Journal of Theoretical and Applied Information Technology
10th July 2014. Vol. 65 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CYBERCRIME PREVENTION IN THE KINGDOM OF BAHRAIN VIA IT SECURITY AUDIT PLANS

[1]AMNA ALMADHOOB, [2]RAUL VALVERDE
[1] AMEX Middle East, Bahrain
[2]Department of Supply Chain and Business Technology Management, Concordia, Montreal, Canada
E-mail: rvalverde@jmsb.concordia.ca

ABSTRACT

Implementing cybercrime preventing technologies is critical in today's connected world. As companies continue to rely on critical infrastructure, they should also address the risk and threats imposed by the use of these technologies. Bahrain is no different from anywhere else in the world when comes to cybercrimes, however, due to the lack of regulations and laws for the cyber world, small and medium companies were left to navigate their way through the cyber world. To understand how to assist small and medium organizations and the Bahrain cyber risk levels, a survey was designed to solicit Bahraini organization feedback with regards to four cybercrimes (Denial of services, web hacking and defacement, malware, spam and phishing). An audit plan was designed based on a set of proposed critical control objectives. The critical objectives ensure that organizations are well aware about their assets and the risks they are exposed to , build a solid boundary defence, secure configurations and applications, continues to monitor the environment and close any vulnerabilities and most importantly; to be vigilant and prepared to handle and respond to cyber incidents. The audit plan was tested with the help of a case study located in Bahrain and its use to prevent cyber attacks demonstrated in this research.

Keywords: *Cybercrime, IT Audits, Risk Management, Audit plans, Cyber Attack Prevention, Financial Systems*

1. INTRODUCTION

2011, was an eventful year in Middle East and the kingdom of Bahrain in particular, Middle East witnessed increased levels of cybercrimes correlated with the Arabs uprising or what is now known as the Arab Spring. Hactivism groups targeted business, governments and Bahraini citizens. Many government web sites were targeted and defaced including the sites of the Ministry of Housing and Bahrain News Agency.

In Bahrain, there are no specific cyber laws nor computer incident response teams to guide small and medium enterprises to reduce risks of cyber-attacks; Technologies departments and IT professionals could need the use of a customized risk based plan to implement controls that to defence against these forms of crimes[1]. This research aims to conduct an investigative analysis into the design of a risk based IT Security audit plan to assist small and medium organizations in Bahrain to identify business risks and reduce cybercrimes by implementing effective controls.

There are many forms and types of cyber facilitated crimes, the scope of this investigation focuses on analysing four types of cybercrimes for IT security plans: Denial-of-services (DoS) attacks where cyber attackers attempt to bring down websites or networks, Hacking and defacements of websites, malicious software (Viruses, worms and Trojans) distribution and Spam and Phishing emails. The selection of these crimes is based on the reported incidents in Middle East and Bah-rain in 2011 and 2012. This research will attempt to identify appropriate controls to mitigate the identified risks and use these to formulate an IT audit plan to be used by small and medium enterprises.

The research objectives are:

- To produce a risk assessment report on cybercrimes threat sources, impact and recommended controls.
- To generate a risk assessment based audit plan, which can be used by private or public sectors in Bahrain in order to assess

and improve technical, managerial and operational controls.

2. LITERATURE REVIEW

Information Security is concerned with Information Confidentiality, Integrity and availability; the C.I.A. triad. With today's connected work, cybercrimes impact businesses information, compromise one or more angle of the triad. Cybercrimes as defined by UK home office [2] is crimes that fall into two categories, that is "offences committed using new technologies, those targeting computer systems and data such as hacking , or old offences facilitated by the use of technology such as stealing illegal images or fraud". According to Choo [3] cybercrimes have various types of victim impacting them in short or long term basis; short term cybercrimes impacts the daily activities of users and business. Long term impact includes national security breaches, social impact and unrest and loss of intellectual property. In his research, Choo [3] also refers that UK's National Security council has identified cybercrimes as one of the four highest priority security risks.

In a research by Burden,Palmer,Lyde & Gilbert, [4] the team identified some of the key areas of online criminal activity, these include hacking, cyber vandalism (defacement), dissemination of viruses, denial of service attacks, and domain name hijacking. The research community also has made many attempts to prevent and detect online criminal activity, Massa & Valverde [5] created a online fraud detection system for e-commerce applications that detects online attacks including SQL Injection, Cross Site Scripting, buffer overflows and weak authentication policies.

2.1 Denial of Service Attacks

Denial-of-services (DoS) and distributed denial of services (DDoS) are attacks where cyber criminals attempt to bring down websites or networks. "The purpose of this attack is to prevent legitimate users from gaining access or using a particular internet service" [4] DoS can be triggered by multiple methods including Ping floods, Smurf or Fraggle Attacks or SYN/ACK Flood, these methods consumes the bandwidth destined for organization servers and thus freezing or crashing the target system.

