Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns

Gurpreet Dhillon
College of Business, University of Nevada, Las Vegas, Las Vegas, NV 89154-6009, USA, dhillon@nevada.edu.

A majority of computer security breaches occur because internal employees of an organization subvert existing controls. While exploring the issue of violation of safeguards by trusted personnel, with specific reference to Barings Bank and the activities of Nicholas Leeson, this paper provides an understanding of related information security concerns. In a final synthesis, guidelines are provided which organizations could use to prevent computer security breaches.

Introduction
Businesses today are experiencing a problem with managing information security. This is so not only because of increased reliance of individuals and businesses on information and communication technologies but also because the attempts to manage information security have been rather skewed towards implementing increasingly complex technological controls. The importance of technological controls should not be underplayed, but evidence suggests that the violation of safeguards by trusted personnel of an organization is emerging as a primary reason for information security concerns. Between 61 and 81% of computer related crimes are being carried out because of such violations (see Dhillon [5]; Dhillon and Backhouse [6] for a detailed discussion). These insiders could be dishonest or disgruntled employees who would copy, steal, or sabotage information, yet their actions may remain undetected.

Numerous security breaches have been reported in the popular press describing the sequence of events. In the UK for example, a fraud against the National Heritage Department resulted in payments of over £175,000 being made to fictitious organizations. In another case, a small US based Internet service provider, Digital Technologies Group, had its computers completely erased, allegedly by a disgruntled employee. The dismissed employee was later arrested and faced a prison sentence of up to 20 years.

Clearly violations of safeguards by trusted personnel resulting in information security breaches are real and need to be addressed. A requirement also exists for establishing guiding principles that organizations could adopt in moving a step forward to manage such information security problems. In addressing these concerns and needs, this paper reviews the nature of information security breaches occurring because of violation of safeguards by trusted personnel. The case of Barings...
Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns/Gurpreet Dhillon

Bank and the violation of safeguards by Nicholas Lesson, a trusted employee, are used to interpret the nature and scope of such security breaches. This is followed by a discussion that forms the basis for generating principles for effectively managing the violations of safeguards such that the security of computer-based systems within organizations is not compromised.

Violation of Safeguards at Barings Bank

This section reviews the violation of internal organizational controls by an employee to gain undue advantage. It stresses the importance of instituting informal controls if computer security situations are to be adequately managed. The security issues arising from the misuse affect information systems integrity, formal and informal control mechanisms, and organizational cohesion in terms of culture.

Background

Barings Brothers & Co. (BB&Co.), a 223-year-old institution specializing in traditional merchant banking, decided to expand into investment banking in 1984 as a result of deregulation in the British financial markets. BB&Co. established a brokerage firm under the name of Barings Far East Securities, but this was later changed to Barings Securities Limited (BSL). The new company adopted the corporate culture from its founder Christopher Heath, a man recruited from the brokerage firm Henderson, Crosthwaite & Co. Heath brought many like-minded people into the new Barings subsidiary and created a strong corporate culture. This culture was more profit seeking and money-oriented than the traditional merchant banking culture that had existed at BB&Co for centuries.

BB&Co collapsed in 1995 due to one individual's wrongdoing and many other individual's security negligence. Nicholas Leeson, the General Manager of Barings Futures Singapore Pte. Ltd. (BFS), a subsidiary of BB&Co. exploited substandard information security systems and caused the company to be placed under judicial management and eventually to go bankrupt.

Since Leeson had gained an immense amount of trust through his profits, £30 million for Barings in 1994 alone, he was able to circumvent many of the security inquiries against him without consequence. Leeson lost £126 million in Nikkei futures and Japanese Government bonds on 23 February 1995 after losing £701 million over the past two years. Given the lack of correctly enforced organizational and information security constraints at BB&Co., Leeson was able to hide his losses in a secret account created using Barings' accounting computer systems. This was account 88888.

The basic problem at BB&Co. that is of relevance to this paper, is the lack of correctly enforced organizational information security measures. Even though a functional security plan was in place at BB&Co., it did not take into account any interpretative data in its implementation, so leaving BB&Co vulnerable.

