Acta Informatica Pragensia
3(3), 2014, 222–238, DOI: 10.18267/j.aip.43
Online: aip.vse.cz

Sekce / Section:
Recenzované stati / Peer-reviewed papers

When Sentry Goes Stealing: An Information Systems Security Case Study in Behavioural Context

Syed Irfan Nabi[1], Zaheeruddin Asif [1], Abdulrahman A. Mirza[2]

[1] Faculty of Computer Science, Institute of Business Administration
Main Campus, University Road, Karachi, Pakistan

[2] Information Systems Department, College of Computer and Information Sciences
King Saud University, 2099, Building 31, Riyadh 11543, Saudi Arabia

{snabi, zasif}@iba.edu.pk, amirza@ksu.edu.sa

Abstract: In this paper we describe a case where the top management of a small holding company is involved in a love-hate relationship with its own IT department. The top management firmly believes that IT staff is involved in leaking out company's secrets. However, having no expertise in IT and even lesser grasp on the complexity of IT architecture resulting from recent mergers and acquisition, the top management finds itself crucially dependent on its IT systems, yet unable to trust them fully. The theories of deterrence and reasoned action are used to explain the otherwise objectionable behaviour of the perpetrator.

Keywords: Insider Threat, Human Behaviour, Information Security, Information Systems, Theory of Deterrence.

1 Introduction

Technically the IT department of present-day organizations has access to almost all the information generated, transmitted, processed or stored in its computer-based systems administered by them. The access is required to perform their job, including but not limited to creating and maintaining user accounts, system and data backups, generating reports, etc. They cannot perform their job if they do not have access to systems and data. The smaller the IT department the greater is the degree of access to information and system. By virtue of this access they have to be a group of trusted people. This access does not translate into a license to start looking at the data or snooping on confidential information. The situation becomes critical if these people are suspected of breach of confidentiality and lose trust of the organization. Should the organization continue with these IT people or get rid of them? If replaced, is there any guarantee that the new hires would not follow suit? This dilemma is analyzed in this paper using case-study method with reference to a particular incident in an organization.

The rest of the paper is structured such that we start by presenting the theoretical foundations of behavioral aspects of information security breaches, followed by description of research methodology used for this study. Subsequently we discuss the case in detail. Analysis and discussion are then presented before concluding the paper.

2 Theoretical foundations

It has been established in literature that insiders are responsible for most of the information security breaches (Warkentin, Willison 2009). The breaches tend to be more severe if the perpetrator is disgruntled and has privileged access to information systems and data. Historically more emphasis has been on research on technical measures to check this sort of misuse/abuse (Dhillon, Backhouse 2001). Considering that the perpetrator is a human, recently more multidimensional studies have been conducted that are incorporating human behavioral aspects in information security issues as well (Angell 1994, 2001; Mahmood et al. 2010; Siponen, Oinas-Kukkonen 2007; Warkentin, Willison 2009). As such the theoretical foundations for such work have been borrowed from philosophy, psychology, sociology, and criminology,. The theories that have been used to explain human aspects include, but are not limited to, general and specific theories of deterrence, theory of planned behavior and theory of reasoned action (Bulgurcu et al. 2010; Stanfford, Warr 1993; Siponen 2000). Some of the relevant work is briefly discussed below.

2.1 Human behavior and information security in the light of reference theories

Siponen (2000) argued that the use of 'motivation/behavior theories' could offer new possibilities of "increasing users' commitment to security". He presented a novel persuasion strategy based on theory of planned behavior, technology acceptance model and intrinsic motivation that addressed the human behavior aspect of compliance to security policies. However, the same Theory of Planned Behavior has been used by Leonard et al. (2004) along with Theory of Reasoned Action, to find the factors that significantly influenced attitudes and behavioral intentions, which effectively reduce the misuse of IT resources. Theory of planned behavior was used by Bulgurcu et al. (2010) to show information security awareness (ISA) as a rationality-based factor that affect employees' attitudes and beliefs towards intention to comply with information security policies. Since ISA was found to be important, efforts to increase awareness have been studied by Khan et al. (2011) from the perspectives of psychological theories and models to find the effectiveness of various tools and techniques used

to create the awareness in an organization. Training and communications are part of ISA. Puhakainen and Siponen (2010) used universal constructive instructional theory and elaboration likelihood model to show that IS security policy compliance is enhanced through theory-based training and continuous communications.

2.2 Human behavior and information security policies

Boss et al. (2009) introduced the concept of 'mandatoriness' – the degree to which individuals perceive that compliance with existing security policies and procedures is compulsory. The perception of 'mandatoriness' was found to be very effective in motivating individuals to adhere to security guidelines. Similarly, theories of cognitive moral development and motivational types have been used by Myyry et al. (2009) to explain the behavior of employees towards adherence to information systems security policies and have empirically verified their theoretical model. They found that in real-life situations, pre-conventional reasoning (i.e. making decision based on pleasure or pain received/expected from external and physical events - Kohlberg's Level One of three levels of moral reasoning (Kohlberg 1984) cited by Myyry (2009) positively influences adherence to IS security policies. Straub (1990) looked in to the issue of investment in IS security versus its effectiveness in controlling computer abuse based on general theory of deterrence taken from criminology. His results indicated that computer abuse was reduced if 'deterrent administrative procedures' were used along with technical security measures.

The literature has tackled issue of insider threat by applying the general and special theory of deterrence. In this research we would like to make use of these two theories of deterrence as well as the theory of reasoned action to analyze the situation.

3 Research methodology

We have used the case study method of research. Some of the pertinent works on it are by Gomm et al. (2000); Stake (1995); Yin (2012). Considering the recommendations by Yin (2003) individual case-study is appropriate for this research. In this research we have analyzed the peculiar situation of IT staff breaching confidentiality; sentry stealing the silver. The names and other identifying details have been masked to ensure the confidentiality and privacy of the involved parties. The organization where this happened is referred in this paper as 'Company'.

