MANAGING TECHNOLOGY RISKS IN BANKS IN THE CONTEXT OF BASEL II

By
Sujit Christy

A successful hack on a bank's IT system might bring the bank to a halt for a certain amount of time - this is risk No.1; but it might also have a "reputational" impact which is risk No.2; if the reputational impact, coupled with the business disruption affects the share price - there is a third risk. How does one separate these out and measure them?

The Basel II Accord, with its requirements for operational risk management, has become a significant agenda in the banking industry in Sri Lanka. Banks are the second largest users of technology outside the telecommunications industry. Technology is used to share and or store information. Hence, information and the supporting processes, systems and networks are important business assets which facilitate the bank's operations. Therefore, the information used for operating a bank is entirely IT generated and controlled; reliability of that information is crucial for service delivery and survival. Confidentiality, integrity and availability of information are essential to maintain competitive edge, cashflow, profitability, legal compliance and commercial image.

Increasingly, banks and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means that banks are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increase the difficulty of achieving 'access' control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organizations may also be needed.

Like in Y2K, banks are presented with a calendar goal as a target for adherence. Unlike Y2K, however, compliance is mandatory if institutions are to continue trading. The Y2K was a surge of IT activity oriented just around ensuring information system availability whereas Technology Risk includes Availability, Integrity and Confidentiality.

The Basel II Capital Accord is an amended regulatory framework that has been developed by the Bank of International Settlements that requires all internationally active banks, at every tier within the banking economy, to adopt similar or consistent risk-management practices for tracking and

publicly reporting exposure to operational, credit and market risks. Basel II provides a unique opportunity for banks organizations to build an enterprise in which business systems are truly connected, available and secure; it can be a catalyst for banks to review their information management, integrate that information more effectively with management processes and to build in the control and reporting capabilities that the Accord intrinsically encourages. Banks that take this view will be meeting the Basel II challenge while gaining a clear competitive advantage across the business.

The Accord is designed to prevent banks from going bankrupt after taking bad risks or facing a hostile cyber environment. Among the prompts for updates to the original 1988 Accord was Nick Leeson's role in the collapse of Barings Bank in 1995. Leeson secretly accumulated hundreds of millions of pounds in losses from risky futures and options trades; these losses ultimately ruined the bank.

Basel II sets forth regulations requiring banks to examine and address internal and external risks - specifically operational, credit and market risks. It further requires banks to have a minimum amount of capital to cover these risks that could give rise to financial commitments. This requires a rigorous step-by-step approach. As such, banks need to plan, implement and maintain a comprehensive program of risk prevention, detection, analysis and management.
There's no doubt that implementing the procedures and processes necessary to comply with Basel II will cost banks money. But those financial institutions that take too narrow a view of the provisions of the new Accord are missing the point: the accord will bring about fundamental and positive changes to how banks use their information and operate overall, and how adaptable they are to change. Those institutions that can best reap the direct and indirect rewards of Basel II will do so by aligning risk and compliance with every aspect of their business; their distribution channels, IT systems, front and back office processes, supply chain management, and customer strategies. The collection and storage of data is one of three areas where a financial institution needs to ensure its systems are enhanced and ready for Basel II. Applying the appropriate technology should deliver the required outcomes not only in these three broad areas of compliance, but across the emerging range of business opportunities.

Managing risk has become a complicated business for banks and their IT departments with the implementation of Basel II, the international accord which maps out how the banking industry shall regulate itself for the next generation. The inclusion of operational risk in the digital age has changed from a onedimensional procedure to a highly complex analytical process. This shift in thinking will require multi-level risk assessments and sophisticated analysis of security, operational and management factors. The accord is going to change how institutions capture operational metrics data in the first place. Some heavyweight institutions are going to be looking to their IT Directors, Chief Information Officers and Chief Security Officer to play a big role in making it all happen.

Background to Basel II

The original 1988 Basel Committee (Basel I) ruled that banks should have enough cover for potential losses from transactions (technically, a bank's total capital should never fall to a level of less than 8% of risk-weighted assets) and set out rules for calculating the risk-weighted figure. In a world of interconnected financial systems, it's been recognized that a single risk measure for all

banks is no longer appropriate.