Corporate Restructuring Challenges

As BSL expanded and contributed increasing amounts to the revenues of the entire Barings Group, rivalry developed between BSL and BB&Co. Also, as internal competition between the companies accelerated, so did the incentive to take on more risk at BSL. The risk-taking management style and fast expansion of BSL left little time for implementing proper control mechanisms that would guard against financial impropriety. Barings Group directors became concerned and initiated a corporate restructuring.

The first thing that went wrong with the corporate restructuring was that the preferred corporate culture of fiscal conservatism could not be transferred from BB&Co. to BSL. Had the original conservative culture been instilled at BSL's development, perhaps through the transfer of existing managers from BB&Co. instead of recruiting risk-takers, there probably would have been less rivalry and less unwarranted risk-taking.

Problems could also have been controlled if it was not for the matrix structure. The structure per se was not wrong, but it was not implemented correctly, causing confusion and unclear reporting lines. Management's lack of understanding of its own
responsibilities allowed Leeson and others to go unsupervised locally, which could have prevented the unethical behaviour and its escalation. Adopting a hierarchical control system that limits decision-making could have prevented this. By standardizing jobs, implementing direct supervision, and making sure that checks and balances were in place, no employee would have been able to take covert actions that would have jeopardized the entire organization. The situation at Barings Group was a disaster waiting to happen. It defies probability that the entire collapse did not happen earlier. There are several factors that contribute to this assertion.

The most problematic cause of disaster lies in the roots of BSL itself. BB&Co. began their subsidiary by handing over total control to Christopher Heath. The bank even requested that the staff of the new subsidiary consist of employees of Heath’s current company, Henderson, Crosthwaite & Co., where he was a partner. It was from this moment that BB&Co. placed complete trust of BSL in the hands of an entity unfamiliar to Barings Group. BB&Co. had essentially relinquished control. Even though Heath was a positive influence in creating a company culture that fostered in ambition and individualism, he also created an environment lacking in formal control mechanisms. Another factor that foreshadowed the demise of Barings was the rivalry that developed between the two main firms in Barings Group: BB&Co. and BSL.

When Nicholas Leeson came to Barings Future Singapore (BFS), a subsidiary of BSL, as General Manager, he would soon be credited with bringing down the entire banking organization. He effectively kept his gross misconduct from being openly discovered because of two main reasons: (1) the autonomy of BFS from the central hierarchy and (2) the absurd lack of internal controls throughout the entire Barings Group.

**Evaluation Of Organizational Controls**

**Internal Controls**
The implementation of internal controls for any organization is key to running a ‘well-oiled’ business.

One of the first things accounting auditors learn in their studies is that examining the internal controls of an organization can tell a great deal about the company, how effectively it works, and how aware management is of their business processes. Management is responsible for maintaining the entity’s controls. Of course, the controls’ effectiveness depends on the competency and dependability of the people using it. Clearly, in this case the size, structure, and personnel were available to have effective controls, but Barings did not manage them, prioritize them, or take responsibility for maintaining them.

When management establishes its system of internal controls, there are several principals that are important to their plan. One fundamental principal is segregation of duties. It is important to segregate the areas of revenue generation, or custody of assets, and record keeping. This principal is extremely important because it prevents a single individual from committing misappropriation of company assets or revenue and then concealing the defalcation by altering the records. Some companies even separate controls even further in such a way that it would require two or even three individuals to commit this crime and conceal it on the books.

This internal control was not present at BFS. Leeson was responsible, as part of his position, for overseeing the trading and trade processing, settlement, and administration. He had access to the authorization and creation of trading accounts on the IT system; responsibility for generating income by trading a ‘book of business’, and also the ability to make journal entries that were posted to the system, apparently without review.

Another key problem was the lack of an effective internal auditing department. Problems or weaknesses with the design of the internal controls and discrepancies with the adherence to those internal controls are the primary responsibility of the internal auditing department. Internal auditing departments prioritize their activities based on a risk analysis. Areas that are potentially more vulnerable to the company are their responsibility. Obviously this
department failed to do its job if the activities of a small branch in Singapore were able to bring down the entire bank.

