The Design of a Risk and Vulnerability Assessment Procedure for a Banking Institution

Ludrián J. Marrero Otero
Master in Computer Science
Dr. Jeffrey Duffany
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Regulations in banks are changing constantly and becoming stricter. Threats and technologies are improving. Most antivirus software update their virus definition when the malware is released and attacking. Banks need to define a good network perimeter to avoid these malwares to arrive the systems. Companies don't consider information security a core aim. This can cause systems to be obsolete, leaving a potential system malfunctioning and vulnerable. Sometimes, information security professionals are not well prepared or trained, employees not being loyal to the company, segregation of duties and roles not well defined, are some of the challenges banks are facing.*

Key Terms *— Information Security, Malware, Regulations, Threats, Vulnerable.*

HUMAN FACTOR RISK ASSESSMENT

What are Human Factor Errors?

Human error is a failure of a planned action to achieve a desired outcome [1] and can be caused by low skills in a desired field, obsolete procedure manuals and people who aren't aware of new technology changes. Errors can occur in the planning and execution phase and have two variants: skill-based errors and mistakes.

Skill-based errors occur when the person has full knowledge, skills and experience doing the task. Taking disciplinary action or re-training are not accurate responses to this matter.

FINDING - A memory lapse occurs at some point of doing a task when someone forgets a step, the task sequence is changed. This can occur simply by pressing the right button in the wrong order.

RECOMMENDATION - A checklist is recommended.

REVIEW - On a one to ten chance, there is an 80% of probability to happen on a rush basis. Example; a customer representative is working on a particular user account and need to print an evidence or a letter to send it back to the customer, and the user send the wrong copy/document to the customer. That wrong document could be another customer information or company documentation.

Mistakes are considered as failures in the planning session. They can occur due to inexperience or poor information. Mistakes aren't made on purpose, so disciplinary action is not a good way to solve them.

Knowledge-based mistakes can occur in a trial and error situations. Insufficient knowledge doing a task is the primary reason of this kind of error. Rule-based mistakes often occur when the incorrect application of a good rule occurs. This means that, when a rule works well in previous occasion and is applied to another process expecting the same results. Bad rules may be created based on incorrect knowledge, or a good rule may become bad following changes that are not managed appropriately.

FINDING - Violations tend to be well intentioned, with the goal of task completion and simplification.

RECOMMENDATION - Violations should be managed by the application of disciplinary actions.

REVIEW - On a one to 10 scale, it can occur 90% of the time. Managers often request tasks on an ad hoc basis leaving the user exposed to a short time frame period to perform that task. The user, to perform the task, bypass every procedure and rule and get the job done. Most managers are aware of this, however, they keep this practice ongoing because they need the job to be done leaving systems to be instable or insider data leakage.

Factors that Increase Susceptibility

Social engineering is a common way to get sensitive data from a source and use it against a person to conduct scams, fraud and other kinds of illegal actions.

FINDING - Social engineering can increase if it targets the victim's trust. Asking for small parts of information from different people could lead to a major attack. When emotions such as happiness, anger, excitement are targeted, the victim normally provides information.

REVIEW - We can't measure the likelihood of a social engineering attack to occur. We are exposed to it all the time. However, most banks have in place security awareness programs and tools to avoid external social engineering attacks. Those employees who are in contact with customers are vulnerable to these attacks. Proper training can reduce the impact on this to happen. Internally, user needs to be aware of those employees whose intention is to harm the enterprise or another employee.

Phishing attacks focus is to get usernames, passwords, credit information and sensitive data. Most of these attack these days come from an email message. Messages look legitimate in many cases, but there are other cases where the message's content fails from typos.

FINDING - Writing passwords on a piece of paper, and stored under the keyboard. This leads the attacker, an insider, to appropriate of these credentials and use them. Re-using the same password in different applications and using easy guessable passwords such as: "12345," "qwerty," "123abc" are still a problem that companies are facing.

RECOMMENDATION - Password complexity rule (minimum password length of 8 alpha-numeric characters, user must change password every 60 days, locking –out users after 5 or less incorrect password attempts, minimum of 4 historic password, logging out user after a prolonged period of inactivity, using numbers and special characters).

REVIEW - Most banks active directory rules with password complexity controls. User are in charge of their own password protection. On a one to ten scale, there is an 80% of user that writes their password on a piece of paper or notebook but a 60% to 70% chance the user store the password in an unsafe place. From one to ten chance, 60% of the employees use in their passwords relevant information about them.

Applications requires User ID and password to log in them. A best practice is to use multi factor authentication in which the user is required to answer a challenge question and a password. If the user can access an application remotely, it is required to use a multi factor authentication method plus a token to certify that the user itself is attempting to log in.

FINDING - Having files accessible to every user in a common folder. In most places, several users can work on the same workstation. Having all user accounts at the same privileged access level.

RECOMMENDATION - Information becomes power when it is exchanged. If we want control of what we have, we need to protect it and avoid errors.