The current Basel Committee (Basel II) has developed a new system that will be more risk-sensitive and flexible – and more onerous. Banks will now be expected to examine technology, security, fraud, employment practices and workplace safety, business services, physical damage, business disruption, system failure, service execution-delivery-process management, and legal and reputational factors. Boundaries between types of risk aren't yet clear. Different departments will need to fully understand how risks flow through the organization – what the dependencies and correlations are. Banks should be effective at assessing external and internal factors impacting on their operations to gain an
understanding of risk.

An extension of this issue is that Basel II encourages an integrated risk management approach; risk information will need to be reported both as an aggregate measure and across different business lines. Agreed parameters will give a true picture of the performance.

Just as the banking community has had the foresight to develop its recommendations, so have the IT departments realized that they will have to speak in many different management languages to draw up their plans for Basel II. They will need to show strong leadership in the days to come and need support and encouragement from their respective boards to do so.

Operations risk

During the early part of the 1990s, the focus was on techniques for measuring and managing market risk. As time passed, this shifted to techniques of measuring and managing credit risk. By the end of the decade, firms and regulators were increasingly focusing on risks "other than market and credit risk." These came to be collectively called operational risks. This catch-all category of risks was understood to include,

- employee errors,
- systems failures,
- fire, floods or other losses to physical assets,
- fraud or other criminal activity.

Firms had always managed these risks. The new goal was to do so in a more systematic manner. The approach would parallel - and be integrated with - those that were proving effective with market risk and credit risk.

Operational risk is still a relatively new area of risk management with the requirements for effectively capturing, measuring and managing data still not formalized by the regulators. Due to the required improvements to the gathering and controlling of their operational risk, it is fast becoming one of the key challenges that banks face.

While various regulators have their own unique twists on operational risk, the Bank of International Settlements, through its Basel II Accords, is the most widely accepted. In the Accords, operational risk is defined as “The risk of losses resulting from inadequate or failed internal processes, people, and systems or from external events”. However, the committee indicates that this definition excludes systemic risk, legal risk and reputational risk.

While this definition appears straightforward enough, it is a veritable can of worms. First of all, most of the terms in the definition need definitions themselves. What is a loss? While the concept seems simple - the amount of money it costs you if there is an operational failure, may not cover all resulting costs.

Is it the cost to replace a failed disk drive, the cost associated with a failed trade that resulted from the failed drive, or the cost to replace the entire application because the hardware is no longer current and should be replaced? Should accruing losses be considered from the time the drive failed, or from the time the failure was detected, or the from the time the resulting losses became evident?

Basically, the above definition states that banks lose money because of operational failures. That is not too surprising; every enterprise in every industry does. However, what concerns the regulators is the size of the losses. The Basel II definition of operational risk focuses on predicting the amount of future losses due to operational failure and not how to prevent them. To be compliant, you need only estimate the likelihood and size of future operational losses and set aside capital to cover a portion of that risk, not reduce your risk exposure.

To make operational risk management truly useful, we need a definition of operational risk that, while completely consistent with Basel II, can help us lower operational risk exposure, not simply measure it. It turns out, that is not that hard to do. The fundamental operational objective is “Operating within a targeted level of operational risk and in full compliance with regulatory and corporate guidelines, maximize operational performance while simultaneously minimizing cost”

In other words, operating with an acceptable level of expected losses due to operational failure, produces the highest quality at the lowest cost. While this may not seem an earth shattering finding, we have actually established the crucial link between quality, cost and risk. It may be possible to keep cutting costs and maintain quality in the short run, but once you have reached operational efficiency, in the long-run, cost cutting will lead to higher costs due to operational failures.

Although we have established the important connection between quality, cost, and risk, we still need to come up with a definition of operational risk that is preventative and not simply diagnostic. To do this, we need to transform the definition of operational risk from the risk of financial losses, to one based on the risk that one or more components of operation will fail to meet their quality and cost targets. Hence, the definition “Operational risk is the risk that the Operation will fail to meet one or more operational performance targets”

The task appears daunting. Financial institutions and regulators had to dedicate considerable resources to managing market risk and credit risk; those were wellknown, narrowly-defined risks. Operational risk was anything but well defined. People disagreed about the specific contingencies that should be considered operational risks - should legal risks, tax risks, management

incompetence or reputational risks be included? The debate was more than academic. It would shape the scope of initiatives to manage operational risk.

