Computers & Security Vol.20, No.8, pp.715-723, 2001
Copyright © 2001 Elsevier Science Limited
Printed in Great Britain. All rights reserved
0167-4048/01$20.00

Computer crimes: theorizing about the enemy within

Gurpreet Dhillon and Steve Moores

College of Business, Box 456009, University of Nevada, Las Vegas, NV, 89154-6009, USA
Tel: (702) 895 3676; Fax: (702) 895 4370, Email: dhillon@unlv.edu

Abstract

A majority of computer crimes occur because a current employee of an organization has subverted existing controls. By considering two case studies, this paper analyzes computer crimes resulting because of violations of safeguards by employees. The paper suggests that various technical, procedural and normative controls should be put in place to prevent illegal and malicious acts from taking place. Ultimately a good balance between various kinds of controls would help in instituting a cost-effective means to make both accidental and intentional misconduct difficult. This would also ensure, wherever possible, individual accountability for all potentially sensitive negative actions.

Key words: Computer crime; malicious act; violation of safeguards; information security.

Introduction

Computer crime resulting from violation of safeguards by current employees can be defined as a deliberate misappropriation by which individuals intend to gain dishonest advantages through the use of the computer systems. Such violations constitute a significant proportion of computer crimes - as high as 81%[10]. Misappropriation itself may be opportunist, pressured, or a single-minded calculated contrivance. Computer crime committed by current employees is essentially a rational act and could result because of a combination of personal factors, work situations and available opportunities. These insiders may be dishonest or disgruntled employees who would copy, steal, or sabotage information, yet their actions may remain undetected. Such illegal and often malicious acts can have serious consequences for a business, yet many companies do not follow the proper procedures so as to prevent illegal activities from taking place. This includes having a system of controls in place to help prevent an employee's ability to perform illegal actions. It also involves promoting the values that a business feels are positive, and monitoring employee behaviour.

This paper, by considering the cases of Kidder Peabody and Daiwa Bank, presents an analysis of computer crimes and theorizes about establishing adequate controls. The paper argues that more often than not, computer crimes occur when a current employee of an organization subverts existing controls to take undue advantage from the situation. The paper is organized into six sections. Following a brief introduction, section two and three describe the computer crime situations at Kidder Peabody and Daiwa Bank. Section four presents a comparison of the two situations and section five draws lessons and principles for managing computer crimes. Finally section six draws broad conclusions.

The Kidder Peabody case

Consider the case of illicit activities of Joseph Jett who defrauded Kidder Peabody & Co out of millions of dollars over a course of more than two and half years. Jett was able to exploit the Kidder trading and accounting systems to fabricate profits of approximately US$339 million. Jett was eventually removed from the services of Kidder in April 1994. The US Securities and Exchange Commission claimed that Jett engaged in more than 1000 violations in creating millions of dollars in phony profits so as to earn millions in bonuses. During the course of Jett's involvement with Kidder, he amassed a personal fortune of around $5.5 million and earned himself upwards of $9 million in salary and bonuses. In 1993 alone, he made nearly 80% of the firm's entire annual profit of $439 million.

The opportunity

Prior to joining Kidder, Jett was aware of the manner in which the brokerage business was conducted and the specific conditions at Kidder. Jett realized the shortcomings of the accounting system and began tinkering with it. The management overlooked Jett's actions, especially because he seemed to be performing very well and was adding to the firms' profitability. Jett had been hired to perform arbitrage between Treasury bonds and Strips (Separate Trading of Registered Interest and Principal of Securities). Kidder relied heavily on Expert Systems to perform and value transactions in the bond markets. Based on the valuation of the transactions, Kidder systems automatically updated the firm's inventory and Profit and Loss statements. Jett found out that by entering forward transactions on the reconstituted Strips, he could indefinitely postpone the time when actual losses could be recognized in a Profit and Loss statement. Jett was able to do this by racking up larger positions and reconstituting the Strips. This resulted in Jett's 1992 trading profits touching a $32 million record, previously unheard of in dealing with Strips. Jett's personal bonus was $2 million. The following year Jett reported a $151 million profit and earned $12 million in bonus. It was only in March 1994 that senior management started looking into the dealings. This was because Jett's position included $47 billion worth of Strips and $42 billion worth of reconstituted Strips.