3.1 Study questions

This case study is conducted to answer the following questions:

1. Why would a non-disgruntled employee behave unethically?
2. Why should a suspected perpetrator be allowed to continue operating??
3. Why do top managers need to strike a balance between operational effectiveness and the need to secure information?

3.2 Propositions

Theoretical foundations from literature review in combination with study questions have been used to formulate the following propositions:

1. Deterrence can only work with an employee who is not deemed critical.

2. Personal anguish of violation of privacy is a very strong force that can lead to misjudgment and can adversely affect rational judgment.
3. It is always a balancing act for any organization to decide on appropriate level of security, where business objectives can be used as the balance.

3.3 Unit of analysis

Event of confidentiality breach is the primary unit of analysis, while CEO, Senior Manager of IT and IT Manager are the secondary units of analysis. The company was a conglomerate of six business units. The head office and manufacturing facility were located in a big metropolis in a developing country. The regional and field offices were located in six other major cities. A business unit was located overseas as well.

All pertinent information about the incident, IT infrastructure, information systems, and access policies, were gathered through personal interviews and company records to find relevant data for analysis.

4 The case

The study was undertaken when Company approached us to solve their dilemma of not being able to point out the perpetrator of a serious security breach. Initially it was thought that it would be a quick and simple technical solution to find the perpetrator by making use of system logs combined with a sting operation. When IT department was suspected of involvement, it became clear that we could either opt for an all-out investigative action or use a subtle and disguised approach. As more information about the Company and its IT/IS were disclosed it became clear that the Company's operations were significantly dependent on IT/IS. Any disruption in IT/IS would virtually bring the operations to a standstill. Company was therefore advised to use the latter approach.

4.1 Exposition

Company had been consolidating its business enterprise developed through complimentary mergers and acquisition of different business units from a variety of companies over a period of six years. These business units originally belonged to American and European multinational companies and had brought with them their peculiar work ethics, organizational cultures, and information systems. The dynamic top management of Company worked diligently for smooth transitions to form a conglomerate enterprise. It not only improved its efficiency nationally but also extended its operations overseas. Centralized IS combined with a stringent IT control by very proficient staff had helped tremendously during the mergers in streamlining the subsequent combined operations. The data flow diagram connecting various systems with the financial system part of Company records is given in Figure 1. During this time, new systems and technologies were also introduced to cater for emerging business needs of the enterprise. Figure 2 illustrates the new IT infrastructure of the Company called Network-1. The project plans with business needs and time lines for Network -1 and Network Security are given in Figure 3 and Figure 4 respectively.

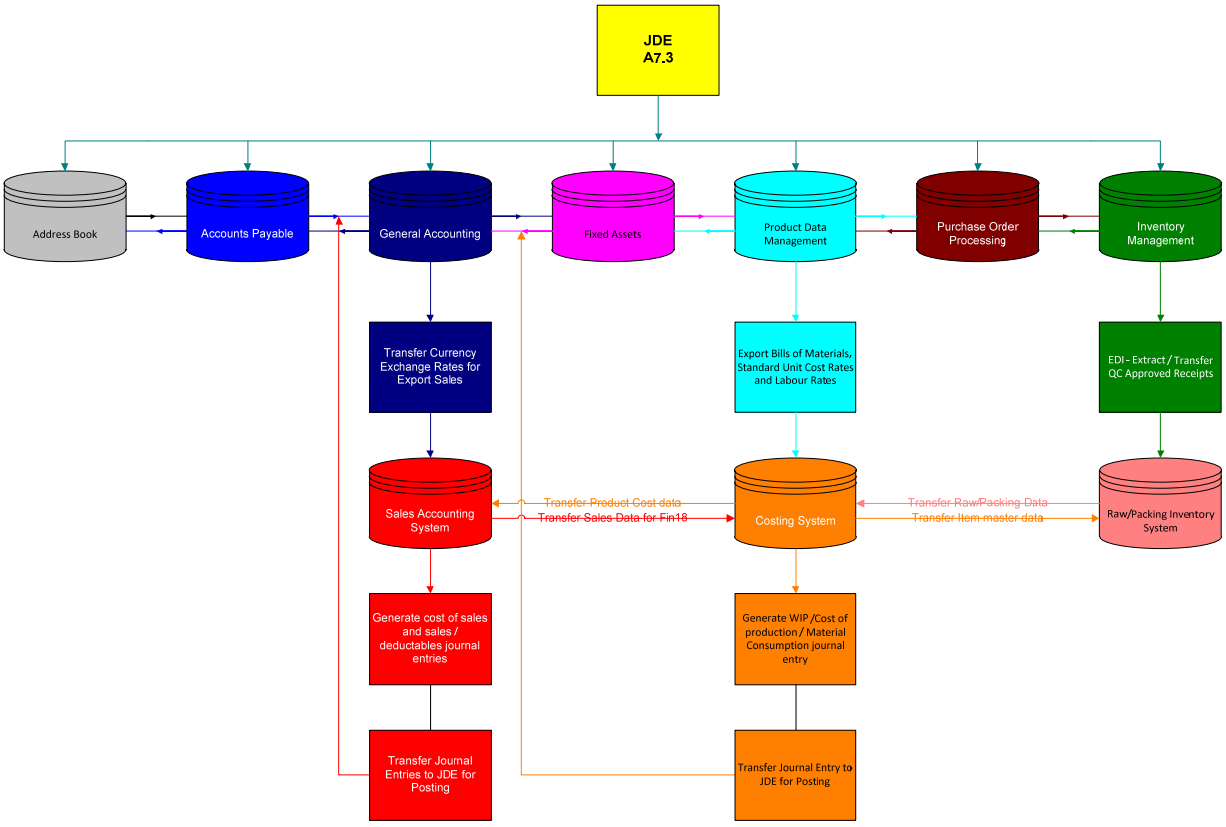

Figure 1: The Data flow diagram showing the data connections between various systems at the Company. Source: Company records.

