5-2012

An Optimized Dynamic Process Model of IS Security Governance Implementation

Mathew Nicho
University of Dubai, mnicho@ud.ac.ae

An Optimized Dynamic Process Model of IS Security Governance Implementation

Mathew Nicho
University of Dubai
mnicho@ud.ac.ae

Abstract:

The year 2011 has witnessed a lot of high profiles data breaches despite the availability of IS security and governance controls, frameworks, standards and models for organisations to choose from; and the technical advances made in intrusion prevention and detection. Taking this issue into account the objective of this paper is to identify and analyse the weaknesses in the IS security defences of organisations from a holistic perspective, and propose a dynamic IS security governance process model for the implementation of appropriate controls and mechanisms for optimised IS security. Optimization is achieved through the strategic overlap of security and governance frameworks implemented in a prioritized phased manner for efficiency and effectiveness in cost, time and effort. The paper starts with the analysis of data breaches to identify the weaknesses in the organisational information system. This is followed by the analysis of recommended requirements and dimensions of effective IS security architecture, IS governance, concepts and models to identify relevant frameworks used in IS security and governance. Thereafter, the best practices for implementing the model is evaluated and finally the frameworks and IS entities are integrated into an optimized Information Systems Security and Governance (ISSG) process model.

Keywords:

IS security governance, IS risk management, security culture, IS security best practices, Data breaches, COBIT, ITIL, RiskIT, PCI DSS 2.0, ISO 27002

1. Introduction

Information system is critical not only for the efficient and effective functioning of an organisation, but have also become the custodian of sensitive customer and corporate information raising legal, regulatory and ethical issues. Hence, any disruption or breach into the organizational network affects all stakeholders. The embrace of cloud computing and outsourcing have compounded the security threat since confidential information is stored in remote servers on the Internet. Morever, the high profile and persistent IS security breaches in 2011 in Sony, the data-security firm RSA, Lockheed Martin, the email wholesaler Epsilon, the Fox broadcast network, NASA, PBS, the European Space Agency, the FBI, the British and French treasuries, Citigroup, and other organisations (Liebowitz, 2011) have exposed the weakness of the current IS security model and architecture, in preventing intrusions into

organisational networks. These breaches have sent the message that technical controls are not sufficient to prevent breaches as hackers have found ways to bypass the organizational IS security defenses by using a combination of social–technical methods.

2. IS Security Breaches

The data breach at RSA, Sony and Epsilon occurred due to spear phishing rather than highly sophisticated hacking. Spear phishing is a type of attack using a technique commonly known as Advanced Persistent Threats (APT), where the attacks target individual employees rather than organizational security defenses. One simple flaw or oversight by the employee is all that is required for entry into these defenses. When it comes to APTs it is not about how safe, secure and good the company is, but that a totally new approach for entering the organization is selected where the attacker does not bother to hack the organization and its infrastructure, but rather focus on hacking the employees and then escalate the privileges. According to a key manager at RSA, technological advances in IS security and the use of IS security controls/frameworks, and compliance on IS security regulations have prevented the IS security breaches to a great extent. However, on March 17th 2011 a data breach occurred in RSA which provides security, risk, and compliance solutions for most of the Fortune 500 companies for managing their security. Unlike other data breaches, no customer data like email addresses, usernames, credit card numbers, date of birth or social security numbers were stolen. The attackers used a common form of phishing called spear phishing where they sent two different phishing emails over a two-day period. The two emails were sent to two small groups of lower level employees with the email subject "2011 Recruitment Plan." The email went to the junk folder, but one employee retrieved it from the junk mail folder, and open the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls. The spreadsheet contained a zero-day exploit (are exploits for vulnerabilities that are not yet publicly known) that installed a backdoor through an Adobe Flash vulnerability. The attacker then proceeded to install a remote administration tool (a variant of Poison Ivy set in reverse mode) that allows the attacker to control the machine. In this reverse connect mode the victim machine reaches out and connect to the command and control rather than the other way around bypassing the firewall state table. Once this was set up, the attacker started digital shoulder surfing to establish the employee's role and their level of access (Rivner, 2011). According to various sources, the estimated cost to the company through this attack is $ 66 million in direct and attributable costs (ibid). It was revealed that a similar methodology was used in the case of Sony PlayStation data breach where it was suspected that the hackers used spear phishing to enter the network and take control of the PC of a system administrator, who had rights to access sensitive information about Sony's customers. They did that by sending the administrator an email message that contained a piece of malicious software that got downloaded onto his or her PC. An analysis of these breaches reveal, that if a few non-technical procedures were followed, majority of these breaches could have been avoided, pointing to the fact that relying on technical controls alone may not be effective.

Statistics on data breaches from various sources point to the severity of the situation. Resources from these sources are taken and analyzed to view the trend and weaknesses in networks. Identity Theft Resource Center (ITRC, 2011), a not for profit organisation tracking data breaches in the United States , reported that hacking accounted for the largest number of breaches in the first quarter of 2011, as almost 37% of breaches were due to malicious attacks on computer systems which is more than double the amount of targeted attacks (17.1%) reflected in the 2010 ITRC Breach List. By the end of 2011 (December 31st 2011), there has been 414 reported breaches with 22,945,773 records compromised in 2011, and this does not include the breaches not reported, veiled from public and unknown. The last five years (2007 to 2011) statistics is shown in table -1, and illustrated in figure -1 and figure -2 (ITRC, 2007, 2008, 2009, 2010, 2011).

Year	Breaches	No. of records
2007	65	3,997,133
2008	97	7,311,833
2009	498	223,146,989
2010	662	16,167,542
2011	414	22,945,773

Table -1 Data breaches in organisations

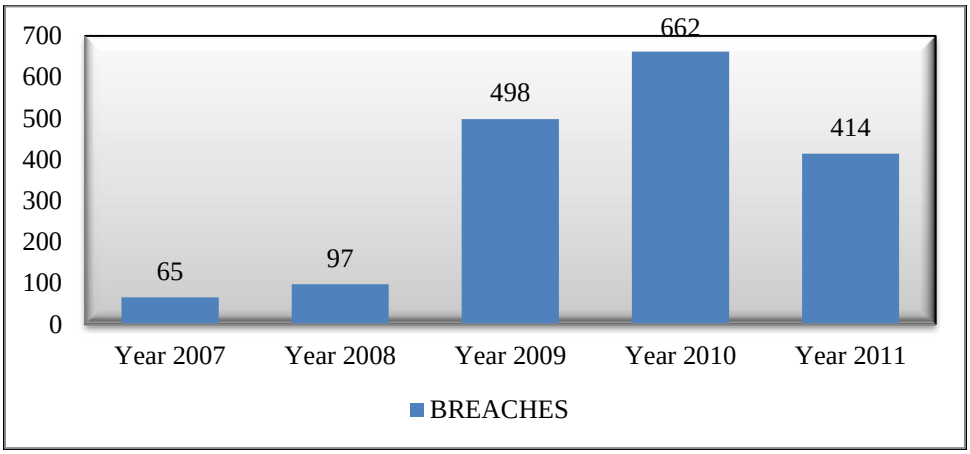

Figure -1 Number of data breaches

While the ITRC statistics (based on publicly reported cases only) point to the decrease in the number of breaches, at the same time the increase in the number of records from each breach, point to the increase in severity of the breach. The year 2009 is an exception since 206 million records was breached from two cases alone (Heartland Payment and US Military of 130 and 76 million records respectively).