Clearly basic safeguards had not been instituted at Kidder. Although the junior traders at Kidder were aware of Jett's activities, the senior management did not make any effort to access this information. These factors certainly influenced Jett's beliefs and his intentions regarding the advantages and disadvantages of engaging in the illicit activities. As a consequence Jett manipulated the accounting information system and deceived the senior management at Kidder.

Prevalent norms

As is typical of many merchant banks, bonuses earned are intricately linked with the profitability of the concern. Kidder offered substantial bonuses for individual contribution to company profits. Even within the parent company, General Electric, CEO Jack Welch had told his employees that he wanted to create a 'cadre of professions' who could perform and be more marketable. This resulted in the employees being subjected to intense pressure to perform and having a focus on serving their self-interest. As a consequence, General Electric did not necessarily afford a culture of loyalty and truthfulness. The employees were inadvertently getting the silent message that they should 'look after themselves and win at any cost'. Critics claim that there was a certain hollowness of purpose beneath Welch's relentlessly demanding management style[6].

Reports of ethical violations had also marred some of General Electric's traditional lines of business. There had been allegations of conspiracy with De Beers mining company of South Africa to fix prices of industrial diamonds. The FBI has also been investigating charges that General Electric had repeatedly ignored warnings about electrical problems that could compromise the safety of aircraft engines. Jack Welch has dismissed these charges and has contended that had General Electric not acquired Kidder Peabody, such discussions would not have surfaced. Irrespective of the nature of defences put up by the General Electric senior management, the fact remains that a dominant culture to win and an aspiration to be number one or two in every market, created an internal context within the organization such that unethical practices could be overlooked.

External variables

Prior to Jett joining Kidder Peabody, no significant ethical problems had been reported at Kidder. Over the past few years the bank had been striving to perform satisfactorily, because at some stage the CEO wanted to dispose of the loss making brokerage unit. It had stayed clear of all sorts of rogue dealings, a phenomenon so common to any merchant bank. In fact lessons had been learnt from dealings in 'junk bonds' elsewhere. For example, the horror stories surrounding the demise of Drexel Burnham Lambert Inc. haunted every major bank involved in the derivatives market.

Kidder Peabody and the parent company General Electric were determined to court political and business acclaim by recruiting a large number of people from ethnic minorities. The bank considered this to be a means of paying back to the society and perhaps gaining esteem from others by lending a helping hand to certain under-privileged sections of the society. Various investigative reports following the Kidder Peabody swindling case have reported that the only reason why Jett got selected was because he happened to be a Black American. There are claims that Jett had falsified information on his vitae, thus making it extremely impressive. The personnel department at Kidder took this information on face value and did not make any attempt to verify it. It follows therefore that Jett's risk taking character and involvement in unethical deeds may have influenced his beliefs, ultimately leading to the demise of Kidder.

Daiwa Bank scandal case

In yet another case, illicit activities of Toshihide Iguchi, a bond trader for the New York office of Japan's Daiwa Bank, resulted in the bank loosing at least $1.1 billion. It is estimated that over a period of eleven years Iguchi made 30,000 unauthorized trades and allegedly fabricated profits at Daiwa, while in reality he was making substantial losses. The fact that Iguchi was able to get away without being caught for so long is astonishing. Iguchi seemingly never sought any monetary gains from his actions. All he was apparently trying to do was conceal his mistakes.

What went wrong

Iguchi's troubles began soon after he was promoted to be a trader in 1984. Daiwa's New York office was small, and in order to save money, Iguchi had also been put in charge of keeping the books. He was simultaneously in charge of making trades and then recording them. This meant that Iguchi himself controlled the input and processing of everything that he bought and sold, and what the bank owned. On becoming a trader, Iguchi misjudged the market, and lost an estimated $200,000 trading U.S. government bonds, an insignificant sum to a bank as large as Daiwa. However Iguchi did not feel he could admit to a mistake, even one relatively as harmless as this. And since he had total control over the input, processing and output of all data, Iguchi was able to conceal his actions without much difficulty. In covering up his actions, Iguchi doctored the data to make it appear that he was making enormous profits for the company. Unlike some of the actors in other high-profile banking scandals, Iguchi apparently never profited from his illegal actions.