There are several general categories of DoS attacks. Thomas [6] classifies DoS based on the attack mechanism as follows:

- Consumption of scarce, limited, or non-renewable resources
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components

DoS Bandwidth attacks, attempts to consume the available bandwidth, the attack uses UDP or ICMP packets to simply consume all traffic thus slowing down the access to network resources. This form of attack works by exploit the throughput limits of servers or network equipment by sending large number of small packets.

Protocol Attacks, use the inherited design in TCP\IP protocol suite such as TCP, UDP and ICMP; SYN flood for example is an asymmetric resource starvation attack in which the attacker floods the victim with TCP SYN packets and the victim allocates resources to accept perceived incoming connections.

Software Vulnerability attack, unlike bandwidth and protocol attacks exploits vulnerabilities in the network resources such as web servers or the underlying TCP\IP stack such as land attack; where IP packets are send to the network with the source address and port set to be the same as the destination address and port [6].

2.2 Web site hacking

Organizations implements web sites and offer online services to enable it potential and existing customers to find all information they are looking for, view the business offered services and settle payment. According SANS [7], web-based application attacks is top priority to cyber criminals, web applications that do not properly check the size of the input, sanitize user input, does not initialize and clear the variables allows attackers to inject exploit such as buffer overflows, SQL injections, Cross-site-scripting, and cross-site forgery attacks.

Web site hacking and defacement is referred to as "cyber vandalism" [4], hacking and defacing websites involves hacking into the web application and altering the content of the web site, usually defacement occurs after exploiting application vulnerabilities such as SQL injections, cross site scripting or local file inclusions.

2.3 Malicious software

Malicious software (Malware) has been ranked as a key cyber threat to business, governments and people [3]. Attackers distribute malicious software via emails or other distribution channels, the malicious software will exploit the host system vulnerabilities causing it to mal function, or be part of larger bot nets acting as a zombie, assisting the a master to commit further crimes including distributing viruses and spam.

Malware is defined by KMPG [8] as "software that takes control of any individual computer to spread a bug to other people's devices or social networking profile". Sophos [9] continues the same definition by adding that it encompasses "viruses, works, spyware, adware and Trojans".

Malicious code can be introduced to a network via web browsing, email attachment and, mobile devices to say the least. Today's malware is capable of capturing sensitive data, disabling antivirus solutions.

Advanced controls to prevent malware includes implementing network access controls solutions to verify system patches and security configurations before granting network access, outbound traffic must be inspected ; large, unauthorized encrypted traffic must be inspected, source machine must be isolated from the network and thoroughly inspected.

Operational controls include implementing incident response procedure, identified malware samples can be provided for antimalware vendors to provide out of band signatures to be deployed in the organization. Patch management is also crucial as malware usually spreads via unpatched systems. Organizations must have a patch management policy, documented and enforced.

2.4 Spam emails and phishing

Spam emails are unsolicited emails sent without the recipients consent, usually spammers use phishing techniques designed to steal login credentials and banking details utilizing social engineering and "the availability of personal information in the internet and social media sites" [3]. Phishing is defined as "criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details" [10].

According to the web sense threat report [9], emails spam dropped to 74% in 2011 in comparison to 84% in 2010 most of which was due to taking down of spam bot net. 92% of analysed spam emails contained URL. In order to reach target victims "Phishers heavily utilize social engineering techniques to lure email users and divulge their valuable data" [11]., similar to the web sense report [11], reports that the most common way of redirecting victims to fraudulent website is via hyperlink available in an email.

According to Bergholz et al. [11] there are two different types of phishing attacks:

- Malware-based phishing: in which malicious software (Malware) is spread by email through exploiting security vulnerabilities of software installed on the user's machines, the malware then acts as key logger storing the users input.
- Deceptive phishing: in which a phisher sends out deceptive emails pretending to come from a reputable institution, and hoping that the end user will provide sensitive information such as bank accounts, user names and passwords etc.

2.5 Risk assessment

To combat cybercrimes, organizations must determine their risk levels and how best to mitigate these risks, this is done by adopting a risk assessment methodology, in which risk are identified and evaluated and risk impact is assessed followed by selection of controls to mitigate the risk.

Risk is defined by the national institute of standard and technology (NIST) [12] as "the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence" or "Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization " Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level."

Risk management consists of three processes namely risk assessment, risk mitigation, and evaluation and assessment. The risk assessment methodology consists of nine steps, which are as follows:

1. *System Characterization:*
   First step of the risk assessment process, in which the "boundaries of the IT system are identified" this step is critical in defining the scope of the risk assessment. System information must be clearly

documented to include all the available information regarding the Hardware, Software, internal and external connectivity, system administrator, system function, and data criticality.

Information required in this phase can be collected by questionnaires, interviews or the use of automated scanning tools.

2. *Threat Identification*

   The purpose of this step is to identify any potential threat source and its motives; threat is defined as the potential for a particular threat source to successfully exercise (intentionality or accidently) a particular vulnerability. This steps must be as through as possible, documenting all possible threat sources even if the likelihood of occurrence is low.