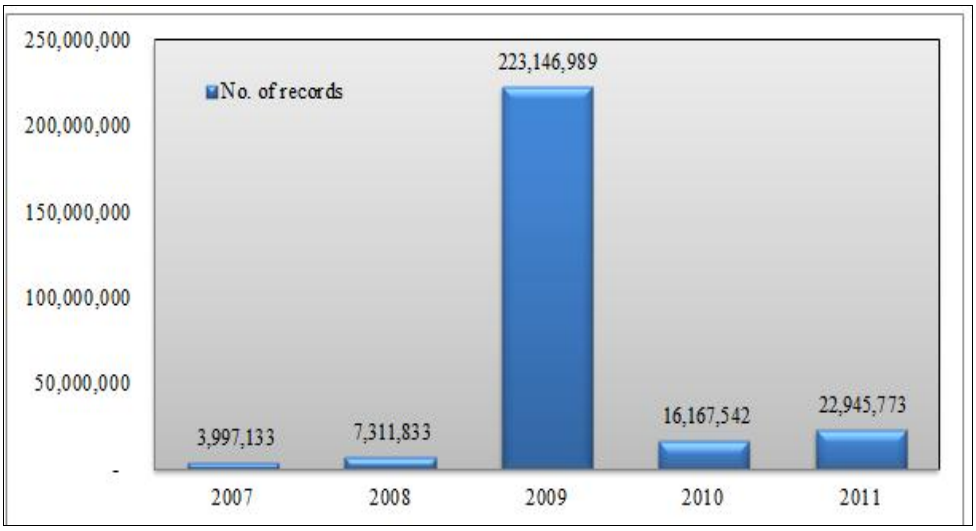

Figure – 2 Number of records breached

The largest breach on record, the Heartland Payment Systems (a PCI DSS compliant transaction processing company transacting US $ 80 billion) attack, was a technical one using SQL injection through a vulnerability in the code written eight years ago for the web form. This allowed access to Heartland's corporate network, according to Robert Russo, general manager of the PCI Security Council (Vijayan 2010). This vulnerability was not identified through annual internal and external audits of Heartland's systems or through continuous internal system-monitoring procedures. This provided a means to extend the compromise from the corporate network to the separate payment processing network (Cheney, 2010). The attack went unnoticed for six months while the attackers continued their nefarious activities in the network. According to Verizon 2011 report, 96% of the breaches were avoidable through simple or intermediate controls. A list of reported breaches in organisations (from January to August 2011) where more than 100,000 records compromised (given in figure 3) is analyzed to find out the factors behind the breaches which shed light on the issues to consider to provide a robust model of IS security (source: ITRC, 2011).

Out of the 20 reported breaches, the largest of these was reported by TRICARE SAIC on Sept. 14. It happened when the backup tapes containing electronic health care records used in the military health system to capture patient data from 1992 through Sept. 7, 2011, in San Antonio-area military treatment facilities was lost. Table 2 presents results based on the analyses of the top twenty breaches, the type of breach and analysis.

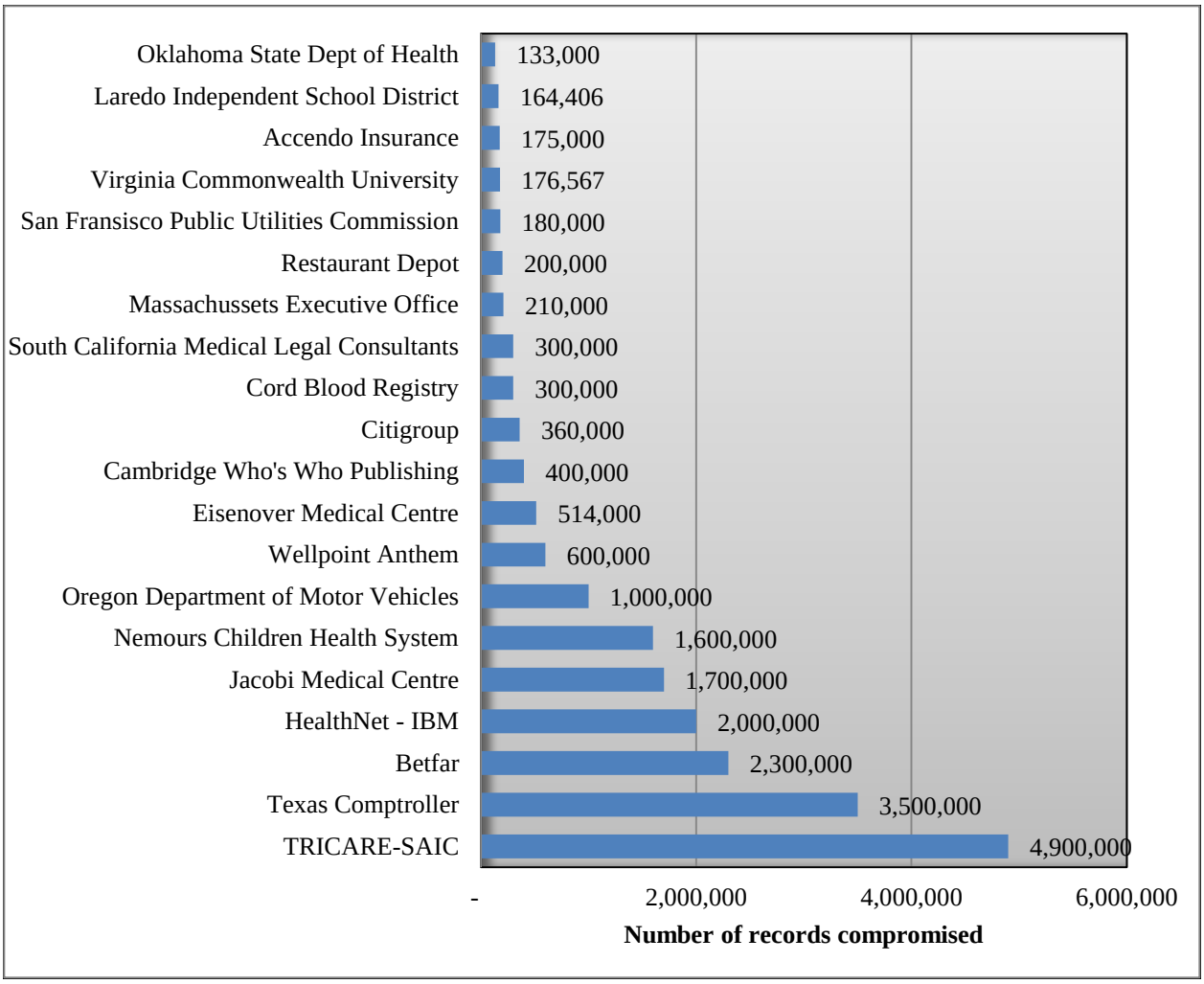

Figure – 3 Data breach in various organisations reported in 2011

	Organisation	Nature of breach	Evaluation
1	TRICARE-SAIC	Backup tapes containing SAIC SAIC data stolen from the car of a Tricare employee.	Non-technical – employee error; procedure not followed
2	Texas Comptroller	Unencrypted information transferred and kept in a server accessible to the public	Correct procedure not followed when transferring information across servers
3	Betfair	SQL injection attack on a code vulnerability	*Technical breach*, procedure not followed especially network segregation and file integrity monitoring.
4	Health Net IBM	Nine server drives went missing from the data centre of the California office of Health Net	Appropriate policies and procedures were not been followed by those responsible for both the physical and logical protection of critical data.