Another problem was that operational contingencies don't always fall into neat categories. Losses can result from a complex confluence of events, which makes it difficult to predict or model contingencies. In 1996, the Crédit Lyonnais trading floor was destroyed by fire. This might be categorized as a loss due to fire. It might also be categorized as a loss due to fraud - investigators suspect employees deliberately set the fire in order to destroy evidence of fraud.

The Basel Committee outlined basic practices in a (February 2003) paper titled "Sound Practices for the Management and Supervision of Operational Risk". That paper, together with efforts by researchers and risk managers at major banks, has helped to shape emerging risk management practices for operational risk.

Most operational risks are best managed within the departments in which they arise. Information technology professionals are best suited for addressing systemsrelated risks. Back office staff are best suited to address settlement risks, etc. However, overall planning, coordination, and monitoring should be provided by a centralized operational risk management department. This should closely coordinate with market risk and credit risk management departments within an overall enterprise risk management framework.

Contingencies broadly fall into two categories:

- those that occur frequently and entail modest losses;
- those that occur infrequently but may entail substantial losses.

Accordingly, operational risk management should combine both qualitative and quantitative techniques for assessing risks. For example, settlement errors in a trading operation's back office happen with sufficient regularity that they can be modelled statistically. Other contingencies affect financial institutions infrequently and are of a non-uniform nature, which makes modelling difficult. Examples include acts of terrorism, natural disasters and trader fraud.

Qualitative techniques include

- loss event reports,
- management oversight,
- employee questionnaires,
- exit interviews,
- management self assessment, and
- internal audit.

Quantitative techniques have been developed primarily for the purpose of assigning capital charges for banks' operational risks. Much work in this field was performed by regulators developing the Basel II accord on bank capital adequacy. Early results were reported in a (January 2001) consultative document, which was included in a package of documents outlining the proposed Basel II accord. Extensive industry feedback on that document led the committee to issue a follow-up (September 2001) working paper on operational risk. A subsequent (April 2003) consultative document made further modifications to Basel II. The
final Basel II accord was released in 2004.

Basel II allows large banks to base operational risk capital requirements on their own internal models. This has spawned considerable independent research into methods for measuring operational risk. Techniques have been borrowed from fields such as actuarial science and engineering reliability analysis. Contingencies of an infrequent but potentially catastrophic nature can, to some extent, be modeled using techniques developed for property & casualty insurance.

Contingencies that arise more frequently are more amendable to statistical analysis. Statistical modeling requires data. For operational contingencies, two forms of data are useful:

- data on historical loss events, and
- data on risk indicators.

Loss events run the gamut - settlement errors, systems failures, petty fraud, customer lawsuits, etc. Losses may be direct (as in the case of theft) or indirect (as in the case of damage to the institution's reputation). There are three ways in which data on loss events can be categorized:

- event
- cause
- consequence

For example, an event might be a mis-entered transaction. The cause might be inadequate training, a systems problem or employee fatigue. Consequences might include a market loss, fees paid to a counterparty, a lawsuit or damage to the firm's reputation. Any event may have multiple causes or consequences. Tracking all three dimensions of loss events facilitates the construction of event matrices, identifying the frequency with which certain causes are associated with specific events and consequences. Even with no further analysis, such matrices can identify for management areas for improvement in procedures, training, staffing, etc.

Categories of Loss Events

The Basel Committee breaks down loss events into seven general categories:

1. Internal Fraud is defined as the loss due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity / discrimination

events, which involves at least one internal party. This can be categorized into unauthorized activity, theft and fraud. The IT aspects will include:

- Deliberate manipulation of programs
- Unauthorized usage of modification functions
- Deliberate manipulation of system instructions
- Deliberate manipulation of hardware
- Deliberate changing of system and application data through hacking
- Using/copying unlicensed or unauthorized software
- Internal circumvention of access privileges

Case 1: **Barings Bank** (February 1995): Barings Plc lost GBP 827 MM because a Singapore-based trader, Nick Leeson, took unauthorized futures and options positions linked to the Nikkei 225 and Japanese government bonds (JGBs).