The key risk items that should have been looked at was, first of all, the lack of segregation of internal control at the branch level. Leeson was a General Manager who was responsible for both making trades and recording them. Second, a small branch in Singapore was showing abnormally large profits. Third, account balances were not reconciled. Daily reconciliation in the computer age is not unreasonable. Fourth, why were receivables in the Singapore Office so high? The internal audit department was either incompetent or lacking in sufficient organizational support to be effective.

There are five components of an ideal internal control mechanism that management should use to design and implement controls to give reasonable assurance that the control objectives are being met. These components are the control environment, risk assessment, control activities, information and communication, and monitoring.

First, the control environment consists of actions, policies, and procedures that reflect the overall attitudes of top management about control and its importance to the corporation. Clearly Barings Bank had some internal controls in place, but they were performed more as a checklist than for true discovery or prevention. Second, management should assess the risk in the design of its internal controls to minimize errors and fraud. Having the level of autonomy that BFS did from the Bank, the risk was much greater and should have caused increased sensitivity for strict adherence to a good internal control system. Third, control activities include other policies and procedures that help to ensure that necessary actions are taken to address risks in the achievement of the company’s objectives. Such control activities, adequate documents and records, physical control, and independent checks on performance are important components of internal control mechanisms. Barings' management knew Leeson had control of both the front and back offices of a division (BFS) they hardly knew anything about. It was discovered in later years that there was evidence of memoranda flying around about this blatant lack of separation of duties long before the collapse, yet nothing was done to change it. Fourth, information technology is used to gather company transactions and to maintain accountability to clearly communicate what is happening in the organization. At Barings Bank the management, internal auditors, and external auditors were all staring at the '88888' account problem, after all, it was a glaring piece of information, yet no-one attempted to reconcile this piece of reported information. It is true that Leeson hid things, forged documents, had information shredded by subordinates, restricted access to financial information, etc., but the fraud could still have been uncovered. Leeson simply had the confidence that even with all the controls in place and the inquiries into discrepancies that were found, he would still be able to beat the internal control system and recover the severe losses he was accumulating because the system was weak, flaky, and, therefore, easily circumvented. Fifth, monitoring the quality of controls periodically is essential to have effective controls. The internal audit department of Barings can best be described as pathetic. Clearly it seems that people at all levels of Barings’ control functions used varying degrees of the “hands-off” approach in performing their jobs.

External Controls

The external auditors also failed in their professional responsibility to detect material fraud at the Singapore office. Deloitte & Touche were the auditors through 1993, the time during which account 88888 was established. By then Leeson’s loss was £23 million; this clearly would have been material to BFS’ operations. Essentially, on the financial statement, Leeson was booking an entry to record the loss as income and as a receivable in order to conceal this loss. Deloitte & Touche failed in their audit of both the revenue of BFS and the assets of BFS. The unprofessional manner that they used to satisfy themselves that the receivable was correct was a major factor contributing to their demise.

After 1993, Coopers & Lybrand were the auditors for BFS. Coopers also failed in their confirmation of

Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns/Gurpreet Dhillon
the bogus Spear, Leeds & Kellogg (a New York trader) receivable. Leeson had earlier claimed it to be a computer error. However, when the auditors pursued the point further, he claimed that it was a receivable. Confirmations should be requested directly from the debtor by the creditor but returned directly to the auditor. Since Leeson produced the documents himself, it was not credible evidence for auditing purposes. Second, if they were to be relied upon, Coopers & Lybrand could have made a phone call to Leeson's point of contact to confirm the documents. The biggest question was why no-one noticed that BSL's Singapore branch had one individual responsible for both the front and back offices, and realized the possibility for fraud. Everybody involved with BSL knew the answer: they were enjoying the benefits accrued from the status quo and did not see a need to scrutinize the BFS' business processes.

