State of Practice of Information Security Management [Pakistan's Perspective] – Assessment and Conclusion

By
Syed Talha Habib
2010-NUST-MS-CCS-11

Supervisor
Dr. Zahid Anwar
Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters in Computer and Communication Security (MS CCS)

In
School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(August, 2014)

Approval

Certified that the contents of thesis document titled "State of practice of Information Security Management [Pakistan's Perspective] – Assessment and Conclusion" submitted by Mr. Syed Talha Habib have been found satisfactory for the requirement of degree.

Advisor: _____

Dr. Zahid Anwar

Committee Member 1: _____

Dr. Adnan Kiyani

Committee Member 2: _____

Mr. M. Ajmal Farooq

Committee Member 3: _____

Mr. Zubair Khan

Abstract

As we are witnessing the emergence of new technologies i.e. Cloud computing, social media and mobile computing new threats and risks are continuously evolving as well. All these threats and risks add to the existing complex environment in organizations. Although budgets have been increased for information security management in organizations, but they continue to fall short as security incidents are on a rise as well. There are many factors which contribute to current information security management practices in organizations.

The intentions of the study are to assess the current posture of InfoSec Management in Pakistan and how it is different from state of practice around the globe. This is the first study of its kind in Pakistan, where a structured survey was conducted between January 2014 and June 2014. A total of 551 respondents from all major sectors participated in this survey. The results depict surprising situation of InfoSec Management in Pakistan.

The main focus of the organizations is toward risk management and implementation of external standard i.e. ISO 27001. Although the budget has been increased, the top priorities, of local organizations for risk mitigation, are inconsistent with global study. As compared to other threats; web defacement, malware and unauthorized access exposed organizations frequently in last 12 months. Financial frauds and attempts to steal financial information (involving credit card numbers) are ranked high as well. The lack of experienced, qualified and certified information security workforce was ranked one of the top challenges for organizations. The capacity building of human resource, especially security awareness is not on the agenda of c-level executives. Alarmingly, 1/3 of the organizations do not assess the effectiveness and efficiency of their information security functions. In most cases, the controls against risks of emerging technologies like cloud computing, social media and mobile computing are either inadequate or absent.

Only a handful respondent from local organizations ranked their processes as mature.

Certificate of Originality

I hereby declare that this submission titled **State of Practice of Information Security Management [Pakistan's Perspective] – Assessment and Conclusion** is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's de sign and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: Syed Talha Habib

Signature: _____

Acknowledgment

First and foremost, I would like to thank ALLAH ALMIGHTY for giving me courage and motivation during the thesis to cater all the difficulties and problems in amicable manner. This motivation helps me to perform tasks with hard work and full dedication and devotion.

I offer sincere gratitude to my supervisor Dr. Zahid Anwar who has put his great effort throughout the thesis phase with his knowledge, expertise and valuable suggestions. He has provided full support, mentorship and continuous assistance that enable me to learn new concepts of related domain and develop an understanding of how to perform research. I wish to thank my committee members Dr. Adnan Kiyani, Mr. M. Ajmal Farooq and Mr. Zubair Khan for their kind support, availability and useful ideas that help me to refine the research work.

I am very blessed to have my wife with me whose great company adds significant contribution to my life and education. I would specially acknowledge my parents for their prayers, patience and support without which I could not be able to achieve all this.

In the end, I thanks to all my friends and everyone who supported me in any manner for the completion of my thesis.

Syed Talha Habib

To my wife who has provided me every possible support to make this dream come true and Abu and Ammi Jaan that has always been a source of inspiration for me.

Table of Contents

Chapter 1 1
Chapter 2 4
Chapter 3 6
Chapter 4 15
Bibliography 17
Annex - A 22

List of Figures

Figure 1: Industry Distribution 5
Figure 2: Motivation for implementing information Security in the organization? [Pakistan's Perspective] 7
Figure 3: "Top Priorities" over the coming 12 months 10
Figure 4: Control against risks of emerging technologies [Pakistan's Perspective] 12
Figure 5: Budget Spending (Top 5 areas) over the next year [Pakistan's Perspective] 13
Figure 6: Maturity of information security management processes 16

Chapter 1

Introduction

The growth of Information Technology in Pakistan is impressive. In year 2012 – 2013, IT projects of Rs. 4.6 billion have been conceived by the Government of Pakistan while 46 IT projects of worth Rs. 22.9 billion are being executed. The core focus of IT projects is to improve current IT infrastructure, enhance human resource in IT and move toward e-government (Express Tribune, 2012).

Many mega projects have been planned in Pakistan and some are expected to close in the next few years (APP, 2013). Many projects have been conceived at the provincial level as well i.e. IT Kiosks, land record automation, paperless environment (K, 2012). Recent technological advancement has been witnessed in Pakistan's first Hydroelectric Project (Khan, 2013). Despite unfavorable environments, there is a growth of 20% in e-tailing and eCommerce furthermore e-banking transactions have reached nearly Rs. 8 Trillion (Attaa, Aamir, 2013), (Khan, 2013). There is growing recognition of usage of ICTs in Health. There is interest from the corporate sector and public sector in e-Health (Qureshi, et al., 2012).

According to (World Economic Forum, 2013), in terms of Information Technology, Pakistan is placed at 105th position out of 144 which indicates that IT sector can grow further. If we look into details, usage of IT is highest among business i.e. Position 99/144 while IT is affordable to the common consumer as well i.e. in affordability at 22/144.