What Iguchi did to cover his initial losses was to illegally take government bonds from Daiwa's own accounts or the accounts of Daiwa's customers and sell them. He would order Bankers Trust New York Corp. to sell the bonds, and, because of the way the system was set up, the statements came directly to Iguchi. He would then forge duplicate copies to make it look as if Bankers Trust still held the bonds that he had just sold. The money he made from these sales went only to recoup his losses, and the plan may have worked if it was used only once. Unfortunately for Iguchi, he kept making bad business decisions, and his losses began to mount. He began trading more and larger sums, up to $500 million in bonds in one day. As his losses grew, so did the cover-up. Over the next eleven years, Iguchi made an estimated 30,000 unauthorized trades while losing $1.1 billion[7].

By 1993, it was becoming more and more difficult for Iguchi to continue covering-up his losses. That year, Daiwa's New York office separated the bond-trading and record-keeping sections of its business. Iguchi no longer had direct and unsupervised control of both functions. Still, Iguchi was able to continue the fraud for another two years. This fact led to suspicions that someone else within the organization was helping Iguchi carry out his scheme. Whether he was working alone or with the help of someone else, Iguchi's unauthorized actions finally came to light in 1995 when he wrote a 30-page letter of confession to Daiwa's then president, Akira Fujita. In the letter Iguchi said that he could no longer withstand the pressure of his misdeeds.

The cover-up

During Iguchi's trial in a Manhattan courtroom, he was quoted as saying: "they asked me to continue concealing the losses". While admitting his role in the fraud, Iguchi also suggested involvement of other Daiwa officials in the scandal. Soon after Iguchi's admission in court, the Federal Reserve Bank revoked Daiwa's charter to do business in the United States. As the evidence mounted, the U.S. Attorney's Office charged Daiwa Bank with 24 counts of conspiracy and fraud. Several top executives were charged with crimes related to the scandal. The cover-up apparently had been going on for nearly ten years, and included lies to federal officials, forged documents, Cayman Island transfers, to name a few.

Even with evidence of such criminal activity by executives at Daiwa, Federal Reserve officials were most interested in the events that took place after July 21, 1995, when Iguchi mailed his confession to Fujita. It is alleged that on July 24, Iguchi mailed another letter to Fujita, this one: "...warning that (Iguchi's) $1.1 billion loss might be detected if headquarters did not replace Treasury bonds from a customer custodial account that Iguchi had secretly sold to cover his losses."[8] Iguchi also said in the letter that it would be impossible for officials in the U.S. to find out about the losses if the Treasuries could be bought back. Daiwa officials apparently even asked for Iguchi's help in devising ways to continue concealing his losses.

Daiwa then sent a team of its executives to New York to take control of the situation. They met with Iguchi and the then New York branch manager Masahiro Tsuda. The executives told Iguchi and Tsuda that Daiwa planned to release information of the losses in November of that year, and until then, the situation must remain secret. They also allegedly asked Iguchi to rewrite his confession, and specifically instructed him to exclude all other information, except the one pertaining to unauthorized trading. Iguchi was also asked to destroy the computer records of his communications.

External variables

Iguchi's ability to defraud Daiwa of $1.1 billion was largely due to the fact that he controlled both the sales and the recording of the transactions. More was involved, though, for Iguchi to get away with it. Japanese businesses tend to "trust" their employees more than American businesses do. Japanese firms expect their employees to be loyal and work for the good of the company. It is relatively unthinkable for a person to behave in a way that is detrimental to the company. Therefore, Japanese firms are traditionally "loose", with few direct controls on the employees.

This idea of employee loyalty only applies to the Japanese employees of a company. Japanese firms constantly monitor American employees. Even though Iguchi had become an American citizen by the time the scandal began, he was Japanese and he spoke Japanese, and his bosses gave him complete trust. Iguchi had almost complete autonomy, something an American employee could never attain.

Daiwa's lack of controls also played a huge role in giving Iguchi the room he needed to pull off his deception. Although Daiwa would perform internal audits at various times, but never contacted Bankers Trust, who held the bonds, to confirm the figures. If they had, it is likely that Iguchi's deeds would have been found out. Daiwa also did not enforce a policy requiring its employees to take vacations. Many businesses, especially banks, force their employees to take vacations because that makes it more difficult to manipulate the data. Iguchi apparently never left for more than a few days at a time. If Daiwa had insisted that its employees take time off for a week or two, it is probable that Iguchi's actions would have been discovered.