At the height of his activities, Leeson controlled 49% of open interest in the Nikkei 225 March 95 contract. Despite having to finance margin calls as the bank lost money, the Barings' board and management claim to have been unaware of Leeson's activities.

Case 2: **Daiwa Bank** (September 1995): One of Daiwa Bank's US-based bond traders, Toshihide Iguchi, concealed USD 1100MM in bond losses over a ten year period. When management learned of the losses, they attempted to hide them from US regulators. Ultimately, Daiwa was forced to cease its US operations and was fined USD340MM in a plea agreement with US prosecutors.

Leeson and Iguchi controlled the internal process and there was no segregation of duties.

2. External Fraud is defined as the losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party. This can be categorized into theft, fraud and system security. The IT aspects include:

- Deliberate manipulation of programs
- Unauthorized usage of modification functions
- Deliberate manipulation of system instructions
- Deliberate manipulation of hardware
- Deliberate changing of system and application data through hacking

Case 3: In a case reported 2003 to the Victoria Police Computer Crime Investigation Squad, the client of a financial institution reported that more than $13,000 was missing from their accounts. The client contacted the bank who then conducted an internal investigation. The investigation identified that the client's account had been accessed via Internet banking and that funds had been transferred to various overseas accounts. A number of IP addresses relevant to the transfers were captured and logged, as was other relevant information. A trace of the source IP addresses revealed that the suspect transactions had been made from public Internet cafés. Enquiries at the cafés proved fruitless. As is the case with the majority of Internet cafés, records relating to the identity of users of their service are rarely kept, or at best are extremely poor and unable to be substantiated. Examination of the client's computer system identified a commonly available trojan program capable of capturing the user's key strokes and therefore the username and password the client typed to access the on-line banking facility.

Case 4: Richard Glenn Dopps pleaded guilty to one felony count of "obtaining information from a protected computer." Until February 2001, Dopps was employed by The Bergman Companies (TBC), a contracting firm based in Chino. After leaving TBC to go work for a competitor, Dopps used his Internet connection to gain access to TBC's computer systems on more than 20 occasions. Once Dopps was inside the TBC systems, he read email messages of TBC executives to stay informed of TBC's ongoing business and to obtain a commercial advantage for his new employer. Dopps' unauthorized access into TBC's computer system caused approximately $21,636 in damages and costs to TBC.

Case 5: According to the case record of Sept 26th, 1996, Kevin David Mitnick "obtained unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and educational institutions; stealing, copying, and misappropriating proprietary computer software from "Motorola, Fujitsu, Nokia, Sun, Novell, and NEC." After being incarcerated, awaiting full trial for 4 years, Kevin served 10 additional months and was released on conditional probation; He may not use a computer, cellular phone, or any other Internet device until 2003, nor profit from his crimes in any way.

Case 6: An Australian based hacker chose to advertise his presence, but only after he had covertly observed the victim for a nine month period. In January 2001, a victim in the United States advised USA law enforcement that a hacker had gained access to his computer via his high-speed cable modem.

The victim had installed anti-virus software in late 1999 but had not updated it since that time. The victim alleged the intruder was able to type messages to him on his screen, describe what he was wearing via his web cam and access, delete and modify files on his computer. Forensic analysis of the victim's computer revealed the presence of the SubSeven trojan. The trojan was placed on the victim's system in May 2000. A personal firewall was installed on the victim's system in October 2000, but the intruder retained access to the victim's computer despite its presence. The Trojan was configured to notify the attacker on an IRC chat channel when the victim was online and with which IP address. Certain information regarding the source of the intrusion was found through analysis of the victim's computer, including information programmed into the trojan by the attacker. This did not conclusively indicate the source of the attack, but provided avenues of inquiry for investigators. Inquiries with Internet service providers in the United States and subsequently in Australia identified the probable attacker. When interviewed, the offender

admitted to his actions and was cautioned but not
charged by police.