The journey for IS/IT was not easy. The hurdles were overcome with determination and hard work by IT department coupled with strong support of top management. The consolidation had its share of organizational challenges. There had been some grouping within the employees based on their acquaintanceships prior to mergers and acquisitions. The allegiance to old-time familiarity and companionship was subdued but could not be removed completely. The divide, although muffled, had widened due to layoffs and reduction in manpower during consolidation. During the course of integration, for some business reason Company decided to lay off certain people in Business Development and Human Resource Departments and hire an executive in Finance Department. Before the information could be announced officially to the employees the news was leaked.

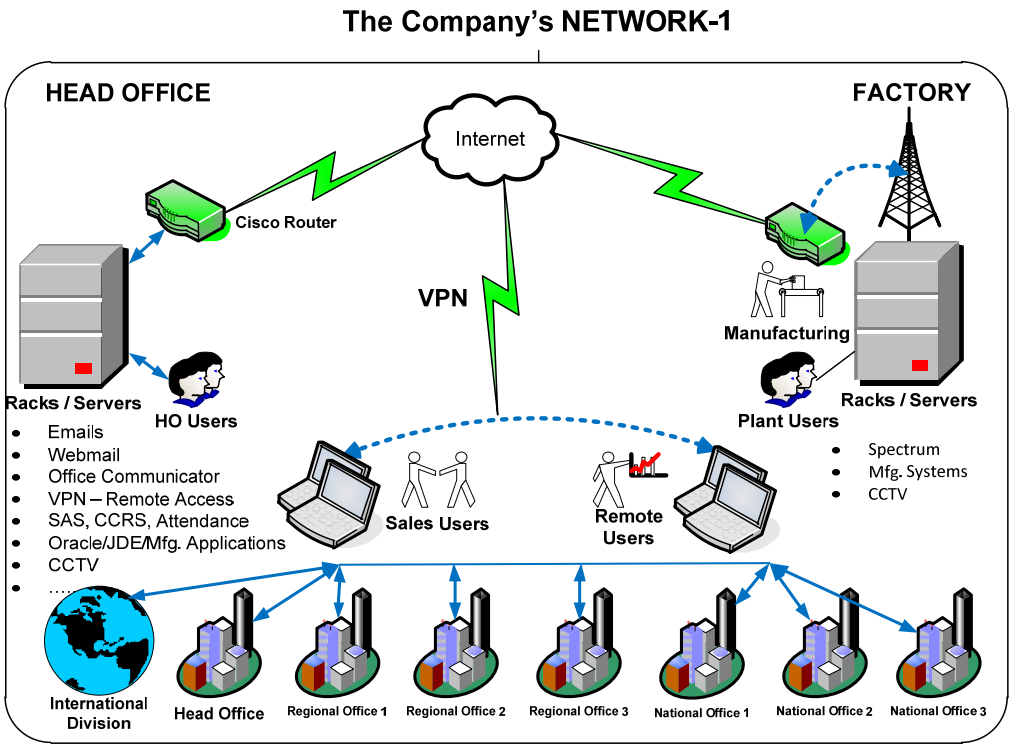

Figure 2: The Company the Information Network – Network -1. Source: Company records.