Jett vs. Iguchi

There are a few similarities between Jett's and Iguchi's actions. Both were able to subvert the controls at their respective businesses. And clearly their actions were illegal and unethical, which caused each of their companies to loose huge amounts of money. Jett's apparent motives were to increase Kidder's profits while making huge bonuses for himself. His attitude seemed to be that it didn't matter what he was doing was illegal or unethical as long as he was making money. He has been quoted several times as saying that he didn't do anything wrong, and that what he did was no different from what other traders do. The implication is that Jett believed that it was perfectly acceptable to perform illegal actions as long as 'everyone else is doing it'. Jett is an example of one of those employees who, no matter how hard a business tries to encourage fair and ethical behaviour, may never be converted.

Iguchi's attitudes were the exact opposite of Jett's, although the outcome was the same. Iguchi's beliefs and attitudes were shaped by the Japanese culture, where loyalty and hard work are held in high esteem. As stated before, Iguchi never personally profited from what he did. His actions were motivated by loyalty to his employer, as well as his desire to avoid embarrassment. Iguchi seemed to think that he could fix the problem, although it kept getting worse. He wanted his company to do well, and he felt that it was his obligation to Daiwa to correct his mistakes.

Even though the fundamental attitudes and beliefs of Jett and Iguchi were very different, the ultimate outcome was the same. One employee was motivated by greed, and wound up causing problems. The other employee was motivated by loyalty to his company, but also caused his company major problems. This shows that encouraging desirable beliefs and attitudes can have major benefits in influencing the behaviour of employees, but is not adequate to prevent disaster.

Although it is very important for a company to focus on the values, beliefs, and attitudes of its employees, this is not enough to ensure that computer related crimes will be prevented. No matter how hard a business tries to shape and enhance its employees' ideals, there are always bound to be a few who would resist. Hence it is essential that a firm have in place controls that will prevent the odd employee from performing illegal actions. However, just having controls does not mean that they will be effective. These controls also need to be used properly. Kidder Peabody had implemented controls that could have caught Jett's actions early if they had been used the way they were designed to be used. A report by former Securities & Exchange Commission enforcement chief Gary Lynch stated that the scandal at Kidder was the result of 'lax oversight' and 'poor judgments'.[11] The report also claims that Kidder had a: "cavalier disregard for normal operating procedures in pursuit of profits."[9] As long as Jett seemed to be making tremendous profits for Kidder, officials were happy to look the other way, and any scepticism about Jett's actions was dismissed.

At Daiwa, it was a lack of controls that allowed the scandal to take place. There was little direct oversight of Iguchi, and he was free to conduct business as he saw fit. Daiwa had put the 'fox' in charge of the 'hen house'. Daiwa neglected the most basic safeguards, and made a huge error in risk control by letting Iguchi record his own transactions.

In both cases, management put too much trust in its employees, and failed to supervise them closely enough. They just assumed that their employees wouldn't do anything wrong. Both Daiwa and Kidder officials did not follow the practices generally accepted in the finance industry for monitoring trading activities and for risk management. In both cases this proved disastrous. Key lessons from the two cases are discussed in the following section.

Drawing lessons for managing computer crime situations

The cases of Kidder Peabody and Daiwa Bank suggest that there are certain basic safeguards that organizations can put in place thereby minimizing chances of a computer crime taking place. Safeguards or controls that could be put in place can be classified into three categories – technical, formal or informal interventions[3]. However the success in implementing controls is achieved by establishing the right balance between various controls (c.f. Dhillon).[4] Technical interventions essentially deal with restricting access, which may be to the buildings and rooms or to computer systems and programs. Formal interventions deal with establishing rules and ensuring compliance to the laws and procedures. Usually formal interventions can be instituted by considering and establishing the requisite organizational structures and processes. It also entails identifying roles and responsibilities that go with formal organizational structures. Informal interventions relate to the educational and awareness programs that could be put in place within organizations.

Technical controls

Clearly, both in the case of Kidder Peabody and Daiwa Bank, there were opportunities to establish appropriate technical controls that could have prevented crimes from taking place in the first place. As described earlier, Kidder relied on advanced information technology systems to manage the various transactions. And Jett identified a means to postpone the actual time when a loss could appear on the Profit and Loss statement. Simply put, this is a systems and analysis design problem. When the systems were developed in the first instance, little attention was perhaps placed on instituting the controls. Baskerville[1] suggests this to be typical of most systems development activities where the introduction of controls is not even considered during the systems analysis and design stages of system development. As a consequence security of systems is an after thought at best. There were certainly other problems with Kidder Peabody in that there was over-reliance on one individual to post all transactions, an issue also identified by Dhillon[5] in reviewing the shortcoming in the case of Barings Bank. In the case of Daiwa bank, a similar situation existed. The computer-based systems used by Iguchi had virtually no established controls. As a result one individual could input and doctor the data. Obviously there was lack of supervision and separation of responsibilities.