3. *Vulnerability Identification*

   Vulnerability is defined as "A flaw or weakness in system security procedure, design, implementation or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result on a security breach"

   This steps goal is to identify vulnerabilities that can be exploited by the previously identified threat agents. Vulnerabilities can be identified using different sources, including but not limited to previous risk assessment, penetration test, and security configurations and professional organizations vulnerability databases.

   During this phase, security requirement check list is also documented; the checklist contains the basic security requirements that can be used to evaluate and identify the vulnerabilities of the identified assets in three different saucily arenas: management, operational and technical.

4. *Control Analysis*

   NIST [12] "The goal of this step is to analyse the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability"

   The same controls can be used to defend against cyber-attacks; organizations must implement controls necessary to negate these attacks. These controls can be managerial, technical or operational [12]:

   - Managerial controls: These controls covers issues that focus concerning the overall security program and risks within organizations, managerial controls focuses on the implementation of computer security policies, security program management, and risk management.
   - Operational controls: These controls are put in place to improve the security of a particular system, and focuses on issues concerning the personnel. Example of these controls includes Incident Handling, Awareness, Training and Education.
   - Technical controls: Technical controls are those placed into systems and dependent on them to function, such as Identification and Authentication, logical Access Control, Audit Trails and the use of Cryptography.

5. *Likelihood Determination*

   This step focuses on determining the likelihood of potential vulnerability being exploited by an identified threat-source. The likelihood levels are high, medium, or low.

6. *Impact Analysis*

   This steps goal is to determine the impact of threat materialising on security, to be specific on the C.I.A triad causing loss of integrity, Loss of Availability, Loss of Confidentiality or combinations of these security goals.

7. *Risk Determination*

   Risk determination step focuses on calculating the risk level to organization systems; which is expressed as a function of threat likelihood, impact and the adequacy of the planned or implemented controls. NIST [12] methodology uses a 3 x 3 risk matrix. "The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low; the value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low" [12].

8. *Control Recommendations*

   In this step, organization recommends controls that can be used to mitigate or eliminate risks. The control selection should consider the effectiveness of recommended controls, any legislation and regulation, organizational policy and any operational impact [12].

9. *Results Documentation*

The results of the risk assessment must be documented and shared with senior management and decision makers.

2.6 Information Technology Auditing Theory

"An audit is an independent examination of an organization's management assertions that must follow a set of guidelines and standards promulgated by an external sanctioning body" [13].

Audits adopts a risk based approach that is that identify potential risk, priorities them, and assess controls effectiveness. Activities carried out during an IT audit include:

- Reviewing business processes documentation;
- Evaluating application controls;
- Reviewing audit logs; and
- Reviewing the validity of the records within the database

IT Audits are beneficial to organizations, as it assists in the "identification and documentation of effective control mechanisms for information systems", or helps management and make them aware about the lack of controls. Moreover, IT audit assists in the generation of suitable documentation for the IT environment, its controls and overall architecture and hence enables management to have in-depth understanding of the various business process and IT function supporting it [13].

According to ISACA [14] Information system auditors must develop and document the following items as part of the audit planning:

- A risk-based audit approach for the information systems in scope.
- "An audit plan that details the nature and objectives, timing and extent, objectives, and resources required"
- "An audit programme and/or plan detailing the nature, timing and extent of the audit procedures required to complete the audit"

Audit and information assurance professionals must also adopt an appropriate risk assessment methodology to develop the IT audit plan and determine the resources priorities; planning individual reviews must not overlook the relationships between the audited area and others included within the scope of the audit. "A clear project definition" is a key factor to ensure the audit effectiveness and identify, the plan should clearly indicate the objectives, scope of work, schedule and resources allocations. The developed plan, that forms part of the in-house audit plan, must be reviewed at least annually in accordance with the auditing standards.

Moroney et al [15]explains that there are five stages for audit; it starts with planning stage which involves gaining an understanding of the client and the environment, "identifying risk factors, developing audit strategy, and assessing materiality" followed by materiality, audit strategy, execution and reporting stages.

Although research in the area of cyber security is available namely in the areas of protocol security, product security and operational guidelines [16], there is however a need to research and deliver standards that assist in the use of these cyber security solutions and provide guidelines to small and medium size organizations who does not necessary have dedicated security of audit functions.

Research usually either focus on exploring critical controls that needs to be implemented or risk assessment methodologies and how it should be adopted, organizations needs to be able to adopt risk assessment methodology and have audit plans that assist them identify the critical controls required based on risk assessment conducted by their organization as threats, while similar, differ to each organizations.

The proposed research will attempt to combine the risk assessment, control research and cyber security research to guide organizations to prioritize control based on their unique situation. Most researches focus on critical infrastructure protection and national cyber security activities and little focus in given to small organizations.

3. RESEARCH METHODOLOGY

Qualitative and quantitative approaches will be followed to conduct this research project, with the objective of identifying risks associated with four cybercrimes (DoS, Malware, Spam and defacement), and determining controls necessary to prevent and reduce the impact of these threats.

