23.

Janis, I. L. (1972). *Victims of Groupthink*. Boston: Houghton-Mifflin.

Loomis, Jay. (2005). "Hotels Have Room to Improve Security." *The Journal News*, Nov. 11, D1.

McConnell, Donald K., Jr. and Banks, George Y. (2003). " How Sarbanes-Oxley Will Change the Audit Process." *Journal of Accountancy*, Vol. 196, Issue 3, 49-55.

Postmes, Tom and Spears, Russell (2001). "Quality of Decision Making and Group Norms." *Journal of Personality and Social Psychology*, Vol. 80, No. 6, 918-930.

Pavlo, Walt. (2007). "Lies, Fraud, and Felony." *Industrial Engineer*, August, 28-33.

Ramamoorti, Sridhar (2008). "The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula." *Issues in Accounting Education,* Vol. 23, No. 4, 521-533.

Sloan, Paul A., Berman, Mitchell E., Zeigler-Hill, Virgil, Bullock, Joshua S. (2009). "Group Influences on Self-Aggression: Conformity and Dissenter Effects." *Journal of Social and Clinical Psychology*, Vol. 28, No. 5, 535-553.

Troyer, Lisa and Youngreen, Reef (2009). "Conflict and Creativity in Groups." *Journal of Social Issues*, Vol. 65, No. 2, 409-427.