Some sectors of Pakistan i.e. Telecommunications, Banking and Finance, Multinationals etc. have been driving force for IT growth in

Pakistan (PSEB, 2010). With fundamental policies in place, all relevant sectors can tap into growth opportunities for sustainability and economic development in Pakistan (Masood, et al., 2008).

Cloud computing empowers businesses with flexibility to become more strategy focused and cloud computing is one of the main driver for innovation and service delivery. Universities like LUMS, NUST, FAST has whole heartedly adopted cloud computing for their LMS systems. Mobile devices are much more powerful now and play a vital role in communication and considered must have tool for both office and personal use. In April 2014, Mobile subscriber jumped to approximately 137 million in Pakistan. The area of cell phone coverage has been increased to cover approximately 90 percent of Pakistanis. The highest mobile penetration rate has been recorded in Pakistan in the South Asian region. The mobile devices poses a severe threat to the organization's security as well.

As new technology becomes part of operational plans, advanced and fairly new risks emerge to disrupt the flow of operations in organizations. In recent years, Pakistan's IT industry witnessed increasing number of social media scams, SMS scams, blackmailing etc. Cyber criminals are very active in cyberspace and cyber crimes are on a rise with alarming pace (Hassan, 2012). More than 5 websites of Pakistani Banks were hacked in 2013 and many other consumer websites, i.e. NADRA e-Sahulat, PTCL etc. were also hacked (Attaa, Aamir, 2013) (Attaa, Aamir, 2013) (Attaa, Aamir, 2013). After recent attacks on IT infrastructure of business and industry, efforts are being made by government to promulgate laws for cyber security and cyber crimes (APP, 2013), (Attaa, Aamir, 2013).

In absence of Information Security, organizations may witness the detrimental impact on reputation, productivity, stakeholder value, IPR as well as financial (Humphreys, 2006) . There is a requisite need to explore motives, challenges and impact of information security management in Pakistani organizations.

Currently, there is no study available on the current posture of Information security management and how it is different with state for practice (globally) which makes it difficult for senior management and vendors to focus on the right segments, thus there is a requisite need to explore the state of practice of Information Security Management in Pakistan's perspective.

Chapter 2

Methodology

For this study referred as "local study", a structured survey is conducted between January and June 2014. The survey was automated using a Google form, and only complete submissions were accepted. There were eight (8) main questions in this survey, which covered major areas of information security management. 551 respondents from all major sectors of Pakistan participated. Our target population comprised of CIOs, CISOs, CTOs and information security executives/analyst while target sectors consisted of Banking, Telecommunications, Technology Services, Manufacturing, Government and public sector, Health Care, Power and utilities, Oil and gas, Education Sector, Media and Entertainment (figure 1). The results of local survey were compared with EY's Global Information Security Survey 2013 referred as "global study" to assess the difference between local and global posture of information security management. All figures were extracted from the survey, otherwise noted.

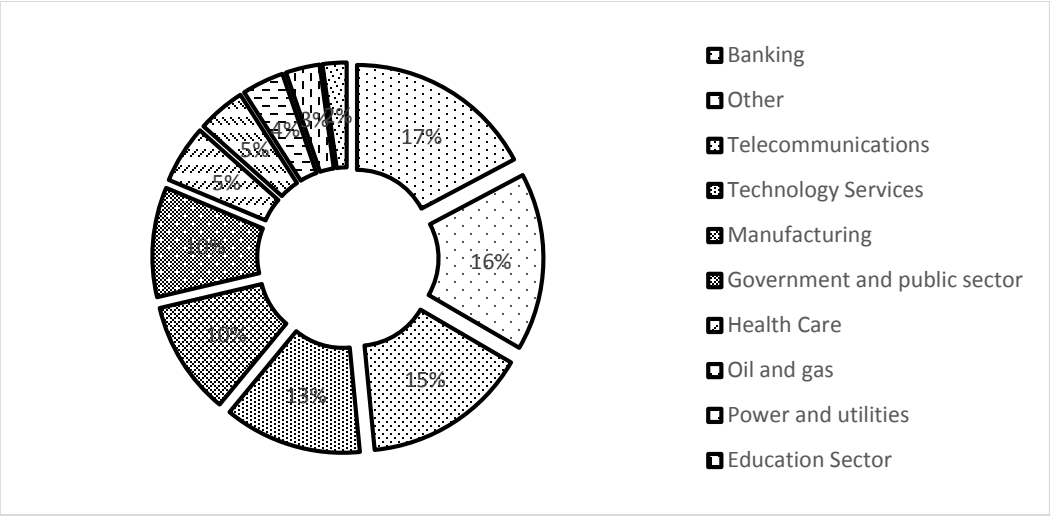


Figure 1: Industry Distribution

Chapter 3

Discussion

A decade ago, remote access was the single most important factor for information security investments. After initial era of malware where viruses and worms have been a major actor, compliance became a major factor for security implementations in the organizations thus information security function became compliance driven as well. In general, the security management function is considered an essential fragment of organizations, but the drivers of security initiative may vary from organization to organization. Bringing improvement in the security posture of organization and competitive advantage proved to be common motivation for implementation (Abusaad et al, 2011) but legislations and industry requirements also play major role. Such requirements and legislations can prove itself counterproductive if compliance is done just for the sake of compliance with these requirements (Mataracioglu et al, 2011).