A core component of the research is to identify cyber threats and the controls that need to be in place to defend organizations from these cybercrimes. Main sources of cybercrimes threats and controls will be driven from the following sources:

- SysAdmin, Audit, Network, Security (SANS) to be specific the top 20 controls for effective cyber defence.
- National Institute of standard and technology (NIST) Computer Security Division (CSD).
- Information Systems Audit and Control Association (ISACA).
- Standards like the International Organization for Standardization (ISO) and the Payment Card Industry Data Security Standard (PCIDSS).

Once threats and necessary controls are defined, the critical path or the minimum requirements to protect against the four mentioned crimes will be identified to form a set of audit control objectives that will form the base of the cyber security prevention audit plan. A survey will be then designed and distributed to solicit feedback and comments on the plan. An audit case study will be presented for the plan execution in one private sector organization.

The research deliverables are as follows:

- Statistics about the number of reported cybercrimes, and a current overview of Bahrain cyber security technologies implemented.
- An Audit plan, which can be used by private or public sectors in Bahrain in order to assess and improve technical, managerial and operational controls.

A case(s) study performed against a Bahraini organization using the developed plan and audit controls.

A core component of this research involves collecting data from security vendors and participants. A short survey consisting of 28 questions was designed and included in Appendix A. The survey was distributed through Twitter, Face book, LinkedIn and email.

For the purpose of this research, a short survey is designed to achieve the following objectives:

1) Measure the level of awareness about cybercrimes in Bahrain.
2) Collect data with regards to the cybercrimes reported in Bahrain.
3) Validate that the control analysis phase includes all possible controls used to protect against the mentioned cybercrimes (DOS, web hacking, malware and spam).
4) Verify which cyber security technologies are implemented in Bahrain.
5) Solicit feedback and review of the modified risk assessment methodology and designed audit plan.

Target audience for this survey includes ISACA CISM\CISA members, Information Security professionals such as ISSO, CIO, system and network administrators. The target list is 34 participants from Bahrain.

The Audit plan design consists of a set of audit requirements and objectives and testing procedures. The designed audit plan will be designed in a table with four columns with the following headings:

1) Audit objective –which defines the control objectives and the set of requirements listed in relation with crime prevention
2) Testing procedure- which assists the auditor to check for the requirements supporting the control objective. Testing procedure will also define the personnel who can provide input to each requirement.
3) In place, not in place: to provide whether a requirement is in place or not along with the appropriate observation and comments that can be used as evidence to support the selection.

The proposed audit plan will be designed with the following control objectives:

1) Ensure that the organization has current assets register: Keeping a register of the organization systems not only forms an input to the risk assessment process but it considered an important security controls as well; cyber criminals continuously scan networks to identify new systems to exploit, un-patched and unsecured systems that are connected to the network could allow internal or external attacks to penetration the network defence.
2) Ensure that the organization has solid boundary defence: Attack generated from hosts outside the network must penetrate the perimeter network, the initial points of attack usually includes hosts connected to the internet. As attackers perform their on-going

reconnaissance activities they can identify new hosts connected to the network and start their malicious hacking activities.

3) Ensure that the organization has secure configurations for all its assets: Attackers launch attacks that targets vulnerable software or set using the default security configuration allowing for system to be exploited. Organization should ensure that all servers, workstations and network equipment are implemented with a secure hardened baseline and ensuring that these confutations are continuously reviewed and updated

4) Ensure that the organization builds and obtain secure applications: The organization can obtain software of develop these in house, software installation could have vulnerabilities built into them, the objective of this audit is to verify that organization develop software based on best practices and ensure that software vulnerabilities are not introduced.

5) Ensure that organization have continuous monitoring and security review of the environment and its vulnerabilities: Companies needs to ensure that the environment is secured at all times, the purpose of this audit objective is to ensure that companies have a process of testing the securing of their environment and making necessary corrections to the vulnerabilities identified.

6) Ensure that the organization is prepared for incidents and incident handling: Without effective incident response plan and procedures organization might not be able to detect attacks or responded to them to.

These core six objectives ensure that organization implements layered security in its environment; perimeter security, network security, and host security.

RESULTS AND EVALUATION

4.1 Survey Analysis

The survey consisted of 28 questions; the total participants were 34 that successfully completed all questions in the survey. Participants were mostly from technologies departments and audit however there were some participants who were in HR and technical sales teams.

4.2 Cybercrimes Awareness

With regards to Denial of services and distributed denial of services crimes, 88.2% (30 participants) were aware about the form of crime. 11.8% of the participants (4 participants) did not know what it means. Surprisingly the participants who did not know this form of crime were filling the positions of developer, IT Administrator, Supervisor and System support engineer.

With regards to web hacking and defacements, 97.1% (33 participants) were aware about this form of crime, only one participant who is a supervisor in a government sector did not understand this crime. Each cybercrime specific section of the research contained definition of the crime to increase participant’s awareness and assist them to answer the survey questions.