As Dhillon[3] suggests implementation of technical controls is usually considered in a rather narrow and mechanistic manner. There is practically little or no emphasis on incorporating numerous technical control structures into the systems development processes. Merely establishing a password is not enough. What is really needed is an understanding of the organizational structures and business processes and identifying a range of checks and balances that could be established. These could then be incorporated into the systems development processes. Even today this remains a far-fetched idea. Dhillon[2] provides evidence, where in a British Hospital CRAMM, the risk management methodology, was used in a haphazard manner hence forgoing the potential benefits in instituting the controls.

Formal controls

Formal controls deal with establishing adequate business structures and processes so as to maintain high integrity data flow and the general conduct of the business. Establishing adequate processes also ensures compliance to regulatory bodies, organizational rules and policies. Therefore it goes without saying, good business processes and structures ensure the safe running of the business and preventing crime from taking place. Clearly mature organizations have well established and institutionalized processes and newer enterprises have to engage in the process of innovation and institutionalization. To a large extent high integrity processes are a consequence of adequate planning and policy implementation. In the realm of information security there is a general lack of appreciation for the importance of planning and policy issues. In cases where consideration has been given to security policy formulation and implementation, security and computer crime prevention has been treated largely as a technical issue with a predominance of technical controls. These are usually in the form of passwords, firewalls and encryption (for a detailed discussion see[4]).

Lack of consideration to formal controls is evidenced in the case of Daiwa Bank were no organizational structure or business process was defined for keeping books and recording trades. As a matter of fact, Iguchi was in charge of both making trades and keeping the books. Consequently there was a significant vulnerability because of lack of segregation of duties and separation of roles.

Many organizations are attempting to institute formal controls by either developing their own standards or adopting codes of conduct developed by independent bodies such as the BS7799. However simply adopting a code or a best practice does little in terms of compliance of individual ownership. Simply adopting a code, mission statement or a credo, without following it up with training and publicity to reinforce the message, will not be enough to prevent employee transgressions. In order for the campaign to be effective, upper management must be highly visible in the conduct of the campaign. Management must make employees at all levels really accept (in other words, internalize) the code of conduct they want the employees to follow.

Another formal control that companies need to consider is to establish procedures and practices to monitoring and preventing deviant behaviour. Since companies want to avoid deviant behaviour from their employees, it is in their best interests to reinforce positive beliefs and attitudes, while at the same time modifying undesirable ones. However, before a business can begin to reinforce these positive aspects in its employees, it must first determine what behaviour and actions that are considered desirable. The business can then consider what kinds of beliefs and attitudes will help achieve the specified behavioural outcomes. At the same time, it would also be useful to determine the range of undesirable behaviours. This will allow the company to take proactive steps to reduce or eliminate certain deviant beliefs and attitudes before they can lead to adverse consequences. Such an orientation would allow a company to develop adequate methods and procedures for promoting certain kinds of behaviour and for monitoring negative changes in employee attitude.

Monitoring employee behaviour is important for determining how well its workers are conforming to the desired 'code of conduct', and to deal with any deviations before they become serious. A company, however, should not be content with fixing problems as they occur. There should also be an emphasis to prevent any problems from occurring in the first place. To a large extent this can be accomplished by instilling a company's values and beliefs in its employees. Businesses and other organizations have a duty to themselves, and to their shareholders, to make absolutely certain that all of their employees fully understand the organization's goals and objectives. Achieving this should begin with the development and publicizing of such things as 'Mission Statements' and 'Company Credos'.

Informal controls

Informal controls, perhaps the most cost-effective type of controls, essentially centre around increasing awareness of employees, ongoing education and training programs, and management development programs focusing on developing a sub-culture that enables everyone to understand the intentions of various stakeholders.