3. Employment Practices and Workplace Safety is defined as losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events. This can be categorized as Suitability, Disclosure & Fiduciary and Improper Business or Market Practices. The IT aspects include:

- Using/copying unlicensed or unauthorized software
- Internal circumvention of access privileges

Case 7: An Australian organization's publicly accessible payroll system was broken into by exploiting a known operating system level vulnerability. The company had not enabled logging at the network, database or operating system levels providing investigators with virtually no forensic trail. Poor security controls and a poor security culture made it easy for the perpetrator to hide his presence. Investigations showed that both the payroll system and
its administrator's desktop computer were similarly compromised. This suggests the payroll system was the target of a deliberate, rather than random, attack. It also suggests that the attack was most likely perpetrated by an employee, someone who would have knowledge of the system and who could benefit from modifying the data within it. However, without adequate logging it was difficult to mount a thorough investigation, let alone prove a case. As with any root compromise of a mission critical system, recovery was painful and protracted.

Case 8: In January 2003, a former employee of a company used the user name and password he held while employed at the company to remotely log into the company's network and accessed the accounts data containing customers' credit card transactions. The offender then changed customers' credit card details and proceeded to make refunds to his credit card through altered accounts. The company only became aware of an anomaly when it noticed an unusual number of refunds were occurring. Queensland Police charged the offender under Section 408C fraud under Criminal Code (Qld) 1899. Because the company failed to disable the employee's system account, the attacker could not be charged for computer offences as a case could not be made to show that the access was unauthorized access to a 'restricted' computer. The case highlights the importance of adopting appropriate practices and procedures to ensure that employees or contractors' access to an organization's network and premises is withdrawn once their employment has terminated.

Case 9: An employee of a telecommunications service in Sydney was dismissed on November 2001. On 16 and 17 January 2002 the employee logged onto a website which he formally administered, which allowed corporate customers to procure hardware. Although his access had been cancelled on termination, it was later discovered that the employee had misused his privileges during his term of employment to create additional user names and passwords. With his newly acquired privileged access, he modified various pricing and availability of the products provided, reducing the price of some to zero dollars and cents. This led to customer service issues and financial losses were incurred to restore the site to its proper condition.

Police from the NSW Computer Crime unit were provided with log for this event, which readily identified the IP addresses used. From this a residential address was identified; occupant of which was the former employee. Police executed a search warrant on the premises and found evidence

including a handwritten list of passwords used to commit these crimes. The offender's laptop contained evidence of access to the web pages and the passwords used in these offences. The former employee was arrested and charged with two counts of 'unauthorized modification of data' under section 308D of the NSW Crimes Act 1900, offences which carry a maximum penalty of 10 years imprisonment. The offender pleaded guilty and was given a 12 month suspended sentence. Although not fully compensating for the losses incurred, the offender was also required to pay compensation of AUD5,570/-.

4. Client, products and business practices is defined as losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product. This can be categorized as suitability, disclosure & fiduciary and improper business or market practices. The IT aspects include:

- Disclosure of sensitive information to outsiders by employees
- Management of third-party suppliers

Case 10: In 2003, an Australian organization (the client) discovered that its valuable confidential and strategic information had been leaked to a competitor. The leak was the source of considerable angst and financial loss not only for the client organization but for the service organization that was entrusted with the information prior to its leak. In order for the service organization to preserve its relationship and reputation with its client, it was necessary to conduct a thorough investigation to determine the cause and source of the leak. Law enforcement agencies were also involved in the investigation. Investigation showed that an employee of the service organization had used the confidential document as a style template but inadvertently failed to save the changes to the document which would normally have removed the sensitive content. The employee e-mailed the unsaved template to another of its clients. The recipient, or someone within the recipient's organization, realizing the significance of the document, subsequently leaked it to the first client's known competitor. Improper use of computer technology led to a breach of security and subsequently to a deliberate leak of confidential information. The case also highlights the potential liability issues which can affect organizations if they contribute to someone else's loss, even inadvertently.