With regards to Malware crimes, 88.2% of the participants (30 participants) did understand this form of crimes; the remaining four participants filled the position of HR Specialist, IT/DC Head, Supervisor and system support engineer.

With regards to Spam, 97.1% (33 participants) were aware about this form of crime, only one participant; System support engineer did not understand this form of crime.

With regards to Phishing, 91.2% (31 participants) were aware about this form of crime, 8.8% (3 participants) which were HR Specialist, IT/DC Head and System support engineer were not aware about this crime.

While the lack of knowledge about Denial of services crimes and web hacking and defacement were acceptable, malware, spam and phishing is common themes that all company employees must be aware about regardless of their positions. While the lack of knowledge about Denial of services crimes and web hacking and defacement were acceptable, malware, spam and phishing is common themes that all company employees must be aware about regardless of their positions. However, knowledge about this form of crimes is a must and hence I conclude that while the awareness level seems high with regards to the participant number, key member of technologies staff should be made aware and educated about these crimes.

10 participants (29.4%) reported that their organization were subject to DOS\DDOS crimes in the past 12 months. The remaining 70.6% did not report or were not aware about this attack made against their organization. In the time of writing

this research report, major network disruption of services was observed across the country. These events were attributed to a major telecom being under DDoS attacks however; this was not confirmed nor denied.

Industries reportedly been subjected to DoS\DDoS is finance, telecommunication, transportation and other.

14.7% (5 participants) were subject to web hacking and defacement, 85% were not subjected to this form of crime in the past 12 months. Those subjected to web hacking were from finance and telecom sectors. 38% of the participants (13 participants) were subjected to malware crimes in the past 12 months, 61.8% were not.

Almost half of the participants were subjected to spam attacks in the past 12 months (52.9%), 16 participants (47.1%) did not report facing these crimes.

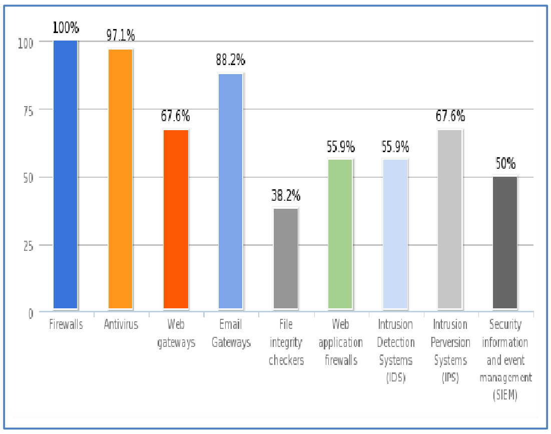
91.2% (31 participants) were subjected to phishing in the past 12 months, 8.8% (3 participants) were not subjected to any phishing targeted at their organization.

Finance, telecom and government sector are the ones mostly facing these crimes in comparison to the other industry sector.

4.3 Cyber security technologies implemented in Bahrain

Participants were asked to identify cyber security technologies implemented in their organizations. All participants had implemented firewalls in their organizations. 97.1% implemented antivirus solutions which is critical protection against malware. Based on the survey results many companies in Bahrain did not implement SIEM solutions, web application firewalls or file integrity checkers and other technologies. Web and email gateways became a must nowadays however these were also missing from some of the participant organizations.

Table 1 Cyber Security Technologies Implemented In Bahrain



Participants recommended adding additional technologies to prevent these crimes; these are listed in the table below:

Table 2 Additional Technologies To Prevent Cyber Crimes

DB firewall
DDoS Mitigation
Honeypot
Incident and Response
Network Traffic Analyser (Zero Day attack), for eg: FireEye
Penetration testing
Policy and Procedure, Change management control, Security Awareness and USB Blocking
User based access
penetration testing systems

4.4 Cybercrime Audit objectives

Based on the research, a control objective framework is developed to assist organization secure their environment against cybercrimes. The same control objective is used as a base to the audit plan. The order of this control objective is based on the priority of the control in the crime prevention as per the research analysis. Participants were requested to review the designed audit objectives and rank these based on their importance in cyber-crime prevention.

Participants ranking of these control objectives was aligned with the designed framework and hence no modification of the order of these controls were required.

Table 3 Cyber Crime Prevention Control Objective Ranked By Participants

Item	Total Score	Overall Rank
knowledge about the environment and all its assets	177	1
solid boundary and network defence	148	2
secure configurations for all assets (Servers, workstations, network equipment)	139	3
build and obtain secure applications	105	4
continuous monitoring and security review of the environment and its vulnerabilities	88	5
incidents and incident handling	57	6

Participants also added that the framework should include objectives to cover users awareness and change management procedures, a procedure to quarterly review the network equipment, these form part of control objective 2, to build a solid boundary defence and control objective 5 to continuously monitor the environment for vulnerabilities. It was also emphasized that awareness and employee background checks are of great importance in cyber-crime prevention which also forms part of control objective 6 of the audit plan.

The audit plan that created as a result of the proposed control objectives and it was included in appendix B.