5	Jacobi Medical Centre	The files (cassette tapes in a box) was stolen from a van operated by GRM Information Management Services, when the driver left the van unattended and unlocked.	Correct procedure not followed prior to and when transporting storage media
6	Nemours Children Health System	Unencrypted computer backup tapes containing patient billing and employee payroll data stolen from a Nemours facility in Wilmington, Delaware	Correct procedure not followed when storing storage media. As per the control, the tapes were supposed to be safely locked
7	Oregon Department of Motor Vehicles	USB or CD containing personal information lost from the department. Thief caught.	Correct procedure were not followed when storing/disposing redundant data
8	WellPoint Anthem	A flaw in the website allowed hackers to manipulate the web address within the site to gain access to applicants' information.	An upgrade to the server caused the vulnerability, but it was later revealed that security measures were not audited and validated for the system
9	Eisenhower Medical Centre	The computer used to check-in patients at the Center in Rancho Mirage was stolen from the open lobby area	Correct procedure not followed. The computer was not protected with any sort of drive encryption mechanisms, and not physically locked.
10	Cambridge Publishing	The data tapes was stolen or lost by an outsourced company when the drive (with the tape inside) was sent for repair to the outsourced company	Correct auditing procedure not followed when repairing storage media. Tape kept inside the drive by mistake.
11	Citigroup	The attackers logged into Citi's consumer website for credit-card holders using legitimate accounts and they changed characters in their Web browsers' address fields to move around to new accounts. Thereafter it was suspected that they automated the process, writing a short program to cycle through possible account numbers and capture the data displayed in the browser window for each one (Wagenseil, 2011).	*Technical flaw*. If the bank had used a method other than the account number to identify the account to the browser, the breach could have been avoided.
12	Cord Blood Registry	A computer along with the backup tapes containing member personal and financial information were stolen from an employee's locked car.	Correct procedure not followed when storing/transporting storage media
13	Southern California Medical-Legal Consultants	Personal medical data were available online in an unsecured format and could be accessed through Internet searches.	*Technical flaw*. SCMLC President admitted that their internal security policies and procedures were not followed (the website was not password protected).
14	Massachusetts Executive Office	A variation of the persistent virus W 32. QAKBOT infected 1,500 computers at the agency's offices and career centers	Procedures on using portable storage devices, download of files and clicking on suspicious web links could have prevented the breach.
15	Restaurant Depot	Hacking - cybercriminals placed malware	*Technical breach* by expert hackers

		onto the credit and debit card processing systems used in Restaurant Depot's stores, harvested the stolen data and sent it to a server in Russia.	
16	San Francisco Public Utilities Commission	The incident involved a server housing sensitive data got infected with malware. " The server was open onto the Internet and had an encoded file with customer data.	*Technical breach*. Procedures were not followed. It was speculated that hackers might have injected malware through an open port on the server . The file was not encrypted and the data was stored in plain text.
17	Virginia Commonwealth University	According to forensic reports hackers accessed the system from an IP address within US and planted malware on one server (outside the firewall) which infected another server (containing sensitive data inside the firewall) and created two accounts	*Technical breach*. Breach discovered on 24th October. Analysis still going on regarding the cause
18	Accendo Insurance	Personal information may have been exposed during mailings of transition fill letters to physicians. While the mailings were addressed correctly and received by the recipients, a formatting change shifted the text of the letters, showing some lines of text through the envelope window.	Non-technical error, attributed to formatting of letters while drafting and sent to printer
19	Laredo Independent School District	A disk holding personal information current and former students in the Laredo Independent School District has gone missing/lots in transit.	Non-technical error, when standard encryption and data media transport policy was not enforced. The school doesn't know who has signed off the disk to be sent.
20	Oklahoma State Dept of Health	Department laptop which contained client personal information was stolen from the car of OSDH's employee in broad daylight.	Procedure not followed for transport of electronic and storage devices along public places. A Simple laptop encryption software could have mitigated the risk

Table -2 Analysis of the top twenty breaches

A review of these twenty cases reveal that sophisticated hacking took place only in four cases (numbers 3, 15, 16 and 17) compromising only 20% of the cases with 13.73% of the 20.81 million records (in the top 20 listed in figure -3) breached. Technical error resulted in 15% of the cases with 6.05% of total records breached. Compared to these two technical attacks, non-technical errors (which could not have been prevented through normal network security defenses) accounted for 65% of the cases with 80.22% of total records breached. This means that 13 out of 20 breaches or 16.6 million out of 20.81 million record breach could have been prevented by implementing and following relevant IS security and governance controls.

Expanding the statistics from the sample of twenty cases to the entire 414 reported breaches, reveal that breaches in 269 out of 414 organizations could have avoided. Converting this into financial terms, the above figure and loss statistics of Ponemon Institute (2011) is taken for

analysis. They estimated that the annualized cost of cybercrime to an organizations is $5.9 million per year (based on the median annualized cost for 50 benchmarked organizations); which in the ITRC cases, amount to $1587 million (269.1 x $5.9 million) saved by following simple procedures. If those organisations that had been breached, but not reported or veiled from public have been included, the savings in US alone can be staggering. To evaluate whether this amount ($1587 million) is realistic another statistic is taken to compute the values. According to Forrester Research, (Gaudin, 2007) the cost of breach of a record which includes outside legal fees, notification costs, increased call center costs, marketing and PR costs, and discounted product offers falls between $90 and $ 305. This amounts to (20.81 million x $90 - $ 305 = $ 1872 to $ 6347 million (the conservative figure $ 1872 million comes close to the previous calculated amount).

In a survey on UK business on IS security (by the UK Government Department for Business Enterprise and Regulatory Reform and PriceWaterhouseCoopers in 2008), it was revealed that 45% of the companies with less than 50 staff; 72% with more than 250 staff and 96% of the companies with more than 500 staff have suffered a security incident in the previous year. This comes to an average of 71% of companies being subjected to a security incident. Regarding the cost of responding to an attack Ponemon Institute (2011) found that from 2010 to 2011, the time and cost required to respond to security breaches has increased from 14 days in 2010 to 18 days in 2011 with an average daily cost of attacks increasing from $17,600 to nearly $23,000. Incorporating the PWC research statistics of 71% of the entire companies in UK having experienced an attack to the tune of $17000 to $23000 the total amount spent/lost is staggering.