5. Damage to Physical Assets is defined as Losses arising from loss or damage to physical assets from natural disaster or other events. This can be categorized as disaster events & other events. The IT aspect includes:

- Misuse of IT resources
- Lack of security responsiveness

Case 11: An Australian university reported to the law enforcement that a machine within its network had been compromised, allegedly from an Australian ISP. It appeared this machine had been used as a base for the hacking of about 70 other machines over a two week period. The secondary victim sites were predominantly machines owned by academic institutions from around the world. Utilizing AusCERT's contacts, the owners of these machines were notified that they had

possibly been compromised and were requested to provide details to law enforcement. A number of secondary victims subsequently confirmed they had been successfully compromised. Law enforcement investigation determined the apparent source of the intrusion into the university was a compromised account with the ISP. Further inquiries identified a telephone number used to dial into the account and a probable attacker. The attacker installed a trojaned secure shell (ssh) on the primary university system, allowing connection to the machine bypassing other controls. Many of the secondary victim systems were running Red Hat Linux 6.2 'out of the box', with little configuration, no patching and no routine logging or system monitoring. There was evidence that the secondary compromised machines had been used to conduct further hacking activity and Distributed Denial of Service attacks (DDoS). When conducting inquiries with the source ISP and other telecommunication providers, other compromised accounts used by the attacker were identified (in addition to that used to attack the primary university victim). When interviewed, the offender made a full admission of hacking into the ISP, the university system and then into other systems worldwide. In September 2001, the offender entered a plea of guilty to charges of computer offences. He said he was aware of what he was doing and did it for the 'thrill'.

6. Business Disruption & Systems Failures is defined as Losses arising from disruption of business or system failures. This can be categorized as systems.

The IT aspects include:

- Hardware or software malfunction
- Communications failure
- Employee sabotage
- Loss of key IT staff
- Destruction of software/data files
- Theft of software or sensitive information
- Computer viruses
- Failure to back up
- (Distributed) denial-of-service attacks
- Configuration control error

Case 12: In March 2000, the Computer Crime Investigation Unit of the Commercial Crime Agency, NSW Police, investigated a sabotage attack against the GreenGrocer's network, which made it fail on two occasions. One of the attacks involved remotely deleting operating system files and caused the site to be unavailable for five days while analysis, clean up and recovery occurred. As an e-commerce merchant, GreenGrocer's network was critical to the company's ability to receive orders and earn revenue, which at the time was estimated to be about $22,500 per day. As a result of a

complaint made by GreenGrocer, NSW Police made enquiries with Telstra. An audit trail maintained by Telstra showed a remote connection immediately prior to the two incidents originated from an IP address belonging to a cable modem customer, who was identified as a former computer network engineer who had resigned from GreenGrocer days previously following a dispute with management. Further forensic analysis showed the perpetrator had on the first occasion telneted into the GreenGrocer's network router and deleted critical router files, rebooted the router and caused GreenGrocer to lose its connection to the Internet. In the second attack, using the pcAnywhere application, the perpetrator remotely accessed a server and deleted critical operating system files causing the server to fail. The perpetrator launched the attacks by utilising remote access services which were enabled during the period of his employment. The case highlights the importance of adopting sound personnel security practices such as disabling accounts following the departure of employees with privileged levels of access and of the need to monitor and better secure remote access services when they are required.

The perpetrator was convicted in February 2002 on two counts of damaging data in a computer, which carries a maximum sentence of 10 years imprisonment under s. 310(a) of the NSW Crimes Act 1900 but received an 18 month suspended sentence.

7. Execution, Delivery & Process Management is defined as Losses from failed transaction processing or process management, from relations with trade counterparties and vendors. This can be categorized as Transaction Capture,

Execution & Maintenance. The IT aspects include:

- Error in handling electronic media
- Unattended workstation
- Change control error
- Incomplete input of transactions
- Errors on data input/output
- Programming/testing error
- Operator error, e.g., in recovery procedures
- Manual procedure error

Case 13: October 19, 2000, when hundreds of flights were grounded or delayed because of software problem in Los Angeles air traffic control system, the cause was attributed to Mexican Controller typing 9 instead of 5 characters of flight-description data, resulting buffer overflow.

Risk indicators differ from loss events. They are not associated with specific losses, but indicate the general level of operational risk. Examples of risk indicators a firm might track are:

- amount of overtime being performed by back-office staff,
- staffing levels,
- daily transaction volumes,
- employee turnover rates,
- systems downtime.

From a modeling standpoint, the goal is to find relationships between specific risk indicators and corresponding rates of loss events. If such relationships can be identified, then risk indicators can be used to identify periods of elevated operational risk.