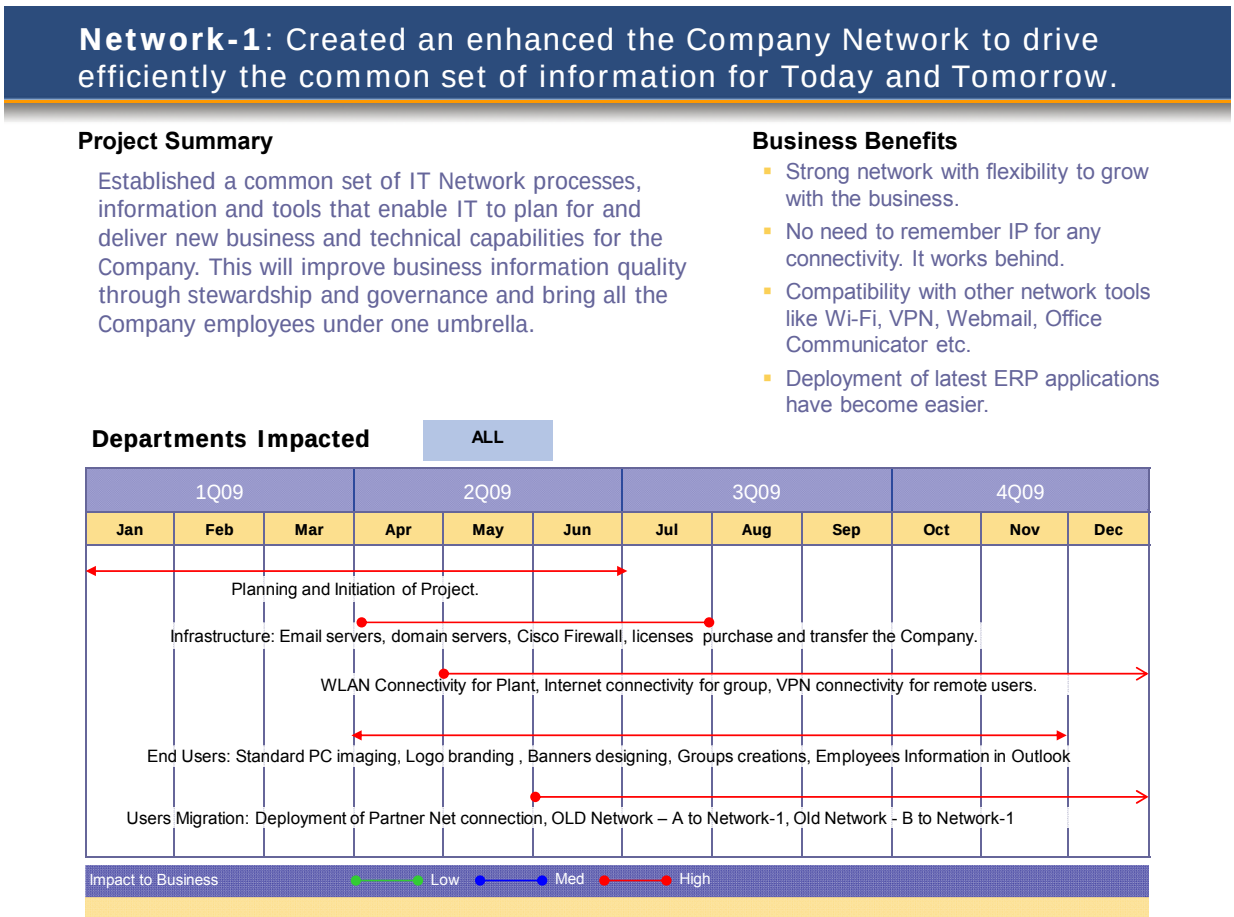

Figure 3: The Network -1; project summary, business needs and time line. Source: Company records.

4.2 Dilemma

With the spread of this news anger and frustration increased in the Company. Those to be laid off were angry while those not to be promoted were frustrated. This created certain resentment in the Company. Top executives were also frustrated that the hiring and firing could not be done smoothly and that some umbrage had been created among the company employees. They were also furious on the breach of confidentiality of the otherwise classified information discussed in personal communications between CEO and Senior Director – the top two positions in the Company.

A quick meeting of top executives was called to discuss and analyze the situation. It was decided to promptly have a veiled investigation to find the person responsible for the breach. This preliminary investigation revealed that it was an internal job pointing strongly to IT department as possible suspect.

Without exact knowledge or evidence against the perpetrator other than strong suspicion, frustration arose. Due to privacy violation it peaked to such an extent that CEO was willing to fire the whole IT department. It was obviously a vengeful thought that needed to be restrained. It was critical to curb the impulse. Not that it had many people - it had only 4 employees - but because it was very efficiently controlling the whole set of diverse information systems. They were also providing centralized IT support. Their performance had been exceptional, except for this incident. The business operations of the Company spread locally, nationally as well as globally, were centrally controlled from its head office that also housed the IT department. Complexity of the situation was that the smooth continuation of IT department was vital to the operations of the company. Any hint of doubt or distrust from top management, even if subtle, could potentially jeopardize the whole business continuity.

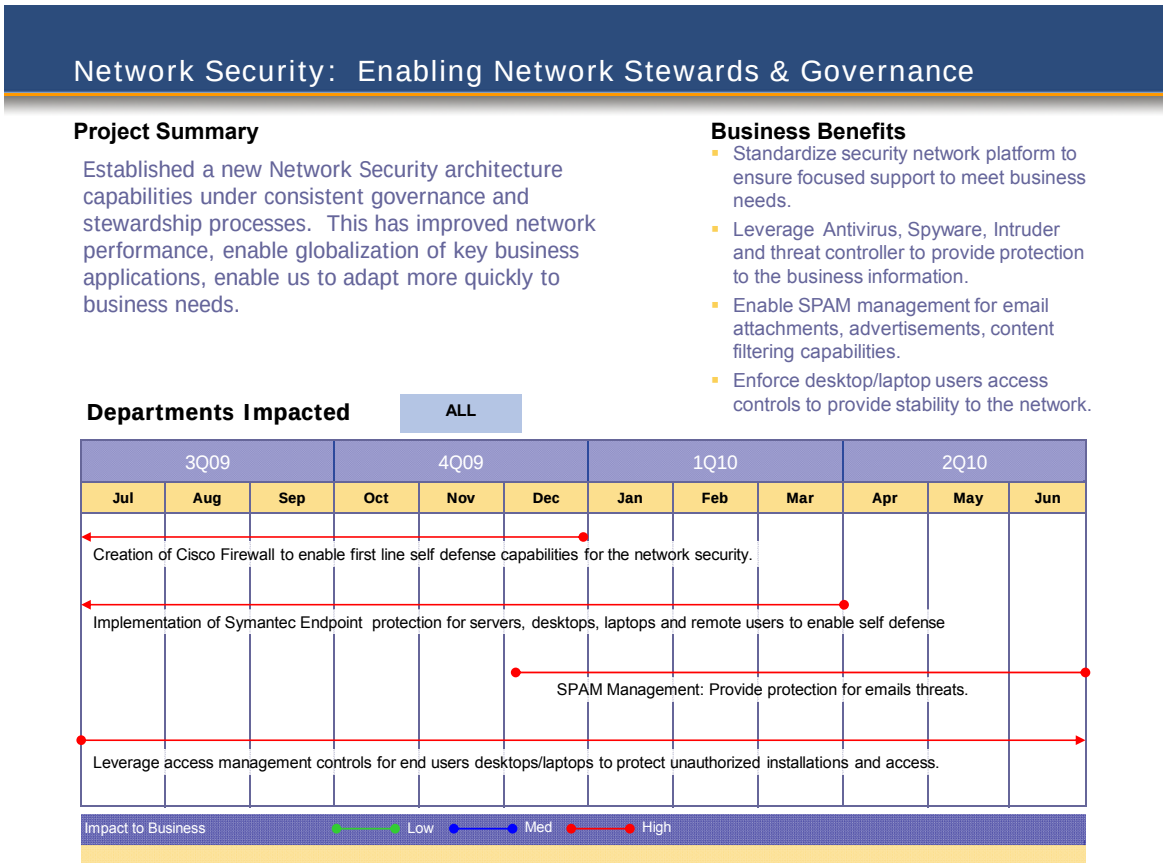

Figure 4: The information Systems and Network Security; project summary, business needs and time line. Source: Company records.