In local perspective, "Business Requirement / Need" and "Data Protection" are biggest motivation to implement information security within organizations (about 76% of respondents each). This is particularly good to see that business need and data protection are prime reasons for all information security initiatives in the organizations. Very few respondents (about 21%) claimed that competitive edge is also a motivation for security implementations. Legislations play a minor role because national cyber security policy and/or frameworks are not available, but still more than half respondents ranked "Legal, business and contractual requirement" as one of top influence. Despite of its importance, information security is still a new entrant in local market so professionals are adopting best practices in their respective industries thus making us aligned global

practices. The top 3 motivations for information security management are same, if we compare global practice and local's perspective, but inverse in trend though (figure 2).

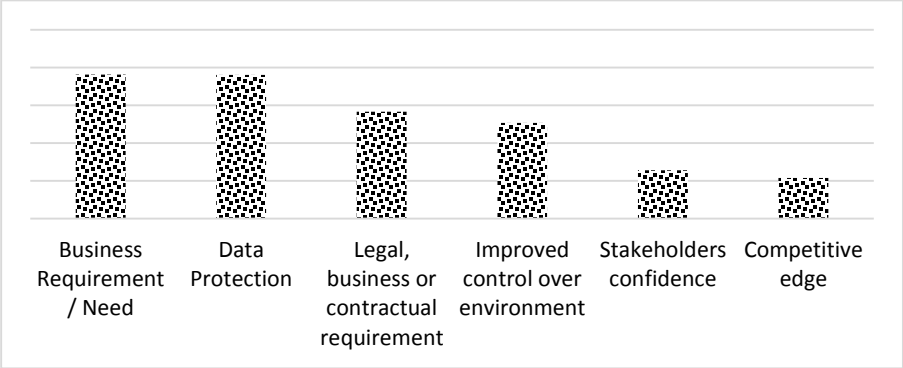
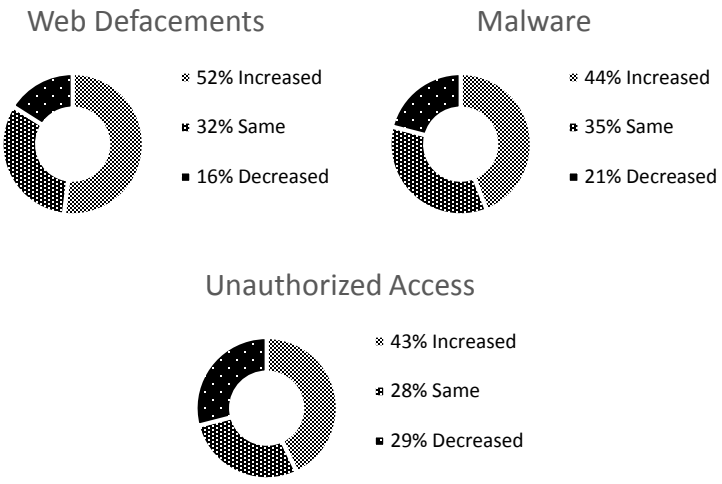


Figure 2: Motivation for implementing information Security in the organization? [Pakistan's Perspective]

Information Security plays an important role today as information systems are being used extensively within organizations. The risk has been greater now as more and more user have access to powerful handheld devices and social media. As reliance on technology has been increased, the hackers are particularly targeting organizations for different motives. The amplification of cybercrimes can be witnessed (Hassan, 2012). Due to nonexistence of cybercrime laws in Pakistan, the organizations have become playground for hackers. In the last year, the websites of most of financial institutes has been defaced and many other local internet services for consumers were hacked as well (Attaa, Aamir, 2013).

The risk of "Web defacements", "Malware" and "Unauthorized access" is considered to be increased significantly. Phishing incidents have increased as 37% of respondents faced phishing incidents over the past 12 months and that is considered as the major threat to information security and same is the case with malware including Trojans and viruses. In recent years, there has been a lot of awareness about social media globally so 58% of respondents of global study felt that risks related to social media websites has been decreasing significantly

while it is opposite in organization of Pakistan. The financial frauds are on an upsurge as 56% of respondents highlighted it. The risk of espionage has been decreased in last year as 44% of respondents have not been affected by espionage.



After a rapid change in the information security canvas the organizations are now realizing the importance and coping up with the changing priorities. Information Security is taken as a vital lifeline for the organization's success and progress. Today, security operations such as intrusion detection systems (IDS), antivirus encryption, etc. are mature in a majority of organizations. Data protection has moved ahead from just a contractual line in a service level agreement. Organizations have withdrawn their assumptions that everyone is taking care of information security.

Talking about priorities, the implementation of information security standards (about 68%) and recruitment of qualified human resources (approx. 66%) has been named as one of top priorities. In Pakistan, organizations are focusing to improve "security operations" and to have greater assurance of security operations through alignment with international best practices available as standards. There are many advantages of implementing ISMS based on external standards, but

there exists some pitfalls as well. The implementation of security standard takes a lot of efforts so it is advisable to have keen eye on benefits. In (Neubauer et al, 2011), a phased approach for implementation of security controls is required while having maximum visibility with compliance and benefits by senior management. Authors, in (Sevgi Ozkan, 2010), suggest that organizations should have limited scope initially and it should be increased gradually as original route of ISMS implementation based on external standards can be very challenging.

External security standards provide the requirements and organizations use those requirements as guidelines to implement Information Security Management System (ISMS) but the implementation does not guarantee the effectiveness of the ISMS (Boehmer, 2009). There are many reasons of low adoption of external security standards such as ISO 27001 in Pakistan and even globally. One important factor is involvement of substantial resources i.e. money, time, human resource etc. Another important issue is "enormous" amount of paperwork and documentation. Lack of publications in this area also contributes to low adoption of external standards (Fomin et al, 2008). Furthermore, these standards can also provide independent assessment for the effectiveness of information security function. In Korea, the authors identified common defects i.e. assets management, incident response, access control etc. in ISMS which can be used as reference for new implementations and improvements in existing ISMS (Kwon, et al., 2007).