An overview of analysis of threats from various sources, reveal the extent of threat. In the year 2010 alone Symantec encountered more than 286 million unique variants of malware; 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009 and an average of 260,000 identities exposed in each of the data breaches caused by hacking (Symantec, 2011). Symantec also reported a 42% rise in the number of reported new mobile operating system vulnerabilities (from 115 to 163), 6253 new vulnerabilities, and 14 new zero day vulnerabilities in applications such as Internet Explorer, Adobe Reader, and Adobe Flash Player.

The 2011 Verizon data breach investigation report conducted by the Verizon Risk team, the US Secret Service and the Dutch High Tech Crime Unit reveals that most of the data breaches in organizations in 2010 are not the result of highly sophisticated attacks, but rather the victims are a target of opportunity than choice (Verizon, 2011). Moreover, according to Verizon almost all breaches are avoidable without difficult or expensive corrective action. In the year 2010 Verizon reported that 83% of victims were targets of opportunity, 92% of attacks were not highly difficult, 76% of all data was compromised from servers, 86% were discovered by a third party, 96% of breaches were avoidable through simple or intermediate controls, and 89% of victims subject to PCI-DSS had not achieved compliance.

These points to the fact that implementing security mechanism alone is not sufficient to prevent data breaches as technical, non-technical controls and best practices in information security and governance is required to provide optimized rather than adequate protection. For instance, in the

case of the Betfair data breach (Amsel, 2011), the forensic investigation report prepared by the digital security consultants - Information Risk Management concluded that:

> "Information security was not implemented in accordance with best practice … appropriate information security governance is not in place within Betfair and as a consequence the business has been exposed to significant risks … appropriate technical controls relating to such elements as network segregation and file integrity monitoring that would provide Betfair the ability to deter, prevent and detect such an incident are not in place."

To find out the reasons for the persistent attacks and weakness in IS security it is imperative to look at the actual issues facing IS security managers from their perspective and get recommendations/requirements for an efficient and effective security architecture.

3. Issues and Requirements in IS Security

Data breaches and hacking through carelessness in following procedures and controls have emerged as a serious and growing issue in organisations and personal computers alike. Hence it is worthwhile to look at the IS security issues facing organisations to substantiate this. Two studies are taken for analysis, one a global study of 874 IS security certified professionals worldwide, and the other a study of 623 US based IS security professional who re-ranked the same issues (Knapp, Marshall, Rainer & Morrow, 2008). Both the surveys came up with a ranked list of 25 information security issues (see table 3).

An analysis of the issues based on matching the issues in the top five in both the surveys reveal top three common issues four issues namely:

i. Top management support
ii. Malware attacks like viruses, Trojans and worms
iii. User awareness and training

Here non-technical issues like top management support and, user awareness and training comprise two third of the top three issues facing managers followed by malware attacks implying the importance of these two issues in preventing malware attacks. Overall, the issues can be categorized into technical, non-technical, and those that are both technical as well as non-technical in nature (table – 4) that may reveal the extent of support that IT personnel personal have to give to technical as well as non-technical issues in ensuring an effective IT security environment.

The evaluation of the major issues supports the need for a broader perspective of IS security incorporating IT governance (which includes all the non-technical issues, and some technical issues given in table -4). This points to the need to look at IS security from a non- technical perspective as well. This necessitates a review of IS security and governance controls available and employed, to evaluate where these can fit into current IS security domain and to analyse the

available IS security models to see how these can be integrated into an optimized IS security governance framework

	Global Study (874 respondents)		US study (623 respondents)
1	Top management support	1	Top management support
2	User awareness training & education	2	Legal & regulatory issues
3	Malware	3	Malware
4	Patch management	4	User awareness training & education
5	Vulnerability & risk management	**5**	Protection of privileged information
6	Policy related issues (enforcement)	6	Business continuity & disaster preparation
7	Organisational culture	7	Low funding & inadequate budgets
8	Access control & identity management	8	Lack of skilled security workforce
9	Internal threats	9	Fighting spam
10	Business continuity & disaster preparation	10	Inherent insecurity of networks & information systems
11	Low funding & inadequate budgets	11	Standards issues
12	Protection of privileged information	12	Vulnerability & risk management
13	Network security architecture	13	Policy related issues (enforcement)
14	Security training for IT staff	14	Security training for IT staff
15	Justifying security expenditure	15	Governance
16	Inherent insecurity of networks & information systems	16	Patch management
17	Governance	17	Access control & identity management
18	Legal & regulatory issues	18	Justifying security expenditure
19	External connectivity to organisational networks	19	Network security architecture
20	Lack of skilled security workforce	20	Organisational culture
21	Systems development & life cycle support	21	Internal threats
22	Fighting spam	22	Systems development & life cycle support
23	Firewall & IDS configurations	23	Wireless vulnerabilities
24	Wireless vulnerabilities	24	External connectivity to organisational networks
25	Standards issues	25	Firewall & IDS configurations

Table 3: A comparative study of IS security issues globally and in US

Technical	Non-technical	Both
Malware	Top management support	Vulnerability & risk management
Patch management	User awareness training & education	Internal threats
Access control & identity mngmt	Policy related issues (enforcement)	Protection of privileged information
Network security architecture	Organisational culture	Inherent insecurity of networks & information systems
Fighting spam	Business continuity & disaster preparation	External connectivity to organisational networks
Firewall & IDS configurations	Low funding & inadequate budgets	Systems development & life cycle support
Wireless vulnerabilities	Security training for IT staff	
	Justifying security expenditure	
	Governance	
	Legal & regulatory issues	
	Lack of skilled security workforce	
	Standards issues	

Table 4: Differentiating between technical and non-technical issues in IS security

4. Optimized Perspective of IS Security

The term 'optimal' refers to the relevant components of 'requirements' and 'dimensions' for an organisation thus creating a synergic (multiple) effect through mapping and appropriate integration. IS security problems cost millions of dollars for US companies and billions for the overall US economy and the question is not whether organizations need more security, but to look at cost-benefit methods to evaluate IT security to 'optimize' security countermeasure investments and reduce spending without sacrificing protection (Arora, et al., 2004). Incorporating the requirements and dimensions of information systems security effectiveness results in an optimized information security governance model