Once operational risks have been - qualitatively or quantitatively - assessed, the next step is to somehow manage them. Solutions may attempt to

- avoid certain risks,
- accept others, but attempt to mitigate their consequences, or
- simply accept some risks as a part of doing business.

Specific techniques might include: employee training, close management oversight, segregation of duties, purchase of insurance, employee background checks, exiting certain businesses and the capitalization of risks. Choice of techniques will depend upon a cost-benefit analysis.

Information Security Management System (ISMS)

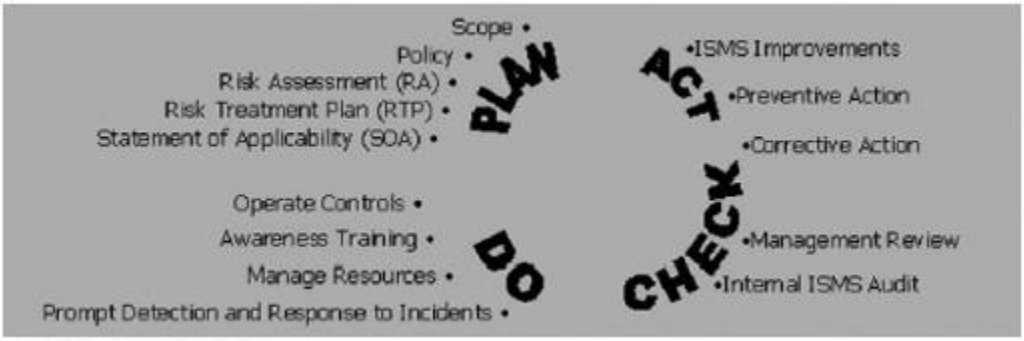
ISO/IEC 17799 (BS7799) can be applied to every bank and concerns information security, not just IT. It includes media such as paper, video telephones, faxes and other forms of electronics as well as personnel, procedures and physical aspects.

The standard stresses the importance of risk management and makes it clear that you do not have to implement every single guideline; only those that are relevant. The scope of the standard covers all forms of information, including voice, graphics and media such as mobile phones and fax machines. The new standard recognizes new ways of doing business, such as e-commerce, the Internet, outsourcing, teleworking and mobile computing.

An ISMS is the means by which Senior Management monitor and control their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer and legal requirements. It forms part of an organization’s internal control system. The Management Standard instructs you how to apply, build, operate, maintain and improve an ISMS. The activities

continually cycle around the PLAN-DO-CHECK-ACT cycle.

The major components of the ISMS can be summarized as follows:



Plan

Scope

The first step is to define the scope of the ISMS. It could be for the whole of the organization. It could be a particular site. It could be just a particular service - Internet banking for example.

ISMS Policy

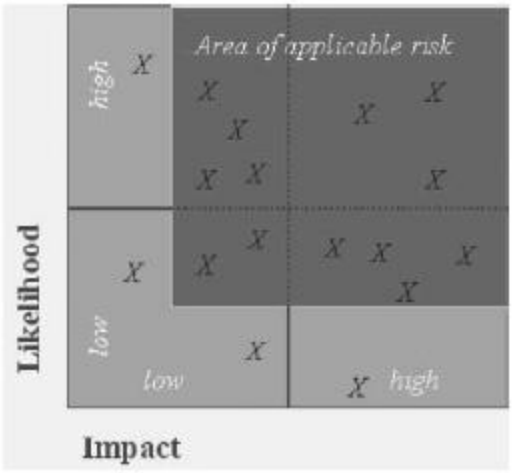
Why is information security important to an organisation? Is there a particular threat or other worries that concern it? What does it want to achieve, for example in terms of confidentiality, integrity and availability? What does it believe as an acceptable level of risk? Are there any constraints, such as laws and regulations, or particular ways in which it wish things done? Answers should be documented in a policy document. Note that it should cover the whole of the ISMS, not just the security controls. It is therefore far more extensive than the “information security policy”, referred to in the Code of Practice. It should be a relatively short document and signed off by the CEO. Security, as with all other internal controls flows down from the top of the organization.

Risk assessment

Now that what needs to be protected is known and what is an acceptable level of risk? What is the organisation’s actual risk? A method that is appropriate to the organization and the scope of its ISMS should be chosen. What are the risks?