If we look at statistics, careless employees were one major source of security incidents. Security awareness is important countermeasure for early detection and effective reduction in incidents at first place. Interestingly, only few of respondents ranked security awareness and training as their top priority. In Pakistan, importance is not given to capacity building and awareness trainings at every level. Inadequate awareness has been witnessed among senior management and security budgets are usually allocated after major security lapse. A similar

trend has been witnessed in Norwegian organizations where awareness trainings were not given importance. It was found that some controls are practiced frequently i.e. security policies etc. while some controls i.e. awareness trainings etc. are practiced less commonly. These practices were contrary to proven effectiveness of controls (Hagen et al, 2008). This reactive approach is being followed by organizations in Slovenia to manage information security and insufficient awareness among senior management is the prime reason for such approach (Bernik, et al., 2013). The lack of awareness can be catered with simple technique. In Oulu, Finland, the lack of awareness was overcome with extensive communication, advocacy and management support (Wiander, 2008).

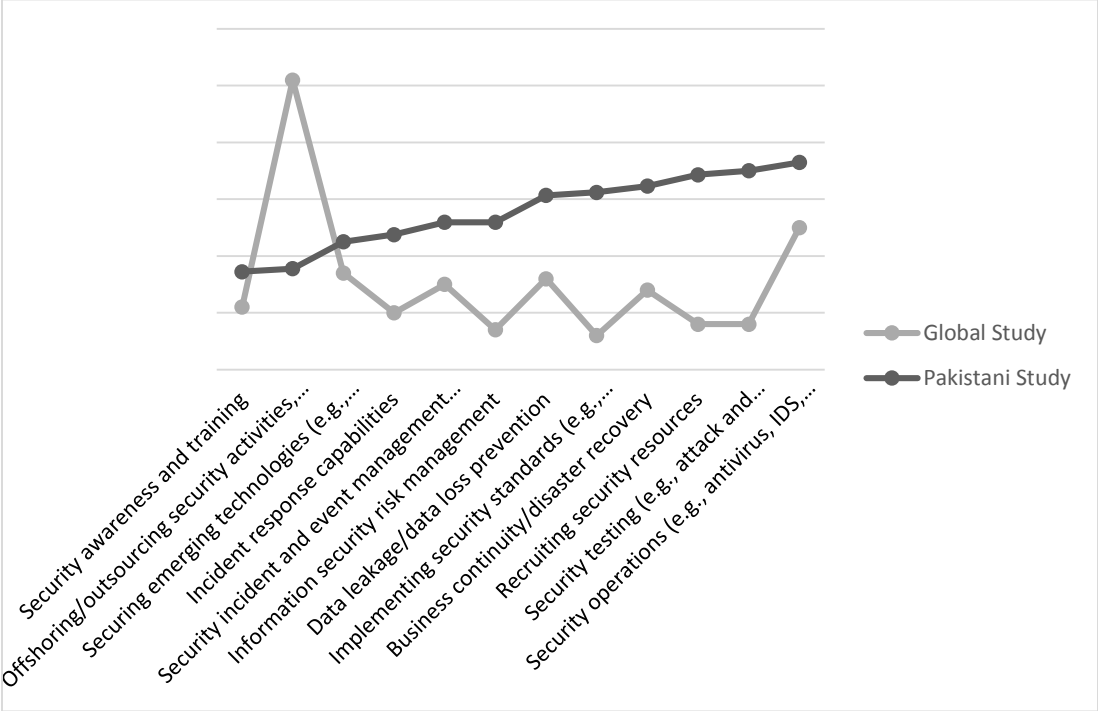


Figure 3: "Top Priorities" over the coming 12 months

Despite of the efforts that organizations have made over the years to improve their information security structure, there is still a lot of improvements to be made. The organizations are focusing extensively while leaving "Security Governance and Management" which is an

important aspect in strategically aligning business objective with security initiatives however it is not among the top priorities. Another area where risks are downplayed is "Vendor / 3rd Party Outsourcing". Most of respondents of local study ranked "Outsourcing Security Activities including 3rd party risk" among the least priority of organization (figure 3). On contrary, special attentions are given to risks of 3rd Party outsourcing as reported by respondents of global study. The focus of global organizations have been shifted from "recruiting security resource" and "Implementing security standards" to other important issues which is contradictory to situation in Pakistan.

As organizations grow through innovation, adoption of emerging technologies and coping with change. Where new technology nurtures growth, it also changes threat or risk profile of an organization. Social media, for example, opened up incredible business opportunities for organizations, but also exposed them to new risks. The information security function must pay close attention to the associated risk of emerging technology.

The risks of new technologies are yet to comprehend by local organizations. The majority of organizations have limited control over risks related to cloud computing, social media and mobile computing. Top choice is to limit or even revoke access / usage while many of the organizations adjusted their policies and procedures. In local study around 42% respondents believed that they have limited / no access to cloud computing, social media and mobile computing. In many organizations (around 41%), the policy has been adjusted to accommodate technological adoption while approximately 40% of respondents claimed that they have done nothing (figure 4). The global study shows that there is an emphasis on "Security Awareness Programs (40%)" and "Encryption (40%)". Currently, when mature solutions are not available yet, adjustment in policies and effective awareness programs can reduce risk to acceptable level but there is a narrow understanding of information security management and how

information security policies are applied. Usually security policies are drafted and implemented without aligning it to international standards or best practices which can be overcome by adopting a formal methodology (Ebru Yeniman Yildirima, 2011).