	Requirements	Methods to achieve this requirement
1	Be holistic and encompassing	*Incorporate and integrate industry relevant security and IT governance frameworks*
2	Make suggestions on how different controls can be synchronised to achieve maximum effect	*Synchronization can be achieved through mapping the different controls to achieve a synergic effect.*
3	Include a comprehensive approach to information security risk management	*Using risk management framework like the RiskIT approach by ISACA*
4	Follow a predetermined life-cycle approach	*Apply a PDCA cycle as stated in ISO 27001. ISO IEC 27001 uses the Plan-Do-Check-Act model. Plan in section - 4, Do in section -5, Check in section – 6 and 7, Act in section – 8.*
5	Be measurable	*Using multi-dimensional measurement methods instead of just a tick it approach. According to CSI Computer Crime and Security Survey 2010/2011 (2011), many respondents named tools that would improve their visibility—better log management, security information and event management, security data visualization, security dashboards and the like.*

Table – 5: IS Security Architecture

The high incidence of security breaches in organizations could be attributed to the organization's inability to adequately focus on non-technical issues in information systems security, namely policies, procedures, practices, and strategies that, organizations normally put in place to minimize threats (Dhillon and Backhouse 2001; Straub and Welke 1998; and Siponen, 2005 cited in Ifendo, 2009). This necessitates an ever increasing need to manage IS security from a multidimensional, holistic and comprehensive manner for ensuring a secure IS environment (Solms, 2001). Moreover IS security need to be built like a staircase of combined measures (Hagen, Albrechtsen and Howden, 2008) as various dimensions of IS security are mutually dependent on each other (Sundt, 2006; Berghel, 2005 cited in Hagen, Albrechtsen and Howden, 2008). Elof & Elof, (2005) have proposed an integrated architectural approach to information and computer security that operates in a distributed, heterogeneous and multidisciplinary business environment. They have given five requirements for the architecture (table -5):

From the breaches mentioned in section - 1 it is evident that a security awareness culture and use of appropriate success factors implementing relevant frameworks is lacking in the affected organisations. This necessitates the need for extended requirements to include a security culture and implementation success factors. Researchers have proposed a information security-aware culture to minimise risks to information (Veiga & Elof, 2010; Niekerk & Solms, 2010). Hence, an additional requirement (requirement -6) is to create and implement a continuous organisation specific dynamic security awareness and training program. While frameworks are in itself best practices for implementing IS security standards and complying with regulations, proper implementation is required to make the model successful. The data breaches and attacks have proved that despite the presence of IS security and governance frameworks, breaches have happened (Eg: Heartland Payment Systems Breach the largest breach reported since 2008 was PCI DSS compliant and certified). This requires following industry specific critical success factors and best practices in implementation (requirement – 7) of relevant standards. Success factors have been proposed for IT governance implementation namely the 33 ITG best practices (Grembergen and Haes, 2009) and ITIL best practices (Pederson et. al., 2010; Iden & Langeland, 2010, Tan, Cater-Steel & Toleman, 2009).

Elof & Elof (2005) regard IS security as a multidisciplinary concept cutting across several related disciplines. In this respect Solms (2001, p. 504) stated that "if information security is not addressed in a holistic and comprehensive way, taking all its dimensions into account, real risks exist preventing a really secure environment". In this respect, Solms proposed a multidimensional character of information security, incorporating twelve dimensions focusing on governance, audit, legal, technical, human and measurement areas that need to work together for creating a secure IS environment.

Table 6 illustrates the 12 dimensions and the corresponding frameworks/models/acts. In a global survey on 834 business executives and heads of information technology (IT) covering 21 countries and 10 industries on the control frameworks used in enterprise governance of IT, 28% of those surveyed use ITIL/ISO 20000, 21.1% use ISO 27000/related security frameworks, 15.1% use Six Sigma, 12.9% use COBIT, 12.7% use PMI/PMBOK, and 12% use RiskIT framework of Information Systems Audit and Control Association (ISACA), along with other frameworks (ITGI, 2011). Out of these, only Six Sigma and PMI/PMBOK are less oriented towards IT security and governance. While the above controls are IT governance oriented encompassing IT security, PCI DSS is a standard focusing purely on the technical aspects of information technology focusing on protecting cardholder data.

Dimensions	Available frameworks
Strategic/corporate governance	Commonly used frameworks are ITIL/ISO 20000, ISO 27000 and related security frameworks, Six Sigma, COBIT, PMI/PMBOK, RiskIT, and other related frameworks (ITGI, 2011)
Governance/ organisational	Evident in the four domains of COBIT and encompass the IS in the organisation
Policy	IS Security policy endorsed in COBIT, ISO 27K series, NIST, ITIL
Best practice	33 ITG best practices (Grembergen and Haes, 2009); ITIL best practices (Pederson et. al., 2010; Iden & Langeland, 2010)
Ethical	Extended Information Systems Secure Interconnection (ISSI) model (Leiwo & Heikkuri, 1998) address the ethical aspect of IS security
Certification	Certifications available for COBIT, ITIL, ISO
Legal	Regulations like FISMA, HIPAA, SOX relate to IS security
Insurance	*(Relevant only for insurance companies)*
Personnel/human resource	Taken care of in relevant section/controls in COBIT, ITIL, ISO 27002 controls
Awareness	Information Security Culture Framework (Veiga & Eloff, 2010; Schlienger & Teufel, 2003)
Technical	PCI DSS 2.0 & ITIL are more technical in nature than COBIT
Measurement/metrics	Guidelines given in COBIT, ISO 27004 & ITIL – as metrics, goals, key performance indicators, key goals indicators, and maturity model in COBIT.
Audit	COBIT is an IS audit tool. Moreover European Union selected COBIT as an auditing standard for IT Security (Summerfield, 2005)

Table – 6: Dimensions of IS security mapped with related IS control frameworks/standards

5. Role of Governance in IS Security

Since IT governance is an integral part of IT Secuirity (Elof & Elof, 2005; Solms, 2001), the definition and management of IT security is analysed to view its role. *Information security management* is defined as "the process of administering people, policies, and programs with the objective of assuring continuity of operations while maintaining strategic alignment with the organisational mission" (Cazemer et al. 2000, cited in Choobineh, et al., p. 959) while the management of information security is primarily concerned with strategic, tactical, and operational issues surrounding the planning, analysis, design, implementation and maintenance of the IS security program (Choobineh, Dhillon, Grimaila & Rees, 2007). The definition and management not only provides a very broad meaning taking into account technical, non-technical and strategic aspects of IS security, it emphasizes maintaining the IS operations with the objective of IS security management as being strategic alignment in nature. This strategic alignment of linking IS security mission and goals with the organizational strategic mission and goals is the prime objective of IT governance. Moreover, in a global survey of 7000 IT professionals, the importance of strategic alignment of organisational goals with the IT goals was cited by 90% of the surveyed as vital to organisation (ITGI, 2006; ITGI, 2008). Thus it can be safely assumed that the effective implementation of information security involves, using a strategic mix of the IT governance frameworks, (that aligns the IT goals with the organisational