4.3 Systems integration study

The emotions of top management were difficult to pacify, thus it was decided to get professional help as soon as possible. The obsessive determination by CEO was; "Find me who is getting into my emails?" Since IT Department itself was a suspect an appropriate cover had to be devised. As information security professionals we were contacted for the purpose. Quick preliminary analysis of situation led us to conclude that it was a complicated situation and taking on the IT personnel directly might jeopardize the operations of the company. After some preliminary off-site meetings it was decided to launch a clandestine hunt for the culprit under the garb of a research study. Since the company cherished successful integration of its various legacy systems that came with mergers and acquisitions, it was decided to conduct an official research study of the 'successful systems integration'. The IT Department was proud of its accomplishment and we thought that they would be very pleased and ready to talk to us at length about it. This could serve multiple purposes: first, we could get to know the intricate details of the existing systems that would allow us to better ascertain the necessity of retaining current IT personnel for continuity of operations; second, willingness to talk about one's accomplishments could help us build a rapport with them; third, spending time and talking at length with them we thought that we might be able to pick up clues as to who was the culprit or was the department as a whole involved in it.

Accordingly after preparing a legitimate cover, the 'study' began. Three site visits were planned for the study. The CEO, head of Finance Department and IT staff were interviewed.

On the first visit the CEO briefed everyone on the issue and the objectives of the 'project'. Later on head of Finance Department also joined the meeting. The Finance Department, to whom IT personnel reported, was asked to extend full cooperation in this regard. Subsequently, Senior Manager IT and Manager IT were asked to brief the visitors on the IT infrastructure, systems and workings.

We returned a week later for another meeting with IT personnel. This time detailed discussion was held with Senior Manager IT about the legacy systems, their importance and role in current operations, as well as issues and challenges of integrating and maintaining them. Further, the current systems and future expansions were also discussed. Subsequently another follow-up meeting was held. This time detailed discussions on current IT infrastructure, computer network and development of Network 1, computer, network and information security system projects and future plans were done with Manager IT.

4.4 The Company's IT environment

After the visits and detailed discussions we found that:

1. The Company had a very tightly regulated and controlled IT environment. It was standardized and being managed very professionally. It was more closely matched to international IT best practices than those found in a typical local business setup. Figure 3 gives the details.
2. The company had a unified IT network that supported LAN and WiFi as well as remote access. Cisco firewall and ISA server were used to secure the network and user access along with Symantec Endpoint antivirus software. Microsoft Exchange server was used to handle all emails. The details can be seen in Figure 4.
3. The core financial systems ran on Oracle, while J D Edwards provided operations support systems. These were legacy systems and some sort of interfacing had been done but there was no real integration. Oracle based systems were looked after by IT Manager who had been working with these systems before these were acquired by the Company. He had known these systems very well. While the JD Edwards systems were RPG-II based and still ran on IBM AS400, which came with the systems during acquisition from another parent company. The Company also hired an IT person from the parent company as Senior Manager IT who was very well acquainted with these systems. There were some other support systems as well. This can be seen in Figure 1.
4. Various business support systems and services were being run at the company. The ownership of these rested with concerned business units/functions that provided business process trouble-shooting support to the end users, while the IT provided technical support.

4.5 Limitations

The major limitation of this study was the requirement to maintain complete secrecy. Only a few top executives knew the real intent of the 'study'. For the rest of the organization it was only an academic research into successful systems integration. Working under disguise made it practically impossible to ask any specific questions related to the actual incident except to the top management with whom the case could not be discussed inside the company premises. Any information that has security relevance is always a sensitive issue for any organization and such information is not readily shared with 'outsiders'. Although we had the blessings of CEO, yet we did not anticipate any overwhelming response to any direct security related queries. It may

be noted that CEO had given us an option to remove our cover and move into an interrogative stance any time we felt it necessary. The offer was declined because we were not professional interrogators and were concerned more about the business continuity than in catching the culprit. It is important to note that according to our analysis of the current situation, catching the culprit was not significant to the future of the company, yet the significance of the information leakage could not be overlooked. It is very important to stop any leakage of information even if it is deemed non-critical because if ignored (or accepted), subsequent confidentiality breaches might leak sensitive or critical information leading to potential loss of business continuity. Also, it can lead to an organizational culture where information security is ignored and misuse of access rights to organizational data is considered ethically appropriate i.e. a socially accepter norm. This can have a very negative impact on the organization as a whole and the organization may eventually fail.

5 Analysis and Discussion

5.1 Situation Analysis

The IT network and infrastructure were very tightly controlled thus it was not easy to break into them. Since IT personnel were suspected, it was not possible to use any tool to monitor and catch them without their knowing about it. Once they knew it, they could easily circumvent it. Technically speaking, server administrator is defined as a person who has access to all the files on the server to do his job. Therefore, restricting his access makes no sense. Similarly, mail server administrator has access to all the users' emails and does not need to break or hack into any email account. The audit can be turned on for the MS Exchange (email) server which can log all the activities done on the server including accessing users' emails. But this service can only be turned on with administrative access rights on the server. The MS Exchange (mail server) administrator surely can stop this service, as well as erase the log, if and when he wants to.

As mentioned earlier, at that time of the study all the systems and services at the Company head office seemed to be professionally managed based on international best-practices. Thus IT staff appeared to be competent. The IT staff was specialized in their own particular area. However, it did not look like that there was much cross-training within the IT department on the legacy systems. This was fine since the systems were old but it did increase the Company's dependence on IT personnel. On the other hand, there was no strict segregation of duties, therefore access to network, servers, and systems seemed to be shared. The legacy systems required existing experienced IT staff to operate and maintain them.