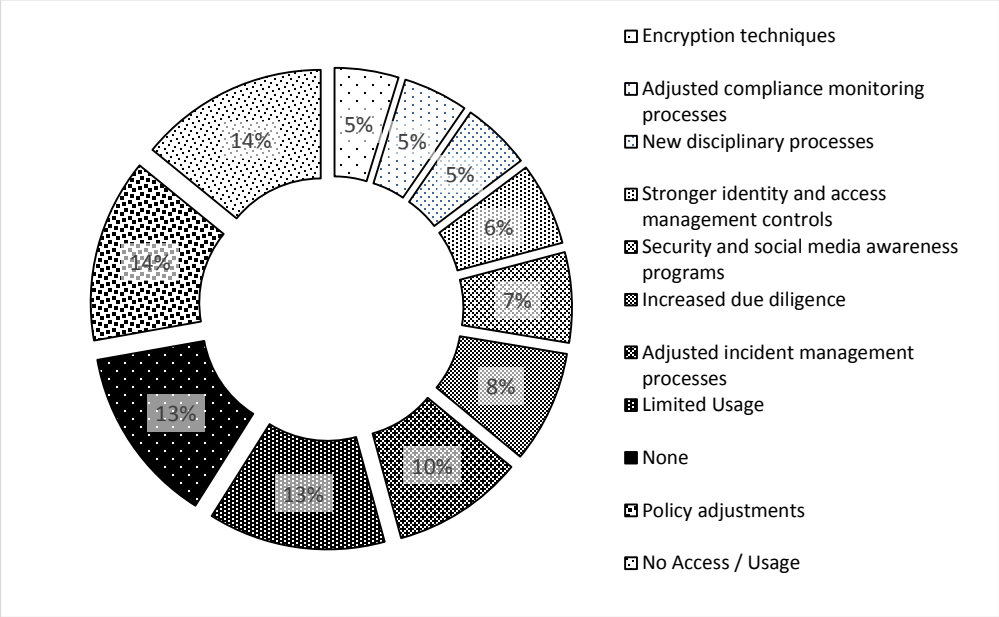


Figure 4: Control against risks of emerging technologies [Pakistan's Perspective]

Where local organizations are willing to spend their budget in next year? According to results of local study, the organizations would spend more on information security risk management (about 45%) and there would be more outlay on implementation of security standard (around 43%). From figure 4, we can deduct that our organizations are still taking foundational steps in securing themselves and a lot has to be done. Information Security Risk Management (ISRM) must not be an ad-hoc function in the organizations. Without understanding of risk management, risk cannot be mitigated, transferred or accepted so budget expansion in this area completely makes sense. To adopt a formalized approach to ISRM, organizations are moving ahead to implement security standards as well. In India, implementation of external security standards has impacted organization in a positive way (Singh et al, 2007). The security standards can provide a

systematic approach to manage risk and perform continuous improvement.

With evolving threats and risk, the budget for the information security function is available but is it enough? Despite of the fact that the budget has been increased, 76% of respondents still believe that insufficient budget is a pain point. The lack of support from senior management follows it with around 56%. A study shows that all information security initiatives lose worth if it lacks management buy-in and support. The information Security initiative must be top down and driven by senior management (Broderick, 2006). It is common practice to assume that security management responsibility of IT or security department. Around half of respondents claimed that people with right skill and training are really hard to find in Pakistan. According to another study, lack of experienced workforce and complexity of environment were major obstacles in information security management (Abusaad et al, 2011) in Saudi Arabia as well.

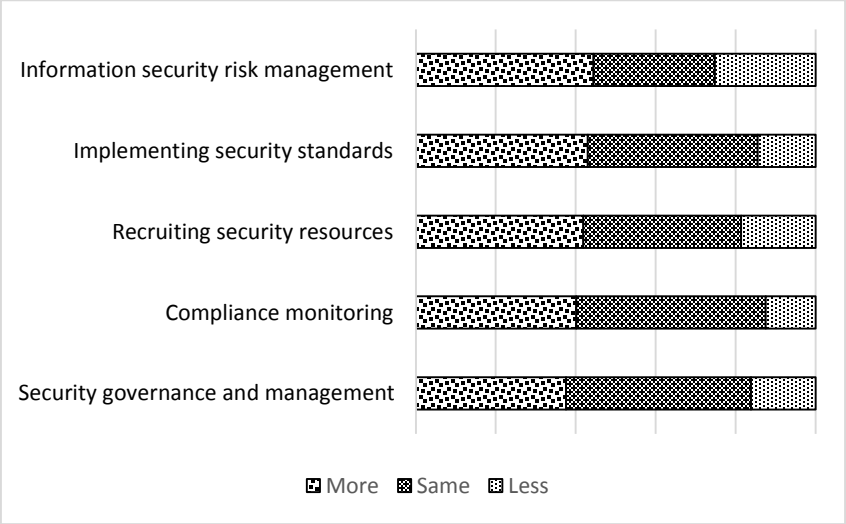


Figure 5: Budget Spending (Top 5 areas) over the next year [Pakistan's Perspective]

There can be multiple ways and means to monitor information security management function in an organization. The external assessment are trusted by management as it is done by completely independent firms

and usually linked with external certification authorities. Key Performance Indicators (KPI) can be used to measure effectiveness and efficiency of ISMS within an organization. In local organizations, the operational performance of security department (56% of respondents) is measured to gauge effectiveness information security program furthermore 55% of respondents stated that IT department self-evaluates its performance. Alarmingly, more than 38% respondents claim that they do not evaluate the performance of information security in their organizations or there is no mechanism of evaluation and testing.