Understanding the Issue

The discussion on Barings Bank and the violation of safeguards by Leeson, a trusted employee, constitutes a kind of an information system security breach that is intentional in nature. Generally, intentional acts could result in frauds, virus infections, and invasion of privacy and sabotage. Parker [11] uses the term ‘computer abuse’ to describes such acts as vandalism and malicious mischief and places them in the same category as white-collar crime. White-collar crime is defined by Parker as “any endeavour or practice involving the stifling of free enterprise or promoting of unfair competition; a breach of trust against an individual or an institution; a violation of occupational conduct or jeopardizing of consumers and clientele”. Information system security breaches resulting from the violation of safeguards by internal employees can therefore be defined as a deliberate misappropriation by which individuals intend to gain dishonest advantages through the use of the computer systems. Misappropriation itself may be opportunistic, pressured, or a single-minded calculated contrivance.

Computer crime committed by internal employees is essentially a rational act and could result from a combination of personal factors, work situations and available opportunities [2]. Hearnend [8] believes that most of the perpetrators are motivated by greed, financial and other personnel problems. Forester and Morrison [7] suggest that sometimes even love and sex could provide a powerful stimulus for carrying out computer crimes. A survey conducted by the UK Audit Commission in 1994 found, in addition to personal factors, disregard for basic internal controls (password not changed, computer activities not traceable etc.) and ineffective monitoring procedures contributed significantly to incidents of computer crime. An earlier study by Parker [13] found that in most organizations, sufficient methods of deterrence, detection, prevention and recovery did not exist. Clearly, the Barings Bank situation was a case in point.

In the previous section, a number of issues have been presented which could be considered as reasons why information system security breaches occur in the first place. However, there is considerable debate as to the extent to which information system security problems exist in reality. Parker [12] found that there was a wide range of opinions regarding the extent of computer security breaches due to the subversion of controls by internal employees. There were reports suggesting that only 374 cases were directly related to computer misuse, hence portraying computer crimes as being of minor significance. However, during the same period nearly 150,000 computers had been installed within US organizations. Clearly, the reported computer crime cases were an underestimation and what we actually see is just the tip of the iceberg. The UK Audit Commission’s study suggests that many individuals and organizations fail to recognize computer crime as a problem. Its survey found employees at the managerial and supervisory levels as falling short of understanding the risks that computer misuse presents. In fact two-thirds of the perpetrators were supervisors who had been in the organization for a minimum four years [1]. Another study based in the US found an astonishing 31% of computer crimes were being carried out by low paid clerks, 25% by managers and 24% by computer personnel [10]. Indeed Balsmeier and Kelly [3] suggest that most organizations had no method to minimize or deter computer crime and that the rewards for
unethical behaviour seem to outweigh the risks. This clearly suggests that Barings Bank, with all the flaws in its internal reporting and control structures, was a victim of an information system security breach that has been considered a significant threat for a while. Yet no learning was incorporated into Baring Bank’s thinking process.

From an auditing perspective, consideration could have been given to at least two aspects. First, the internal audit should have been reported to the audit committee, comprised of the board of directors of the company. Additionally, these members of the audit committee should have been independent board members, rather than board members who work for the company in the capacity of management or other professionals who provide service to the company. The independent, external auditors should also have reported to the audit committee. This is necessary to ensure that the auditors are reporting to a level high enough to ensure that recommendations and warnings do not fall on ‘deaf ears’. Internal and external audits are designed to help assure the board of directors and stockholders that the financial statements of management are materially correct and that management is acting responsibly to maximize shareholder value and safeguard their assets. If they were to report to anyone but the audit committee, that responsibility could be jeopardized by internal politics.

Second, an accountability and responsibility structure for internal auditors should have been created. Although internal auditors report directly to a committee of the board of directors, the internal audit department still needs to be accountable and responsible in order to use the resources that they are given in the most effective manner. The fact that internal auditors let a serious problem with the segregation of duties pass without ‘raising a major ruckus’ was negligent. External auditors also needed to be held accountable. In public accounting, a partner with over 20 years of experience would normally sell the engagements. The client then will not see the partner until the job is over. Unfortunately, most of the audit is performed by staff members, who are usually just one to three years out of college. In this case, the auditors from both firms made a serious mistake. They relied on the internal controls of BFS when the internal controls were defective in the first place. They did not perform any substantive procedures to ensure that this material weakness was not causing materially incorrect balances to certain accounts. The auditors then reported to the board of directors that everything was fine when in reality that could not have been further from the truth.