Further, it is known that disgruntled employees are the single most common cause of information security breach amounting to more than 70% of such incidents (Shey 2012). But we were puzzled. Never during our extensive interaction did the IT personnel come across as disgruntled employees; not even a hint. Thus, it could not be the case of disgruntled employee causing the information security breach. One of the things that we did come across was subtle undercurrent of uneasiness among employees on the continuity of their jobs. Because of mergers and acquisitions, once the operations were integrated some people were laid off. Therefore, this breach seemed more like the action of a under confident employee who was not sure of his long term employment and trying to find out what is going on regarding layoffs in the organization. We concluded that the culprit did not intend to do any harm to the organization per se, rather was trying to avoid any personal surprises. We further concluded that taking any extreme measures right away might not be very conducive to operations of the Company.

5.1.1 Suspect

Apparently it seemed that the breach of privacy might have happened at the IT department, either individually or in collusion. This conclusion was reached on the basis that IT systems had very good technical security in place and IT staff was very competent, whereas the top management was minimally familiar with IT systems to the extent that they could not even change their personal email password. They were completely dependent on IT staff.

After detailed interaction with IT personnel it seemed like a case of an individual act. Although we are neither experts of behaviour/speech analysis nor any such analysis was done, yet through the common sense examination of behaviour of IT personnel we gathered a few rudimentary clues that pointed to the probable perpetrator. One of the odd occurrences in this regards was that during one of our visit we were told that one of the IT personnel has called-in sick that morning. It was decided that we shall meet the available IT staff. But just after the lunch this IT person on 'sick leave' for the day showed up and joined our meeting once he came to know that we were at the Company meeting IT personnel. We thought that this was odd because if one is sick and has taken the day off then one is not expected in the office.

5.1.2 Proof

No substantiated proof existed to implicate any person. The logs were kept under the tight control of the IT management and were not shared. Putting in sniffers or other intelligence gathering hardware or software was not a practical option under the scenario.

5.1.3 Assessment and Recommendations

Based on the analysis it was concluded that:

1. Top executives were in need to develop their IT skills.
2. There was no pure technical solution to produce evidence against IT administrators in the given situation at the Company.
3. The Company had specialized old systems (complex legacy systems) which were meeting their needs but required dedicated, experienced staff to operate them especially as modifications incorporated in them were known only to the selected few concerned staff involved with that particular system. There was no redundancy. Therefore no member of the IT staff could be reprimanded/punished even if found guilty because then he could decide to resign altogether leaving the system without an administrator.
4. In order to reprimand/punish IT staff, if so desired, a subtle action was needed. This would ensure operations did not totally collapse or even get severely hampered in case a current IT staff member was taken to task. It would obviate any cause of apprehension among the concerned employees.
5. Positive identification of the culprit could place the top management ill at ease, unable to assuage their anger. In order to ensure continuity of operations they might have had to continue working with the person that they did not want to keep.
6. The confidentiality of email operations could be ensured in future. It would be more effective and a worthwhile undertaking for the organization rather than punishing past culprits.

The two major sets of actions identified to help the Company were:

Administrative Actions:

A. Securing future email communications

It was recommended that separate email services be acquired for the top management immediately. Subsequently, an IT security policy could be adopted for IT systems that required segregation of duties among IT administration roles. In particular mail server administration (creating, deleting and maintaining user accounts) needed to be segregated from Backup role. It was further suggested that the audit be turned on the Exchange Server with audit log on a highly restricted separate server with no access rights to the IT staff. Access to the log server be placed strictly under direct supervision of the CEO. It was also suggested that the Company email services be outsourced altogether.

B. Removing dependence on IT personnel

To remove dependency on existing IT personnel it was recommended that the legacy systems be replaced with new, and preferably with a single, integrated, enterprise system. The IT department had recommended that earlier but the idea was dropped by the top management due to financial reasons. It was suggested that this option could once again be looked into.

Behavioral Change Actions:

Information security awareness (ISA) is an important aspect of creating an organizational culture conducive to information security. The organization should plan and implement information security awareness through a series of interventions. Internal seminars, morning meetings, small-group meetings, and even one-to-one personal meetings aimed at importance of information security can be highly effective in creating ISA (Khan et al. 2011). It can be reinforced with expected ethical behavior of the custodians of organizational data and that of IT personnel.

In this regard, the top executives needed this awareness much more than the other employees. They needed to know the importance of information security both for their personal as well as professional effectiveness and to develop IT skills that are a must for the executives of a high-tech organization they were becoming. Without becoming proficient in safe computing e.g. creating and managing strong passwords, it would not be possible to reduce information security breaches.

Further, the importance of communication cannot be stressed more. It is very important to keep the employees informed, especially of the bad news. This will enhance the confidence of the employees in the top management. Layoffs were an issue in the organization and lack of communication about it created an undue fear of uncertainty among the employees. Coming out openly and honestly about the issue would improve the morale of the employees.

5.2 Discussion

The question of a non-disgruntled employee behaving unethically can be answered if we analyze the situation of the two senior people in the IT department. Both the Senior Manager and the Manager were critical assets of the company, had successfully completed challenging

assignments in the past, were paid well and faced no imminent threat of a lay-off. Yet, as mentioned above, there were layoffs and this potentially affected the job security/continuity of all employees. Let's look at the theory of deterrence, based on the severity and surety of punishment (Stanfford, Warr 1993), and see if it can explain the situation. The deterrence theory holds that more the severe, the certain, and the swift a punishment is the more it will deter potential offenders. The general theory of deterrence is to discourage the unacceptable behavior by the people at large by making an example of the offender while the specific theory of deterrence is for behavioral correction of the concerned offender (Stanfford & Warr 1993). Since in this case the IT personnel knew their worth and significance to the company as well as the improbability of being punished even if 'caught', they were not deterred. Hence the proposition that deterrence can only work with an employee who is not deemed indispensable stands.