These should be determined by a consideration of the impacts that would occur if some threat exploits a weakness in the organisation’s defenses to compromise the security of an asset and how likely is the impact to occur. Evaluate the risks. If the likelihood of the impact occurring against the magnitude of the impact is plotted, it may be felt that the risks are not of any great concern because even if they would have a major impact, they are extremely unlikely or even if they occurred all the time, they would have an insignificant impact.

The remaining risks are referred to as the applicable risks. These are the risks



that need to be controlled. The controls that reduce the risk to an acceptable level should either be in place, or they need to be introduced. It should be ensured that controls are in place that will indicate if a non-applicable risk turns into an applicable risk.

Risk management/Risk treatment

After completing the assessment of risk, ISMA requires decisions on how the risk can be managed. Should the organization merely rely on its ability to promptly detect and respond to security incidents? Or should the risks be avoided and transferred it to a third party (e.g. via insurance) or should appropriate controls be applied? This will result in a risk treatment plan.

Select control objectives and controls

The list is not exhaustive and additional control objectives and controls could be from ISMS. Not all of those listed in standard may be relevant to the Organisation's ISMS.

Statement of Applicability (SOA)

It is required that all the chosen security controls be identified and justified as to why it is felt that they are appropriate, and show why those BS7799 controls that have not been chosen are not relevant. The standard requires the selection of the controls be related back to the risk assessment. In practice, the selection of controls can be related back to statements in the ISMS policy.

Do

The DO part of the cycle requires the Organisation to operate the controls. A procedure is needed, as mentioned above, to ensure the prompt detection and response to incidents. It is also needed to ensure that all staff are security aware, are appropriately trained and are competent to carry out their respective security tasks. To ensure that all of this is carried out, it will be necessary manage the required resources.

Check

The purpose of the CHECK phase is to ensure that the controls are in place and are achieving their objectives. The standard identifies a variety of possible check activities:

- Intrusion detection
- Incident handling
- Routine checks
- Self-policing procedures
- Learning from others (e.g. CERT)
- Internal ISMS audit
- Management Review

Internal ISMS audit and management review are mandatory requirements of the standard. The others are optional.

Act

The outcomes of the CHECK activity are actions. There are three varieties:

- corrective action
- preventive action
- improvements.

BS7799 is a good standard to be used as a framework to manage technology risks and information security. ISO/IEC 17799:2005 defines 132 security controls structured under 11 major headings viz., Security Policy, Organizing Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communication and Operational Management, Access Control, Information System Acquisition, Development and Maintenance, Information Security Incident Management, Business Continuity Management and Compliance, to enable readers to identify the particular safeguards that are appropriate to their particular business or specific area of responsibility. These security controls contain further detailed controls bringing the overall number somewhere in the region of 5000+ controls and elements of best practice.

Advantages of BS 7799 Certification

- It will provide a structured, risk based approach to information security to manage technology risk
- The employees will have to take security seriously as adequate policies and penalties for any

breach of security have been framed.

- Clients and customers will be assured about the organisations' security seriousness.

- Foreign Partners that are paranoid about information security may feel comfortable dealing with the organisation if they have not already made it mandatory for it to be certified or audited by a security consultant.

- Since availability is one of the critical components for the banks, adequate business continuity management plans should have been set up.

All of the above can be done without aiming for a certification, but a marketing advantage is achieved if a certification is obtained .

References

ISO/IEC 17799:2005
CSI/FBI Computer Crime and Security Survey – 2003, 2004, 2005
Australian Computer Crime and Security Survey – 2003, 2004, 2005
Web Page on Computer Crimes of the Dept of Justice, U S A

Sujit Christy

Sujit Christy is a Manager Information Security with Keells Business Systems Limited, Colombo. He is a regular speaker at conferences, seminars and workshops on various information security topics. He has over 12 years of experience in Information security, consulting and auditing. He obtained his Bachelors Degree in Commerce from the University of Madras, India. Sujit is a Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP) and a BS7799 Lead Auditor. He is the CISA/CISM certifications coordinator and a member of the Board of Information Systems Audit Control and Association (ISACA) Sri Lanka Chapter. He is the founder and secretary of the Information Systems Security Association (ISSA), Sri Lanka Chapter.