goals), IT service management framework (that maintain efficient and effective continuity of operations), along with compliance with relevant security standards (policies and programs).
While it has been emphasised that governance is a key to success in setting standards, success is more likely if the governance structure includes all of the various interests in the network, and moreover the standards (ex. ISO 27 K, PCI DSS, ISO 20000) themselves need to be effective yet flexible enough to satisfy competitive interests (Sullivan, 2010). In this respect Solms (2001, p. 504) have argued that "if information security is not addressed in a holistic and comprehensive way, taking all its dimensions into account, real risks exist preventing a really secure environment". The effective and efficient utilization of information technology requires the alignment of the IT strategies with the business strategies (Luftman, Lewis & Oldach, 1993; Luftman & Brier, 1999). Since alignment of IT strategies with the business strategies is the objective of IT governance, it is worthwhile to view security from an IT governance lens taking into account the internal and external issues that impact IS security. In this respect, information security should not be perceived as a technical issue alone, but as a business and governance challenge that involves adequate risk management, reporting, and accountability. Thus apart from securing information systems assets organisations have the extra role of complying with mandatory and voluntary standard and regulations imposed by external entities. Hence it is worthwhile to view IS security from a compliance and assurance perspective. According to Bishop (2003) security has three components namely requirements, policy and mechanisms.
Ponemon Institute's (2011) study of 160 senior managers in a sample of 46 multinational organizations revealed that the average cost of compliance was $3,529,570 while the cost incurred due to non-compliance was $9,368,351. This amounted to a net savings of $ 5,838,781 ($9,368,351-$3,529,570) for compliant companies. Thus, the non-compliance cost is 2.65 times the cost of compliance. Since compliance to a variety of information security standards is mandated by regulations, organisations need to act and implement a proactive information security enforcement strategy (Madan & Madan, 2010).

6. IT Control Frameworks for IS Security

Information Security Governance, which is an important component of the IT governance and an integral part of the enterprise governance, could be regarded as implementing the governance concepts and principles on information security issues (Abu-Musa, 2010) (ibid). While a "control framework is a recognised system of control categories that covers all internal controls expected in an organisation" (IIARF 2002, cited in Liu & Ridley, 2005, p. 2), an internal control provides reasonable assurance regarding the achievement of objectives in the area of effectiveness and efficiency of operations, reliability of financial reporting and compliance with regulations (Pathak, 2003). Internal controls are policies, procedures, practices, and organisational structures put in place to reduce risks (Kim, et al., 2008). Currently implementations of IS control frameworks are on the rise worldwide, due to compliance and regulatory requirements to various regulations and standards.

In a survey of security professionals, the Enterprise Strategy Group (ESG) discovered that 72 percent of North American organizations with 1,000 or more employees have implemented one or more formal IT best-practice control and process models (Turner et al., 2009). Among these, the study stated that the most widely used commercial IT control frameworks are ITIL, ISO 27002 and COBIT, which provide optimal security management. Furthermore, it had been stated that ISO/IEC 27002, COBIT, ISO 20000, and ITIL are the most applicable and widely used standards to manage and maintain IT services (Sahibudin, Sharifi & Ayat, 2009). IT control implementers use, ITIL to define strategies, plans and processes, COBIT for metrics, benchmarks and audits and, ISO/IEC 27002 to address security issues to mitigate the risks (ibid).

Considering the more technical security aspects of protecting cardholder data, the requirements set by PCI DSS are in line with the IT security best practices required by widely recognised standards such as ISO 27002, and COBIT (Laredo, 2009). Gikas (2010) did a mapping of ISO 27000 with the PCI DSS and found out 70 similar technical controls between these two standards. PCI DSS is a regulatory requirement that is mandatory for those dealing with credit cards to ensure the protection of cardholder data; ISO 27002 is a non-regulatory code of practice for information security (ISO, 2011); and ISO/IEC 20000 (an internal requirement), is the first international standard for IT Service Management implemented through ITIL. On the other hand, COBIT address the business issues namely company-wide principles, goals and needs in terms of information processing through its various controls in the four domains of IS (Humphreys et al., cited in Posthumous & Solms, 2004). In the case of a risk-based approach to IS security, ISACA has released the Risk IT Framework (ISACA, 2009) as a framework to identify, govern and manage information technology risks. This framework fills the gap between generic (non–technical) risk management frameworks and technical (security-related) IT risk management frameworks.

7. Optimized IS Security Governance (ISSG) Implementation Model

An optimized IS security governance model takes into account the following (based on mapping the overlapped extended requirements outlined in table 5 and dimensions in table 6):

1. A holistic approach to IS security incorporating the comprehensive non-technical aspects of corporate/IS governance encompassing the entire IS in the organisation, as well as technical enough to ensure layered and detailed protection to organisational information assets;
2. An effective and ethical IS security policy that complies with the legal and regulatory requirements;
3. Synchronizing and mapping relevant IS security and governance control frameworks for efficiency, effectiveness and synergy;
4. Viewing IT governance security from a risk based perspective using the Risk IT framework or similar approach;

5. Following a life cycle approach to implementation incorporating industry specific dynamic success factors before, during and after implementation
6. Making sure that the people involved in IT and business share a common security culture through continuous multi-level optimally crafted technical and non-technical training.
7. A multilevel multidimensional aggregated dashboard for tracking and monitoring IS security governance entities using more than one metric.

IS security governance is an ongoing process due to external factors like the dynamic nature of security threats, technological advances and changes/introduction of IS related regulations and internal factors namely the dynamic change in strategic direction, change/update of IS assets, and personnel movement and turnover. Thus, a dynamic process model is preferred to a static model. Based on the seven components, the Figure – 6 provides the process of implementing the optimized ISSG model.