Locally, in comparison with other sectors, more respondents from banking and telecom industry ranked their information security management "developed" or "mature". Banking and Telecom industry is ahead of rest of sectors due to their relatively higher dependency on information systems. In Saudi Arabia, banking sector was also more proactive in security management (Nabi et al, 2010) than rest of sectors. The information security processes have been developed in many local organizations while ad hoc practices are also prevailing. Even if organizations have technology (encryption, IPS, firewall etc.) available, organizations still need qualified people and processes i.e. configuration management, patch management, vulnerability management etc. Alarmingly, in many organization, some processes are still nonexistent and local organizations are lagging behind in term of maturity of processes. In comparison with the global study, only a handful of respondents from local organizations ranked their processes as mature.

Chapter 4

Conclusion

According to study, following can be determined:

- Keeping in view that the organizations are facing new challenges every day, it is a good sign that information security management is driven because of business requirement and data protection needs.
- The main focus of organizations is toward risk management and implementation of external standard i.e. ISO 27001. There is inconsistency between global trend and priorities of local organizations. The respondents from most of the organizations are satisfied with current security implementation and design while very few organizations are transforming fundamental information security design.
- The organizations are currently looking to have trained and certified security professionals. Although, organizations have allocated more budget to recruit and retain human resource in this domain.
- There is a lot of ground to be covered for security awareness and communication. The Security awareness is still not a priority of c-level executives. One prime reason for this shortcoming is again lack of awareness at higher level.
- Despite of the fact that financial frauds and attempts to steal financial information (involving credit card numbers) are ranked high, interestingly, the organizations are not opting to spend on forensic/fraud support with only 20% organizations interested to look into that sector.
- There are multiple methods to evaluate the efficiency and effectiveness of information security management. Alarmingly,

around 1/3 of organizations do not assess effectiveness and efficiency of their information security function.

- It is particularly difficult to have ample resources when information security function is considered a cost centric function. With current budget and support of senior management, it is felt that they have developed their information security management processes but they are not yet mature.

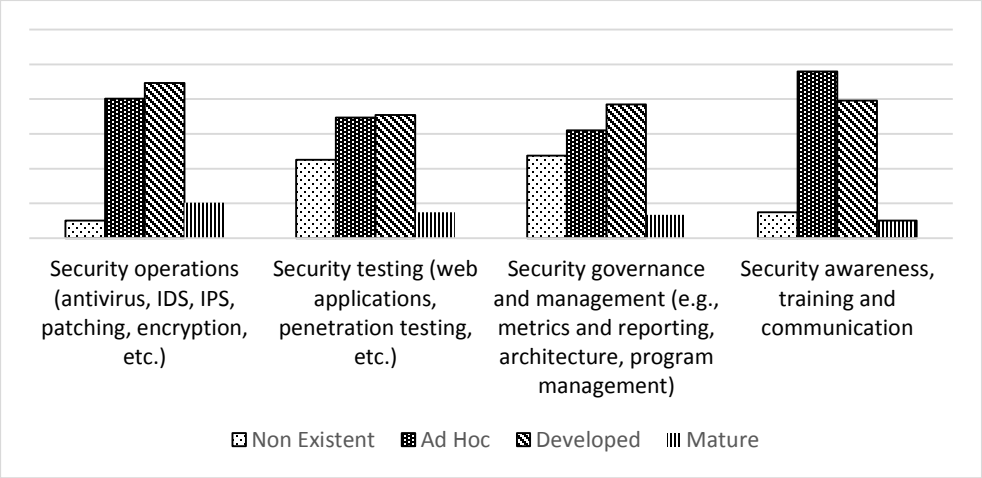


Figure 6: Maturity of information security management processes

Bibliography

Abusaad et al. 2011. Implementation of ISO 27001 in Saudi Arabia– Obstacles, Motivations, Outcomes, And Lessons Learned. 2011.

APP. 2013. Senate committee proposes 7-point Action Plan for Cyber Secure Pakistan. *propakistani.pk.* [Online] 2013. [Cited: November 27, 2013.] http://dawn.com/news/1023706/senate-committee-proposes-7-point-action-plan-for-cyber-secure-pakistan.

APP. 2013. The Nation. *nation.com.pk.* [Online] November 20, 2013. [Cited: December 17, 2013.] http://www.nation.com.pk/business/20-Nov-2013/new-islamabad-airport-to-be-operative-by-2015.

Attaa, Aamir. 2013. Despite Tough Conditions, Ecommerce Businesses in Pakistan is on the Rise. *propakistani.pk.* [Online] April 22, 2013. [Cited: December 17, 2013.] http://propakistani.pk/2013/04/22/despite-tough-conditions-ecommerce-businesses-in-pakistan-is-on-the-rise/.

Attaa, Aamir. 2013. MCB Targeted by Hackers, Becomes Third Defaced Bank in One Week! *ProPakistani.pk.* [Online] July 19, 2013. [Cited: December 17, 2013.] http://propakistani.pk/2013/07/19/mcb-targeted-by-hackers-becomes-third-defaced-bank-in-one-week/.

Attaa, Aamir. 2013. Official Website of NADRA E-Sahulat Gets Hacked, User Data Compromised. *Propakistani.pk.* [Online] 2013, September 16, 2013. [Cited: 12 17, 2013.] http://propakistani.pk/2013/09/16/official-website-of-nadra-e-sahulat-gets-hacked-user-data-compromised/.