5. CONCLUSIONS

The survey supporting this research showed that some high level positions within the IT departments lacked an understanding about cybercrimes, this raises an alarm as organization relies on technologies staff and department to protect them from cybercrimes. Educating senior management is as important as educating the end users about security.

Implementing technical controls such as firewall is not sufficient preventive control as it needs to be backed up by operational controls such as the continuous firewall rule reviews and on-going verification of these rules. Based on the research it was evident that cybercrime prevention control objectives should focus on multiple layers within the organization including technical, management and operational controls. While having technical controls a major role based on the research the least implemented technical control was File integrity checkers, in which only 13 out of 34 participants had implemented it in their organization. The lack of these controls could mean that organization is not aware about the changes that happen in their environment which is a significant control in the prevention of crimes. The same applies to web gateways, and antivirus as not all participants had implemented it in their organization ; making them at a high risk of having malicious software or malicious web content being accessed and downloaded by their staff members. The case study also emphasised this point as the company under review had many of the technologies implemented however, operational and management controls are missing or not enforced and hence the audit plan provided the company with missing gaps in their cyber security efforts that needs to be prioritized and implemented by the organization.

One of the biggest limitations of this study was the sample size. The sample size here was 34. Whilst this may appear to be a small number and some might argue about the generalization of the results, it does actually represent a large body of knowledge, experience and expertise in a less explored area of research. Respondents are Information Security professionals from Bahrain and they were carefully selected based on their qualifications and experience.

REFERENCES:

[1] Stephens, J., & Valverde, R. (2013). Security of E-Procurement Transactions in Supply Chain Reengineering. *Computer & Information Science*, *6*(3).

[2] UK Home Office (2012), “Cyber Crime Strategy” retrieved Jan 10, 20012, [Online] from http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf

[3] Choo, K. K. R. (2011), The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719-731.

[4] Burden, K., & Palmer, C. (2003). Internet crime: Cyber Crime—A new breed of criminal?.

Computer Law & Security Review, *19*(3), 222-227.

[5] Massa D and Valverde R (2014), A fraud detection system based on anomaly intrusion detection for E-commerce applications, *Computer and Information Science*, 7 (2).

[6] Thomas, R. (2001). Managing the Threat of Denial-of-Service Attacks. CERT Coordination Center.

[7] SANS (2011) "Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)" [Online] available from: http://www.sans.org/critical-security-controls/cag3_1.pdf (Accessed 27-Apr-2012)

[8] KPMG (2011) "Cyber Crime – A Growing Challenge for Governments" retrieved March 10 2012 [Online] form: http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf

.[9] Sophos (2012) "Security Threat Report 2012" retrieved March 10 2012 [Online] from http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx

[10] Loganathan, M., & Kirubakaran, E. (2011). A Study on Cyber Crimes and protection. *International Journal of Computer Science*, *8*.

[11] Bergholz, A., De Beer, J., Glahn, S., Moens, M. F., Paaß, G., & Strobel, S. (2010). New filtering approaches for phishing email. Journal of computer security, 18(1), 7-35.

[12] National Institute of Standards and Technology (NIST) (2001), Standard Reference Database Number 69, July 2001, Gaithersburg, MD 20899, webbook. nist. gov .

[13] Merhout, J. W., & Havelka, D. (2008). Information technology auditing: A value-added IT governance partnership between IT management and audit. *Communications of the Association for Information Systems*, *23*(1), 26.

[14] ISACA, C. (2010). Control Objectives for Information and related Technologies.

[15] Moroney, R., Campbell, F., Hamilton J.(2012), Auditing: A Practical Approach First Canadian Edition, Wiley

[16] US Govement General accounting office (2004) "Technology assessment Cybersecurity for Critical Infrastructure Protection" [Online] Available from :http://www.gao.gov/products/GAO-04-321(Accessed 10-Aug-2012)

APPENDICES

APPENDIX A-Survey

1) Participant position*

Please enter your position \Job title

2) Organization industry*

( ) Agriculture, Mining

( ) Construction

( ) Finance, Insurance

( ) Real Estate

( ) Government

( ) Health Care

( ) Telecommunication

( ) Manufacturing

( ) Retail, Wholesale

( ) Transportation

( ) Non-profit organization

( ) other

3) Number of employees*

4) Do you know what is DOS \DDOS?*

( ) Yes

( ) No

5) Has your organization been subjected to DOS\DOS attacks? In the past 12 months?*

( ) Yes

( ) No

6) In your opinion, who is the most likely source to launch DOS attacks?-please order them based on the likelihood*

_______Hacker, cracker

_______Computer criminal

_______Terrorist

_______Industrial espionage (companies, foreign governments, other government interests)

_______Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)

7) Controls to prevent DOS are listed below, please order these based on the their effectiveness in combating DOS.*