While this proposition only informs that theory of deterrence in not applicable in the given situation, the theory of planned behavior (Ajzen 1991) provides explanation of the actions of perpetrator. In small privately owned organizations top management generally wants to hold and exert complete control over the organization. Generally it is their investment that they want to safeguard. This creates a power differential between them and the rest of the employees. It leads to the development of us versus them mentality and consequently leaking information becomes a norm. In this case the 'us' versus 'them' mentality augmented by subtle fear of layoff may have made finding and leaking such information socially accepted and it became a 'social norm'. Everyone would like to be informed of any such detrimental decision by 'them' sooner than later so as to get as much time as possible to plan a response against 'their' decision. Thus, it seems like a plausible explanation of the action of accessing 'their' confidential information about layoffs and leaking the same to the employees.

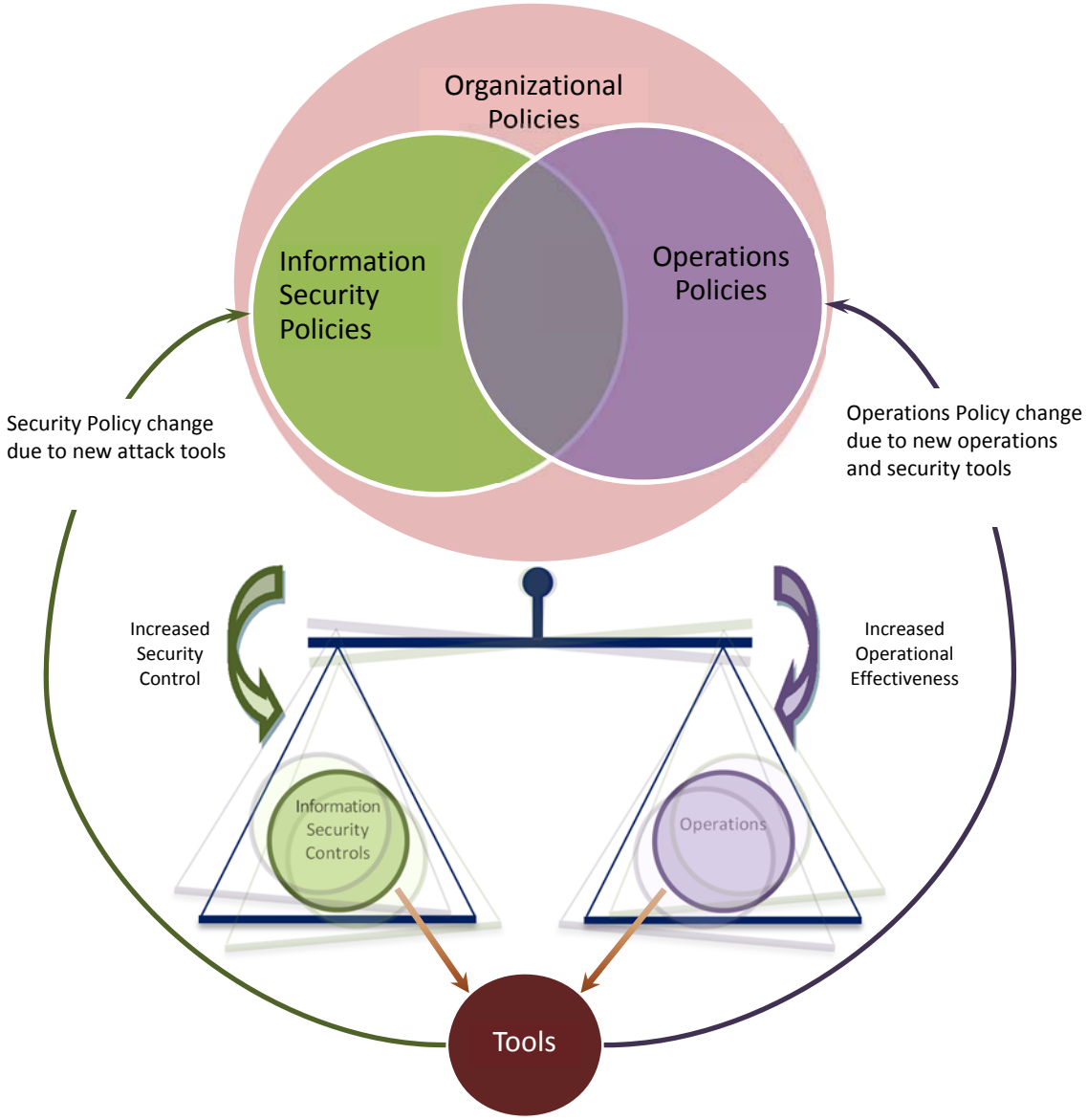

Figure 5: Relationship between information security and operations. Source Authors.

The next question was about the CEO's dilemma of allowing the suspected perpetrator to continue operating. This can be a very stressful and challenging situation for a manager. The necessity of allowing a suspect to continue working for successful continuation of a business, which in turn ensures retention of the employees, availability of the service/product to the end-users and financial returns to the stockholders carry more weight than ego satisfaction of a single person or a small group of people (CEO and Senior Director in this case). The initial reaction in such incidents is to catch the criminal but this urge has to be suppressed to give way to a more rational action of continuation of the business operations. In this case, even if the identity of the perpetrator could be positively established with corroborating evidence, it would have created a more anxious psychological situation for the CEO than resolving the issue. That is because the CEO could not fire the person due to the detrimental dependence of the business on IT personnel. Not only that, but the CEO would also be forced to work with this person fully aware that he has been unethical. Despite the fact that the CEO showed restraint in carrying out his irrational decision, he could never get this thought out of his mind. Thus, the proposition

that personal anguish felt over violation of privacy is a strong force that can lead to misjudgment and can adversely affect rational judgment holds true.