Attaa, Aamir. 2013. Pakistan is Finally Preparing to Formulate Cyber Laws in the Country. *Propakistani.pk.* [Online] 2013. [Cited: November 27, 2013.] http://propakistani.pk/2013/11/27/pakistan-finally-preparing-formulate-cyber-laws-country/.

Attaa, Aamir. 2013. PTCL Gets Hacked, Again! [Updated]. *Propakistani.pk.* [Online] Jan 3, 2013. [Cited: December 17, 2013.] http://propakistani.pk/2013/01/03/ptcl-gets-hacked-again/.

Azam, Madeeha. 2011. Cyber Security Regime in Pakistan: Still a lot to be done. *Propakistani.pk.* [Online] 2011. [Cited: November 27, 2013.] http://propakistani.pk/2011/01/17/cyber-security-regime-in-pakistan-still-a-lot-to-be-done/.

Baloch, Farooq. 2012. Tough consensus: As stakeholders guard interests, cyber crime bill faces delay. *Tribune.com.pk.* [Online] November 20, 2012. [Cited: December 17, 2013.] http://tribune.com.pk/story/468063/cybercrime-fia-software-company-at-odds-over-peco-redraft/.

Bernik, I and Prislan, K. 2013. Information Security in Risk Management Systems: Slovenian Perspective. *Journal of Criminal Justice and Security.* 2013, 2 (208-221).

Boehmer, Wolfgang. 2009. Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001. *SECURWARE 2008: 224-231.* 2009.

Broderick, J. Stuart. 2006. *ISMS, security standards and security regulations .* s.l. : Information Security Tech. Report 11(1): 26-31, 2006.

Ebru Yeniman Yildirima, Gizem Akalpa, Serpil Aytacb, Nuran Bayramb. 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management.* 2011, Vol. 31, 4.

Fomin et al. 2008. ISO/IEC 27001 Information Systems Security Management Standard: Exploring The Reasons For Low Adoption. 2008.

World Economic Forum. 2013. Global Information Technology Report 2013. [Online] World Economic Forum, 2013. [Cited: November 27,

2013.] http://www.weforum.org/reports/global-information-technology-report-2013.

Express Tribune. 2012. Govt. to Spend Rs.4.6b on IT Projects. *Express Tribune.* [Online] 2012. [Cited: November 28, 2013.] http://tribune.com.pk/story/432124/govt-to-spend-rs4.6b-on-it-projects/.

Hagen et al. 2008. Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security.* 2008, Vol. 16, 4 (377 – 397).

Hashmi, Rehan. 2010. It's no holds barred in cyber space. *tribune.com.pk.* [Online] 2010. [Cited: November 27, 2013.] http://tribune.com.pk/story/60352/its-no-holds-barred-in-cyber-space/.

Hassan, Raza. 2012. Alarming rise in cyber crimes. *Dawn.com.* [Online] 2012. [Cited: November 27, 2013.] http://dawn.com/news/738306/alarming-rise-in-cyber-crimes/.

Humphreys, T. 2006. State-of-the-art information security management system with ISO/IEC 27001:2005. *ISO Management Systems.* 2006.

K, Fahim. 2012. AJK Government Steps Toward IT Revolution. *propakistani.* [Online] June 14, 2012. http://propakistani.pk/2012/06/14/ajk-government-steps-toward-it-revolution/.

Khan, Mehwish. 2013. E-Banking Transactions Reach Rs. 7.9 Trillion in Pakistan. *Propakistani.pk.* [Online] May 31, 2013. [Cited: December 17, 2013.] http://propakistani.pk/2013/05/31/e-banking-transactions-reach-rs-7-9-trillion-in-pakistan-sbp/.

Atta, Aamir. 2013. IBM Empowers Pakistan's first Hydroelectric Project. *Propakistani.pk.* [Online] April 25, 2013. [Cited: December 17, 2013.] http://propakistani.pk/2013/04/25/ibm-empowers-pakistans-first-hydroelectric-project/.

Kwon, Sungho, et al. 2007. Common defects in information security management system of Korean companies. *Journal of Systems and Software.* 2007, Vol. 80, 10.

Masood, Jamshed and Malik, Salman. 2008. *Digital Review of Asia Pacific 2007/2008.* s.l. : Sage Publications. p. 264., 2008.

Mataracioglu et al. 2011. Analysis of the User Acceptance for Implementing ISO/IEC 27001:2005 in Turkish Public Organizations. *International Journal of Managing Information Technology (IJMIT).* 2011, Vol. 3, 1 (1-14).

Nabi et al. 2010. Information Assurance in Saudi Organizations– An Empirical Study. *Springer.* 2010, (18 - 28).

Neubauer et al. 2011. Interactive Selection of ISO 27001 Controls under Multiple Objectives. *IFIP Advances in Information and Communication Technology (AICT) 477-492.* 2011.

PSEB. 2010. *IT Market Assessment Report 2010.* 2010. 62 - 72.

Qureshi, Qamar Afaq, Ahmad, Iftikhar and Nawaz, Allah. 2012. Readiness for eHealth in the Developing countries like Pakistan. *Gomal Journal of Medical Sciences.* 2012, Vol. 10, 1.

Rhee, Hyeun-Suk, Ryu, Young U. and Kim, Cheong-Tag. 2012. Unrealistic optimism on information security management. *Computer and Security, Elsevier.* 2012, Vol. 31, 2.