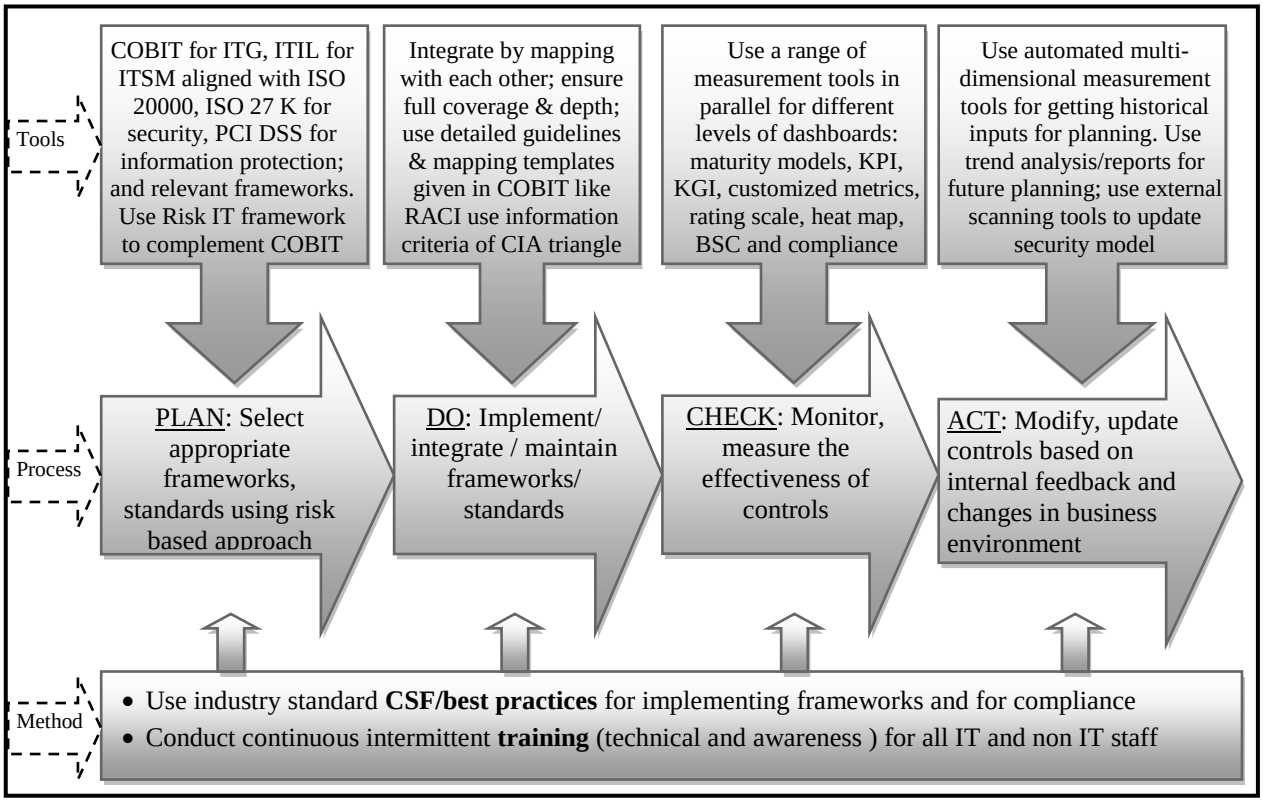

Figure -4 ISSG Implementation Process Model

The central focus of the security model is to manage IS security risk through a risk- based approach. Since the IS security and governance domain includes different frameworks that overlap there are hundreds of controls to choose from that may put undue burden on the organisation in terms of cost, effort and time. Hence, a prioritized systematic approach of choosing controls is preferred (figure – 8), as the objective is to use an optimized set of control

rather than maximum controls, since 100% IS security is an utopian thought. The ISSG model thus rides on:

- ✓ a common set of mandatory controls,
  followed by,
- ✓ a set of heavily overlapped critical controls,
- ✓ a set of partially overlapped industry benchmarked controls,
- ✓ a set of recommended controls and
- ✓ a set of preferred controls.

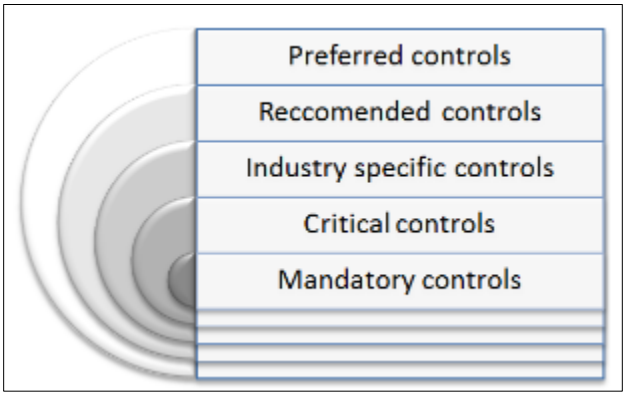

Figure – 5: Prioritized IS Control Implementation

The ISSG process model should initially focus mainly on the mandatory controls for regulatory compliance and then based on the industry and strategic direction, choose to follow other set of controls. Financial sector may choose to follow all the set of controls listed below while organisation in the hospitality sector may choose to follow the mandatory and critical controls only. Since, controls are common across frameworks and levels, these five sets of controls can again overlap with each other presenting a final set of customized controls.

IS security governance is continuous process due to the highly dynamic nature of the information technology sector and the advances made by IS security defense technologies and hackers alike. ISO 27001 reiterates this and incorporates several Plan-Do-Check-Act (PDCA) cycles where the IS controls are regarded as a continuous activity that is reviewed and adjusted to take account of changes in the security threats, vulnerabilities and impacts of information security failures. Thus, the implementation process of ISSG follows the PDCA cycle of Deming where relevant frameworks/standards followed by appropriate controls are selected followed by mapping and prioritizing the selected controls taking into account the overlap. The implementation step takes into account the guidelines provided by the frameworks for implementation and optimal integration.

Measurement being a requirement for effective security governance, COBIT provides a set of tools and techniques for measurement of controls ranging from a simple compliance (complaint and non-complaint), key performance/goal indicators (using quantitative scales), maturity model

and the balance score card (BSC). Other measurements used are the heat map (red-amber-green) and rating scale. A continuous approach of monitoring involves the use of automated tools to record results from measurement on a continual basis to view the trend and take corrective action and an external monitoring tool that provides suggestions on continuous improvement of the ISSG model. The proposed model being conceptual in nature is not without its limitations. Hence, the validation of the model through empirical research (case studies) in different contexts and sectors is required to validate it.

8. Conclusion

Incidents, experiences and technological advances have proved that it is not possible to ensure a 100% secure IS network in an organisation. The practical option is to ensure optimal IS security rather than adequate or maximum IS security. This can be achieved through the use of carefully selecting relevant IS control from all domain of IS, prioritize and integrate them to avoid duplication and implement them as a continuous cyclical process taking into account the dynamic nature of technical advances in IS defense, threat, and the dynamic nature of the organisational external and internal environment. This ensures a holistic perspective of IS security governance through a risk based approach; ensure continuous monitoring through multi measurement tools; and monitor the internal and external trends for continuous improvement of the model. Generalization of this model requires validation through empirical research (case studies) in different sectors of the industry and in different geographical locations.

References

Abu-Musa, A. (2010). Information Security Governance in Saudi Organizations: An Empirical Study. *Information Management & Computer Security*, 18(4), 226-276.

Amsel, P. (2011). Betfair Customer Bank info Hacked Just Months Before Company Went Public [Electronic Version]. Retrieved 12 February from http://calvinayre.com/2011/09/30/business/betfair-customer-bank-info-hacked/.

Arora, A., Hall, D., Piato, C. A., Ramsey, D., & Telang, R. (2004). Measuring the Risk-Based Value of IT Security Solutions. *IT Professional*, *6*(6), 35 - 42.

Bishop, M. (2003). What is Computer Security? *IEEE Security & Privacy* (January/February), 67 - 69.

Cheney, J. S. (2010). *Heartland Payment Systems: Lessons Learned from a Data Breach*. Philadelphia: Payment Cards Center, Federal Reserve Bank of Philadelphia.

Choobineh, J., G. Dhillon, et al. (2007). "Management of Information Security: Challenges and Research Directions." *Communications of the Association for Information Systems* 20(57).

CSI Computer Security Institute. (2011). *CSI Computer Crime and Security Survey 2010/2011*. New York: Computer Security Institute.