Discussion
Since most of the computer security breaches occur because internal employees have subverted the existing controls (see Dhillon [4]), it is important that emphasis is placed on the more pragmatic aspects of an organization. Considering the particular case of Leeson, an individual gets involved in particular acts as a consequence of a combination of a person’s behavioural and normative beliefs. If a person’s attitude to perform an illicit act needs to be influenced, one has to focus of changing the primary belief system. More than any specific communication instrument, an organization-wide feeling of working together to solve problems and not hide them is the key. This ties together the cultural and reporting standards so that Barings could have moved forward and its subsidiaries would not have hidden losses. Rather they should have worked together to solve problems. This, combined with proper auditing techniques, would have allowed Barings and its subsidiaries to avoid collapse. The paragraphs below identify some specific guidelines that organizations should consider if violations of safeguards by trusted personnel are to be avoided.

Formalized Rules
It has been argued that if an organization has a high level of dependence on IT, there is a greater likelihood of it being vulnerable to computer related misuse (e.g. see Moor [9]). It is therefore important that organizations implement effective and systematic policies. The demand for establishing security policies within organizations has long been made by academics and practitioners alike, however such calls have largely gone unheeded. Formalized rules in the
form of security policies will help in facilitating bureaucratic functions such that ambiguities and misunderstandings within organizations can be resolved. Lack of formal rules or an inability to enforce the rules was very well evidenced in the case of Barings Bank and Leeson’s activities. Most regulatory bodies (e.g. the Securities and Exchange Commission in the U.S) demand that certain procedures should be followed. There are even explicit rules regarding supervision. However because of an increased pressure to perform and be profitable, many of the formal rules were overlooked at Barings Bank. The case of Barings Bank suggests that although organizations cherish to instill a culture of efficiency and good practice, poor communication often has a negative impact. The case also suggests that formalized rules are essential for the functioning of an organization and often something more needs to be done. Perhaps there should be an adequate emphasis on informal or normative controls.

Normative Controls

Clearly, mere technical or formal control measures are inadequate to prevent computer security breaches. In other related work Dhillon [4] cites cases where it was relatively easy for insiders to gain access to information systems and camouflage fictitious and fraudulent transactions. In the U.S, one of the most publicized examples of this kind of behaviour is evidenced by the demise of the Kidder Peabody and the dealings of Joseph Jett. Jett was able to exploit a loophole in the accounting system to inflate the profits. It was possible to engage in criminal activities because the person involved was an insider. It therefore becomes obvious that no matter what the extent of formal and technical controls, prevention of insider security breaches demands certain normative controls. Such controls essentially deal with the culture, value and belief system of the individuals concerned (for details see Dhillon [4]).

Employee Behaviour

Previous research has shown that besides personal circumstances, work situations and opportunities available allow individuals to perform criminal acts (e.g. see [2]). In the case of Barings Bank the prevalent work situation and the opportunity to commit criminal acts affected the primary belief system of Leeson, thus creating an environment conducive to a crime being committed. This suggests that monitoring of employee behaviour is an essential step in maintaining the integrity of an organization. Such monitoring does not necessarily have to be formal and rule based. In fact, informal monitoring, such as interpreting behavioural changes and identifying personal and group conflicts, can help in establishing adequate checks and balances.

Conclusion

This paper has presented an analysis of violation of safeguards by trusted personnel by considering the case of Barings Bank and the activities of Nicholas Leeson. The analysis has suggested that organizations need to focus on the underlying beliefs that lead individuals to engage in intentional illicit acts resulting in computer security breaches. Clearly, behavioural change is ultimately the result of changes in beliefs. Thus it is important that people within organizations are exposed to information which will produce changes in their beliefs. In proactively managing the occurrence of adverse events, it is essential that we trace those changes in primary beliefs that result in particular attitudes and subjective norms.

Acknowledgments

Acknowledgments are due to Dr. James Backhouse, director of Computer Security Research Center at the London School of Economics for extensive discussions, comments and feedback on various aspects of information security management. The assistance and comments of number of graduate students at the University of Nevada, Las Vegas and London School of Economics, including Russell Cook, Roy Dajalos and Freddy Tan are also acknowledged.

References

Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns/Gurpreet Dhillon