The last question was about balancing the need for operational effectiveness with the need to secure the information. The tightly controlled IT environment was very helpful in promoting business strategy of IT enabled services that provide the Company with competitive advantage along with minimal IT overhead and simpler IT support. However, this resulted in heavy dependence on an otherwise very small IT department. There is a compromise between security and operations and it is a business decision in the end as illustrated in Figure 5. The proposition holds true that it is always a balancing act for any organization to decide on appropriate level of security, where business objectives can be used as to balance the power of IT versus top management.

This leads us to the importance of role and scope of IT department in an organization. Each organization needs to define and plan the scope of its IT department and role it is going to play in business. These have to be well-thought and deliberate strategic choices. These would then be translated into organizational policies to balance the top management control versus IT department access as well as between information security and business operations.

6 Conclusion

From the analysis and discussion the answers to the questions posed in the beginning can be concluded. The answer to the first question is that a non-disgruntled employee may engage in security breech if they know their power, and the indispensability of their positions. The answer to second question is that a suspected perpetrator should be allowed to go free to allow for business continuity. Especially in such unique circumstances where top management has not realized in time the importance and power of IT staff. Finally for the last question the answer is yes, balance is always needed.

This research has looked into the breach of information security and conclude that an apparently satisfied employee can also cause a breach and leak information if looking for and leaking a particular type of information has become a 'socially accepted norm' in the organization. In this case it was the information about layoffs. As discussed in the recommendation section, coming out openly and honestly about bad news and/or policies emanating from them is very important. Frequent and truthful communications can play a big role in reducing the uncertainty and enhancing the effectiveness of an organization and its employees through mutual trust, while lack of it can be detrimental, as seen in this case-study. The implication is that top management is responsible for setting the stage for 'socially accepted norms' it must strive to get the 'right' norms socially accepted.

On the other hand, lack of detailed planning about the role and scope of the IT department may result in unanticipated skewed power equations between the IT and top management, especially among small and medium sized organizations. These new equations can drastically change the organizational parameters needed for creating a strong IT security policy of an organization. Under these conditions it is critical to assess the situation in a holistic manner from a strategic point of view with due care being given to operational efficiency in addition to IT security. The case demonstrated the need to maintain a balance between top management and IT personnel as well as the business continuity concerns and IT security technical needs. It is pertinent to note that parameters of IT security policy need to take into account IT security assumptions which are context dependent.

Overall, a theoretical conclusion that can be drawn from this case study is that IT security policies are sensitive to the organizational circumstances and in smaller organizations the power equation between IT and top management makes trust an important factor in IT security policy.

In future we intend to research how certain information security behaviours get socially accepted as 'norms' and how can it be used effectively to increase the overall information security in an organization by getting the 'right' required behaviours socially accepted.

7 References

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes,* 50(2), 179–211

Angell, I. (1994). The impact of globalization on today's business, and why Information System Security is strategic. In *Annual Congress of the European Security Forum*, Cologne, Germany.

Angell, I. (2001). *The New Barbarian Manifesto: How to Survive the Information Age?*. UK: Kogan page.

Boss, S., Kirsch, L., Angermeier, I., Shingler, R., Boss, R. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems,* 18(2), 151–164.

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Quality and Fairness of an Information Security Policy As Antecedents of Employees' Security Engagement in the Workplace: An Empirical Investigation. In *43rd Hawaii International Conference on System Sciences* (HICSS) (pp. 1–7).

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), 70–104.

Dhillon, G., Backhouse, J. 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal,* 11(2), 127–154.

Eloff, J., Labuschagne, L., Badenhorst, K. (1993). A comparative framework for risk analysis methods. *Computers & Security,* 12(6), 597–603.

Garg, A., Curtis, J., Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security.* 11(2), 74–83.

Gomm, R., Hammersley, M., Foster, P. (Eds.). (2000). *Case study method: Key texts, key issues.* Thousand Oaks: SAGE Publications.

Halliday, S., Badenhorst, K., Solms, R. von. (1996). A business approach to effective information technology risk analysis and management. *Information Management & Computer Security,* 4(1), 19-31.

Householder, A., Houle, K., Dougherty, C. (2002). Computer attack trends challenge internet security. *Computer*, 35(4), 5-7.

Khan, B., Alghathbar, K., Nabi, S., Khan, M. (2011). Effectiveness of Information Security Awareness Methods based on Psychological Theories. *African Journal of Business Management,* 5(26), 10862-10868.

Kohlberg, L. (1984). *The psychology of moral development: the nature and validity of moral stages.* New York: Harper & Row.

Leonard, L., Cronan, T., Kreie, J. (2004). What influences IT ethical behavior intentions: planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management,* 42(1), 143–158.

Mahmood, M., Siponen, M., Straub, D., Rao, H., Raghu, T. 2010. Moving toward black hat research in information systems security: an editorial introduction to the special issue. *MIS Quarterly,* 34(3), 431–433.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems,* 18(2), 126–139.

Puhakainen, P., Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly,* 34(4), 757–778.

Shey, H. (2012). *Understand the State of Data Security and Privacy: 2012 To 2013.* Cambridge: Forrester Research.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security,* 8(1), 31–41.

Siponen, M., Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database*, 38(1), 60–80.

Stake, R. E. (1995). *The art of case study research.* Thousand Oaks: SAGE Publications.

Stanfford, M., & Warr, M. 1993. "A Reconceptualization of General and Specific Deterrence," *Journal of Research in Crime and Delinquency* (30:2), pp. 123–135.

Warkentin, M., Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems,* 18(2), 101–105.

Wharton, F. (1992). Risk management: Basic concepts and general principles. In J. Ansell & F. Wharton (eds), *Risk: Analysis, Assessment and Management*. New York: John Wiley & Sons.

Yin, R. K. (2003). *Applications of Case Study Research (applied Social Research Methods)*. Thousand Oaks: Sage Publications.

Yin, R. K. (2013). *Case Study Research: Design and Methods*. Thousand Oaks: SAGE Publications.