Dhillon, G., & Backhouse:, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal*, 11(2), 127-154

Eloff, J. H. P., &Eloff, M. M. (2005). Information Security Architecture. *Computer Fraud & Security*, November, 10-16.

Gaudin, S. (2007). "Security Breach Cost $90 to $ 305 per Lost Record". *Information Week*. Retrieved 12 February from http://www.informationweek.com/news/199000222

Gikas, C. (2010). "A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards." *Information Security Journal: A Global Perspective* 19: 132-141.
Grembergen, W. V., & Haes, S. D. (2009). Enterprise Governance of Information Technology. New York: Springer
Hagen, J. M., Albrechtsen, E., &Hovden, J. (2008). Implementation and Effectiveness of Organizational Information Security Measures. *Information Management & Computer Security*, 16(4), 377 - 397.
Ifinedo, P. (2009). Information Technology Security Management Concerns in Global Financial Services Institutions in National Culture a Differentiator? *Information Management & Computer Security*, 17(5), 372-387.
ISACA. (2009). *The Risk IT Framework*. Illinois: ISACA.
ISO. (2011). ISO/IEC 27002:2005. Retrieved February, 2011, from http://www.iso.org/iso/catalogue_detail?csnumber=50297
ITGI. (2006). *IT Governance Global Status Report - 2006*. Rolling Meadows, Illinois: IT Governance Institute.
ITGI. (2008). *IT Governance Global Status Report.-2008* Rolling Meadows, Illinois: IT Governance Institute.
ITGI. (2011). *Global Status Report on the Governance of Enterprise IT (GEIT)*. Illinois: ISACA & IT Governance Institute.
ITRC Breach Report (2007). *2007 Data Breach Statistics*. San Diego, Identity Theft Resource Centre
ITRC Breach Report (2008). *2008 Data Breach Statistics*. San Diego, Identity Theft Resource Centre
ITRC Breach Report. (2009). *2009 Data Breach Statistics*. San Diego: Identity Theft Resource Centre.
ITRC Breach Report. (2010). *2010 Data Breach Statistics*. San Diego: Identity Theft Resource Centre.
ITRC Breach Report. (2011). *2011 Data Breach Statistics*. San Diego: Identity Theft Resource Centre
Kim, N.-y., Robles, R. J., Sung-Eon, C., Yang-Seon, L., & Tai-hoon, K. (2008). *SOX Act and IT Security Governance* Paper presented at the International Symposium on Ubiquitous Multimedia Computing, Hobart.
Knapp, K. J., Marshall, T. E., Rainer, K., & Morrow, D. (2006). The top Information Security Issues Facing Organisations: What Can Government do to Help? *Information Security and Risk Management* (Sept/Oct).
Laredo, V. G. (2009). PCI DSS Compliance: A Matter of Strategy. *Card Technology Today*.
Liebowitz, M. (2011). 2011 Set to Be Worst Year Ever for Security Breaches. *Security News.* Retrieved 7 July, 2011, from http://www.securitynewsdaily.com/2011-worst-year-ever-security-breaches-0857/
Liu, Q., & Ridley, G. (2005). *IT Control in the Australian Public Sector: A International Comparison.* Paper presented at the Thirteenth European Conference on Information Systems, Regensburg, Germany.
Luftman, J. N., Lewis, P. R., & Oldach, S. H. (1993). Transforming the enterprise: the alignment of business and information technology strategies. *IBM Systems Journal Archive*, 32(1).
Luftman, J., & Brier, T. (1999). Acheiving and Sustaining Business-IT Alignment. *California Management Review*, 1(Fall), 109-122.
Madan, S., & Madan, S. (2010). *Security Standards Perspective to Fortify Web Database Applications from Code Injection Attacks*. Paper presented at the International Conference on Intelligent Systems, Modeling and Simulation, 2010, Liverpool.
Niekerk, J. F. V., & Solms, R. V. (2010). Information Security Culture: A Management Perspective. *Ccomputers & Security 29*, 4 7 6 - 4 8 6.
Ponnemon.Institute. (2011). *The True Cost of Compliance: Benchmark Study of Multinational Organizations*. Michigan.
Posthumusa, S., & Solms, R. v. (2005). IT Oversight: An Important Function of Corporate Governance. *Computer Fraud and Security*, June, 11-17.
Price Water House Coopers, & UK Department of Business Enterprise and Regulatory Forum. (2008). *2008 Information Secuirty Breches Survey*. London.

Rivner, U. (2011). Anatomy of an Attack Retrieved September, 2011, from http://blogs.rsa.com/rivner/anatomy-of-an-attack/

Sahibudin, S., M. Sharifi, et al. (2008). *Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations*. Second Asia International Conference on Modelling& Simulation, Malaysia, IEEE Computer Society.

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. *MIS Quarterly*, 23(2), 261-290.

Schlienger, T., & Teufel, S. (2003). Information Security Culture – From Analysis to Change. *Information Security South Africa*.

Solms, B. v. (2001). Information Security – A Multidimensional Discipline. *Computers & Security*, 20, 504-508.

Straub, D., &Welke, R. (1998). *Coping with Systems Risk: Security Planning Models for Management Decision-Making* :Working paper version. *MIS Quarterly*, 22(4), 441-469.

Sullivan, R. J. (2010, May 21). *The Changing Nature Of U.S. Card Payment Fraud: Issues For Industry And Public Policy*. Paper presented at the Workshop on the Economics of Information Security Harvard University.

Summerfield, B. (2005). EU Selects COBIT as an Auditing Standard [Electronic Version]. *Certification Magazine* from http://www.certmag.com/read.php?in=1196.

Sundt, C. (2006). *Information Security and the Law*. Information Security Technical Report, 11, 2-9.

Symantec. (2011). *Symantec Internet Security Threat Report* [Electronic Version], Vol. 16 from http://www.symantec.com/business/threatreport/.

Tan, W.-G., Cater-Steel, A., & Toleman, M. (2009). Implementing IT Service Management: A Case Study Focussing on Critical Success Factors. *The Journal of Computer Information Systems, 50*(2), 1-12.

Turner, M. J., J. Oltsik, et al. (2009). *"ISO, ITIL, & COBIT Together Foster Optimal Security Investment*." from http://www.thecomplianceauthority.com/iso-itil-a-cobit.php

Veiga, A. D., & Eloff, J. H. P. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*, 29, 1 9 6 - 2 0 7.

Verizon. (2011). *2011 Data Breach Investigations Report (No. MC14949 05/11*): Verizon Business.

Vijayan, J. (2010). Heartland Breach Shows Why Compliance is not Enough [Electronic Version]. *Computerworld*. Retrieved 30 December, 2011 from http://www.computerworld.com/s/article/9143158/Update_Heartland_breach_shows_why_compliance_is_not_enough.

Wagenseil, P. (2011). Citigroup Data Theft So Easy Anyone Could Have Done It [Electronic Version]. *Security News Daily*. Retrieved 28 December 2011 from http://www.securitynewsdaily.com/citigroup-data-theft-so-easy-anyone-could-have-done-it-0874/.