_______Firewalls

_______Antivirus

_______Web gateways

_______Email Gateways

_______File integrity checkers

_______Web application firewall

_______Intrusion Detection Systems (IDS)

_______Intrusion Prevention Systems (IPS)

_______Security Information and Event Management (SIEM)

8) Do you know what is Web hacking and defacement?*

( ) Yes

( ) No

9) Has your organization been subjected to Web hacking and defacement attacks in the past 12 months?*

( ) Yes

( ) No

10) What is the most likely source to launch Web hacking and defacement attacks?-please order them based on the likelihood*

_______Hacker, cracker

_______Computer criminal

_______Terrorist

_______Industrial espionage (companies, foreign governments, other government interests)

_______Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)

11) Controls to prevent Web hacking and defacement are listed below , please order these

based on the their effectiveness in combating Web hacking and defacement*

_______Firewalls

_______Antivirus

_______Web gateways

_______Email Gateways

_______File integrity checkers

_______Web application firewalls

_______Intrusion Detection systems (IDS)

_______Intrusion Perversion systems (IPS)

_______Security Information and Event Management (SIEM)

12) Do you know what Malware is?*

( ) Yes

( ) No

13) Has your organization been subjected to Malware attacks in the past 12 months?*

( ) Yes

( ) No

14) What is the most likely source to launch Malware attacks?-please order them based on the likelihood*

_______Hacker, cracker

_______Computer criminal

_______Terrorist

_______Industrial espionage (companies, foreign governments, other government interests)

_______Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)

15) Controls to prevent Malware are listed below , please order these based on the their effectiveness in combating Malware*

_______Firewalls

_______Antivirus

_______Web gateways

_______Email Gateways

_______File integrity checkers

_______Web application firewalls

_______Intrusion Detection systems (IDS)

_______Intrusion Detection systems (IPS)

_______Security Information and Event Management (SIEM)

16) Do you know what SPAM is?*

( ) Yes

( ) No

17) Do you know what Phishing is?*

( ) Yes

( ) No

18) Has your organization been subjected to SPAM attacks? In the past 12 months?*

( ) Yes

( ) No

19) Has your organization been subjected to Phishing attacks? In the past 12 months?*

( ) Yes

( ) No

20) What is the most likely source to launch SPAM\Phishing attacks?-please order them based on the likelihood*

_______Hacker, cracker

_______Computer criminal

_______Terrorist

_______Industrial espionage (companies, foreign governments, other government interests)

_______Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)

21) Controls to prevent Spam\Phishing are listed below , please order these based on the their effectiveness in combating Spam\Phishing*

_______Firewalls

_______Antivirus

_______Web gateways

_______Email Gateways

_______File integrity checkers

_______Web application firewalls

_______Intrusion Detection systems (IDS)

_______Intrusion Prevention systems (IPS)

_______Security Information and Event Management (SIEM)

22) Which of these technical controls are implemented in your organization or planned to be implemented?*

[ ] Firewalls

[ ] Antivirus

[ ] Web gateways

[ ] Email Gateways

[ ] File integrity checkers

[ ] Web application firewalls

[ ] Intrusion Detection Systems (IDS)

[ ] Intrusion Perversion Systems (IPS)

[ ] Security information and event management (SIEM)

23) Are there any technical controls you would like to add to the above mentioned list of cyber security technologies ?*

( ) Yes

( ) No

24) If yes, please specify which controls you would like to add to the list

25) Based on my research, the following control objectives were selected as a core to combat cybercrimes. Based on your knowledge and expertise please order these based on their importance and effectiveness in the proactive crime prevention (with the most important objective being in first)*

_______knowledge about the environment and all its assets

_______solid boundary and network defence

_______secure configurations for all assets (Servers, workstations, network equipment)

_______build and obtain secure applications

_______continuous monitoring and security review of the environment and its vulnerabilities

_______incidents and incident handling

26) Do you think the control objectives selected offers protection against cybercrimes?*

( ) Yes

( ) No

27) Do you have any comments or suggestions you would like to share with regards to the controls objectives?

28) Based on these controls and the control objectives highlighted in this survey, an IT audit plan is to be designed. Would you like to receive a copy of the audit plan to be used in your organization?*

( ) Yes

( ) No

29) Please add your email address to receive the audit plan

APPENDIX B- Audit Results For The Case Study

Objective	**Testing procedure**	**In place**	**Comments**
Asset registers exits in the organization	Can administration provide the total number of Information assets within the organization: Servers, Workstations, network equipment, mobile devices and storage devices?	YES	Organization maintains a list of all assets in the organization, and utilizes automated tools to validate its assets and discover any unknown assets that are connected to the network. Any lost or stolen assets must be reported directly to the computer security incident response team (CSIRT), physical security team and Bahrain Police.
	Identify the servers and services accessible from the Internet, identify their role and pay attention to web and email servers.	YES	Servers accessible from the Internet are isolated in a DMZ.
Ensure that the organization have solid boundary and network defence	Interview network admin, verify if Network segmentation and different VLANs are implemented; at a minimum a DMZ and internal VLAN is available	YES	The organization implements isolated VLANs , DMZ, Critical Assets VLAN , Server VLAN and floor VLAN
	Is the DMZ isolated from the rest of the network? And separated by a firewall?	YES	
	is Inbound communication is restricted, known malicious IPs are filtered and blocked	YES	
	is the Traffic flowing between VLANs is restricted based on the application and access requirement with a default deny		A process was recently introduced where in each server available in the critical servers VLAN is documented and the necessary firewall rules are updated for that particular server.
	Is Network-based Intrusion Detection System (IDS) and \or Intrusion Prevision System (IPS) implemented at the perimeter.	YES	We have implemented a state of the art IPS with multiple sensors in the DMZ, Servers VLAN and critical assets VLAN as well.