In particular, informal controls could take the form of communicating appropriate behaviour and attitudes, making the employees believe in the organization and assuring individual accountability for any misconduct. Communicating appropriate behaviour and attitude is an important informal control that an organization can establish. Many companies conduct periodic (e.g., annual) briefings for their employees on such topics as sexual harassment, personal responsibility and employee excellence. Similarly there is a need to have seminars to communicate an organization's attitude on various subjects such as computer crime and white collar crime. Such briefings and classes demonstrate to their employees how they are supposed to act, and that there may be consequences for not following the given norms of behaviour. Certain companies have been proactive in conducting such training sessions, albeit following a fraud or some illegal activity. For example, some years ago, six employees of Rockwell International were accused of illegal actions regarding charging to government contracts. Even though the employees were at fault, Rockwell was still held accountable for its employees' actions. As part of the settlement of the case, Rockwell agreed to ensure that every single employee of the corporation attended an annual 'Ethics Training' sessions.

An important informal control that organizations should establish relates to making the employees believe in the company and assure individual accountability for any misconduct. The beliefs and attitudes conveyed by the company to its employees must also be consistent, and should be continuously communicated to the employees over a long period of time. Exposing the employees to the company's moral and ethical beliefs only sporadically is not enough. They will not internalize them, and are not likely to follow them. The same message should always be present, day in and day out, in the work environment. Management also needs to make certain that it does not allow its desire to succeed to take precedence over the company's own beliefs and attitudes regarding personal and business ethics.

Clearly ethical training and 'wheel alignment' campaigns can have the desired effect on the bulk of the employees of an organization. Most of the employees can be endowed with a strong enough set of beliefs and morals to act as effective controls over the way they conduct themselves within a company. It can be safe to assume that most employees will perform their duties according to the company credos, and will not try to subvert controls by engaging in illegal activities. However, there will always be a small percentage of employees who remain immune to the ethical training and to the attitudes surrounding them. These people present a real threat to the company. Even when a system of controls is in place, a company can be severely damaged, or even destroyed, due to the unethical or illegal actions of a single employee. It is therefore important to devise methods to identify such individuals and keep a tab on them.

Some employees might also evade normative controls because of cultural idiosyncrasies. Employees steeped in certain cultures might find it extremely difficult to admit mistakes, and could resort to unethical or illegal activities to try and hide such mistakes. Employees from other cultures might put faith in personal relationships at the expense of company procedures, and, for example, ignore competitive bidding requirements in the awarding of contracts. In any case personal accountability for misconduct needs to be ingrained into the organizational procedures. A policy statement on personal accountability and its communication to the relevant stakeholders will go a long way in addressing the need for informal controls.

Conclusion

Clearly there are a number of controls that could be established to prevent situations like those at Kidder and Daiwa from occurring. As has been stated in the previous sections, such controls are at three possible levels – technical, formal and informal. In particular setting standards for proper business conduct, monitoring employees to detect deviations from standards, implementing risk management procedures to reduce the opportunities for things to go wrong, implementing rigorous employee training, instituting individual accountability for misconduct are some of the immediate steps that businesses could take.

The key guiding principle for any control implementation has to relate to identifying the exact level of resource allocation. Certainly the amount spent should be in proportion to the criticality of the system, cost of the control and probability of the occurrence of an event. Appropriate controls are also necessary to protect organizations from suits against negligent duty and compliance to computer misuse and data protection legislation. Indeed for any control measure to be effective, both management and employees must take them seriously. Encouraging positive attitudes and beliefs and implementing safeguards may not prevent every breach of conduct, but it is well worth the effort.

References

[1] Baskerville, R., Designing information systems security, John Wiley & Sons, New York, 1988.

[2] Dhillon, G., Managing information system security, Macmillan, London, 1997.

[3] Dhillon, G., Managing and controlling computer misuse, Information Management & Computer Security, 7, 5, (1999).

[4] Dhillon, G., "Principles for managing information security in the new millennium," in Dhillon, G., ed., Information

security management: global challenges in the new millennium, Hershey: Idea Group, 2001, p. 173-177.

[5] Dhillon, G.,Violation of safeguards by trusted personnel and understanding related information security concerns, Computers & Security, 20, 2, (2001), 165-172.

[6] Greenwald, J., Jack in the box, Time, 1994.

[7] Greenwald, J., A blown billion, Time, 1995.

[8] Hirsch, M., Tossed out, Newsweek, 1995, p.42-46.

[9] Pare, T.P., Nightmare on Wall Street, Fortune, 1994, p.40-48.

[10] Parker, D., "Seventeen information security myths debunked," in Dittrich, K., Rautakivi, S., and Saari, J., ed., Computer Security and Information Integrity, Amsterdam: Elsevier Science Publishers, 1991, p.363-370.

[11] Smart, T., Wall Street's bitter lessons for GE, Business Week, 1994.