Sevgi Ozkan, Bilge Karabacak. 2010. Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management.* 2010, Vol. 30, 6.

Singh et al. 2007. The Impact of ISO Implementation on Output Parameters in SME's in India. 2007.

Wiander, T. 2008. Implementing the ISO/IEC 17799 standard in practice: experiences on audit phases. *Proceedings of the sixth Australasian conference on Information security.* 2008, Vols. 81 (pp. 115-119).

Yildirima, Ebru Yeniman, et al. 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management.* 2011, Vol. 31, 4.

Zeeshan, Omair. 2011. Investigators suffering from absence of law. *Tribune.com.pk.* [Online] 3 24, 2011. [Cited: December 17, 2013.] http://tribune.com.pk/story/136794/investigators-suffering-from-absence-of-law/.

Annex - A

Questionnaire

Question # 1: What is motivation for implementing information security in your organization? (Check that applies)

- Legal, business or contractual requirement
- Business requirement
- Competitive edge
- Improved control over environment
- Stakeholders confidence
- Data Protection
- Others

Question # 2: Which of the following information security areas are defined as "Top Priorities" over the coming 12 months? (1st – 5th)

- Business continuity/disaster recovery
- Cyber risks/cyber threats
- Data leakage/data loss prevention
- Information security transformation (fundamental redesign)
- Compliance monitoring
- Implementing security standards (e.g., ISO/IEC 27002:2005)
- Identity and access management
- Security governance and management (e.g., metrics and reporting, architecture, program management)
- Information security risk management
- Privacy
- Securing emerging technologies (e.g., cloud computing, virtualization, mobile computing)
- Security operations (e.g., antivirus, IDS, IPS, patching, encryption)
- Recruiting security resources
- Offshoring/outsourcing security activities, including third-party supplier risk
- Secure development processes (e.g., secure coding, QA process)
- Security incident and event management (SIEM)
- Forensics/fraud support
- Security awareness and training

- Threat and vulnerability management (e.g., security analytics, threat intelligence)
- Incident response capabilities
- Security testing (e.g., attack and penetration)

Question # 3: Based on actual incidents, these threats and vulnerabilities have most changed respondents' risk exposure over the last 12 months. (Increase – Same – Decrease)

- Vulnerabilities related to mobile computing use
- Vulnerabilities related to social media use
- Vulnerabilities related to cloud computing use
- Careless or unaware employees
- Unauthorized access (e.g., due to location of data)
- Phishing
- Malware (e.g., viruses, worms and Trojan horses)
- Spam
- Web Defacements
- Fraud
- Cyberattacks to steal financial information (credit card numbers, bank information, etc.)
- Cyberattacks to steal intellectual property or data
- Natural disasters (storms, flooding, etc.)
- Internal attacks (e.g., by disgruntled employees)
- Espionage (e.g., by competitors)

Question # 4: Which of the following controls have you implemented to mitigate the new or increased risks related to social media, cloud and mobile computing?

- Encryption techniques
- Increased due diligence
- Stronger identity and access management controls
- Adjusted compliance monitoring processes
- Adjusted incident management processes
- Limited Usage
- No Access / Usage
- Policy adjustments
- Security and social media awareness programs
- New disciplinary processes
- None

Question # 5: Compared to the previous year, does your organization plan to spend more, spend relatively the same amount or spend less over the next year for the following activities? (More – Same – Less)

- Securing new technologies
- Business continuity/disaster recovery
- Data leakage/data loss prevention technologies and processes
- Identity and access management technologies and processes
- Security awareness and training
- Information security risk management
- Security testing
- Security operations
- Security governance and management
- Threat and vulnerability management technologies and processes
- Compliance monitoring
- Security incident and event management
- Implementing security standards
- Incident response capabilities
- Information security transformation
- Secure development processes
- Privacy
- Recruiting security resources
- Forensics/fraud support
- Offshoring/outsourcing security activities

Question # 6: What are main challenges / obstacles to improving information security?

- Lack of an actionable vision or understanding of how future business needs impact information security
- Lack of an effective information security strategy
- Insufficient budget
- Absence or shortage of in-house technical expertise
- Poorly integrated or overly complex information and IT systems
- Lack of experienced and qualified information security workforce
- Lack of understanding of Industry standards
- Resists change
- Cultural Issue e.g. openness etc.
- Lack of Involvement of Higher Management

- Lots of documentation
- Lack of publications [scholarly articles]

Question # 7: How does your organization assess the efficiency and effectiveness of information security?

- Assessments performed by internal audit function
- Internal self-assessments by IT or information security function
- Assessment by external party
- Monitoring and evaluation of security incidents and events
- In conjunction with the external financial statement audit
- Benchmarking against peers/competition
- Evaluation of information security operational performance
- Formal Certification to external security standard e.g. ISO 27001:2005
- Formal Certification to industry security standard e.g., PCI DSS, HIPPA
- Evaluation of information security costs
- Evaluation of return of investment Performance
- No assessments performed

Question # 8: Maturity of information security management processes in surveyed organizations (Mature – Non Existent)

- Security operations (antivirus, IDS, IPS, patching, encryption, etc.)
- Security testing (web applications, penetration testing, etc.)
- Security awareness, training and communication
- Security governance and management (e.g., metrics and reporting, architecture, program management)

Question # 9: What is your industry / sector?

- Banking
- Telecommunications
- Technology Services
- Manufacturing
- Government and public sector
- Health Care
- Oil and gas
- Power and utilities
- Education Sector
- Media and Entertainment
- Other