	Is a web proxy (web gateway) implemented to filter inbound HTTP traffic and block URLs based on organization policy?	YES	
	is Web application firewalls implemented to protect against known web attacks	YES	
	Is Secure email gateway implemented to filters all incoming and outgoing emails for spam and malicious code	YES	
Ensure that the organization has secure configurations for all its assets (Servers, workstations, net-work equipment)	Interview system admin to identify whether a Secured hardened image and standard build exists for servers and workstations		While a draft base line is documented, hardened images do not exist. All new server implementations are hardened based on CIS benchmarks.
	Interview system admin to identify whether Base built mandate the removal of unnecessary accounts, disabling or removal of unnecessary services.	YES	
	Does Server and workstation build mandate the following :		
	Applying the latest patches to the operating system and the base software's installed	YES	
	Closing open and unused network ports	YES	
	deploying intrusion detection systems and/or intrusion prevention systems, and installing host firewalls	YES	
	Server administration is over secure channels that	YES	

	utilizing SSL or IPSEC		
	File integrity checkers are deployed?	YES	Particular, not all servers have file integrity checkers deployed. The File integrity checkers sets to report any changes on daily basis.
	A secure base configuration exists for each type of network equipment (firewalls, routers, switches)		Point taken, the team should have these available and documented.
	Networking equipment implements ingress and egress filtering	YES	
	Firewall and routers rules are documented and approved with business justification	YES	
	Exception process exists to deviate from the base build	YES	
	End point security solutions (Antivirus and anti-malware) is implemented to protect servers, workstations and mobile assets		It is implemented in all windows based operating systems, there are however different operating systems in use.
	Implemented end point security solutions are set to updates signatures on daily basis	YES	
	Removable media is now allowed to be used (DVD's CDS and USB) unless with a justified business reason	YES	
	End points auto play features are disabled.	YES	

Ensure that the organization builds and obtain secure applications	Interview Software development staff or staff responsible for acquiring software code and advice whether a System Development Life cycle is documented and adhered to.		Some software is developed in house and others are obtained.
	A process is adopted to include security in the development life cycle.	YES	Mandated by the organization Information security policy
	All developed code must be verified for the following:		
	User input is defined in terms of size and format and that it's validated –(Input validation)	YES	
	Input is validated so that SQL commands cannot be executed-	YES	
	Buffer overflows	YES	
	Insecure communications	YES	
	Secure cryptographic storage	YES	
	Error handling	YES	
	Software development personnel receive training in writing secure code for their specific development environment.	YES	Recently introduced as part of the organization process to improve its developers, the same developers were tasked with completing a SDLC
	Software development personnel are aware about secure coding practices.	YES	Recently introduced as part of the organization process to improve its developers, the same developers were tasked with completing a SDLC

Ensure that the organization have continuous monitoring and security review of the environment and its vulnerabilities	Interview Information security team or staff with security responsibilities and advise whether a process of continuous vulnerability assessment is documented and adhered to.	YES	Not documented procedure however mandated by the information security policy. A requirement is added to establish a procedure.
	An automated vulnerability assessment is conducted on frequent bases to identify any vulnerability in the environment, for servers, network equipment and workstations.	YES	Every quarter and after each major change in the environment.
	Identified vulnerabilities are corrected via patches or controls are implemented to prevent these from being exploited.	YES	Policy mandates that patches are applied within 30 days from their release.
	Annual of more frequent penetration testing is conducted internally and externally by certified internal or external security professionals.	YES	Annual test by a partner organization.
	Social engineering is included within a penetration testing exercise.	YES	Phishing and helpdesk phone calls were among the recent penetration tests.
Ensure that the organization is prepared for incidents and incident handling	Interview Information security team or staff with security responsibilities, identify whether a Security Information and Event Management (SIEM) is implemented.	YES	SIEM is one of the recent implementation in the organization, it integrates with file integrity checkers, IPS and have IDS correlation engine build in. it also perform periodic asset search.
	verify that the SIEM collect and correlate from all devices on the network including the DMZ	YES	

	A Security incident response plan is documented and adhered to.	YES	
	Security incident responders are trained on how to handle and respond to security incidents.		Support staff did not have proper incident handling training however; this will be included in the training requirements and submitted to HR for their approval.
	End users are provided with basic security training.	YES	Annual security training is offered, it’s interactive online and a monthly security awareness newsletter is distributed.