REVIEW - On a one to ten chance, there is a 0 to 10% chance to occur. User access and shared folders are assigned based on their roles and duties. The only chance this can occur is when a user is new to a corporation and get accesses wrong defined. They can also occur when a user move internally from one unit to another.

There are five types of human factor errors [2]: acts of omission occurs when people forget to perform a necessary action. Example; an employee who fails to regularly change his or her password. Act of commission is the second type of human factor error and can be a user that performs an incorrect procedure or action. Example; an employee who writes down his password. Doing something unnecessary is the third human factor error. Sequential acts is the fourth human factor error and involves doing something in the wrong order. Time errors is the last human factor error and is caused

when people fail to perform tasks in the required time.

RECOMMENDATION - Communication will be effective if it is clear and accurate on what the audience needs to know. It needs to contain where the risk originates, how it is assessed and the frequency of the risk. Information security communication can cover risk. This has to be communicated in different media such as discussion, meetings, seminars, flyers, emails, forums and many others.

All aspects of information security needs to be related to the strategy and objectives of the organization. Many businesses act upon a potential risk if its cost of reducing or mitigating it is lower than the potential cost posed by the risk.

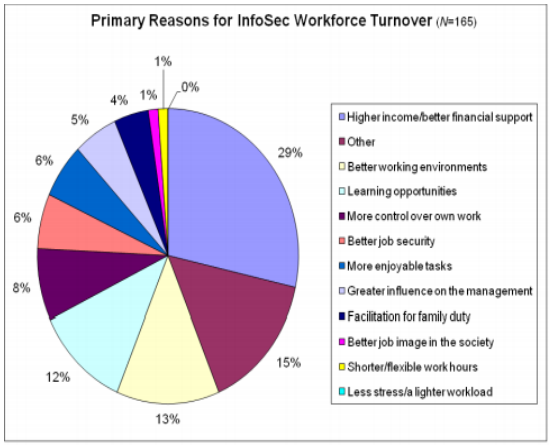

Figure 1
Primary Reasons for Information Security Turnover

PROCESSES RISK ASSESSMENT

How to Well Document Processes?

FINDING - Gather the necessary information.

RECOMMENDATION - This information should be non-technical and technical. Technical information includes network maps with details of internal and external connectivity, hardware and software inventories and configurations, databases and sensitive information. It also has policies and interfaces with external entities, policies and standards. Non-technical information includes policies, standards and procedures addressing physical security, facilities, information assets, personnel security, and contracts.

REVIEW- "Application Owner" is a key contact in the organization to address risk assessments. On a one to ten scale, 90% of the cases, the user needs assistance while completing the assessment. Application owner knowledge is based on who the developer of the application is. The user needs assistance from other business units or the application developer itself. Not having knowledge, can lead the company not complying with the security standards requested by the regulators, audit and problems within the organization. In house built applications, the user possesses full knowledge of the controls and standards used to build the application. These controls in place should be but not limited to: user id and password used (if challenge questions or tokens are available are also considered), access request procedures used to grant access to the application, segregation of duties, if accesses are reviewed periodically, password rules (password complexity, password length, password history, password change time frame, etc.), what information is displayed in the application, backups methods and requirements and many other security measures considering applications through internet and cloud.

FINDING - Identifying the information and the information systems.

RECOMMENDATION - Understand how the information is used by the institution and to how paper-based information is transmitted, managed and stored. This also considers the outsourced companies and how they handle data.

REVIEW- In this case, 100% of the users know the information they are handling. An 80% of the security incident reported consist on giving information to the wrong customer. Banks have implemented several rules in email systems to not send unencrypted emails with private information. These rules are based on patterns and are not always accurate.

FINDING – Institutions should classify and rank sensitive data, applications and systems.

RECOMMENDATION - They must be based on the nature of their function, data and the sensitivity of it.

REVIEW- Information is classified in:

- *Highly restrictive: is protected under regulations or laws of client information, or secrecy policies.*
- *Confidential: refers to the protection of information from unauthorized disclosure.*
- *Internal use: published in the intranet or can be disclosure to external parties with authorization.*
- *Public: may be released to the people in general.*

Threats are events that can damage the integrity, availability and confidentiality of information. Internal threats can be employees, service providers, contractors and insiders. External threats can be criminals, hackers, terrorists or even competitors. Natural and manmade disasters are considered as external. Vulnerabilities are weakness in controls and systems if exploited. Known vulnerabilities are discovered by testing or reviewing systems, policies, processes and others. They can be anticipated to occur in the future. Examples: software bugs or employees who fail to perform their security policy duties.

FINDING - Analyzing the impact if a threat causes damage, cost of the damage and how the damage is going to be restored.

RECOMMENDATION - Identifying and implementing controls to mitigate each vulnerability. Analyzing impacts leads the organization to evaluate control effectiveness.

REVIEW- Each bank must have written procedures and a security incident committee to address incidents. If the committee have ten members, 30% or 40% of them are information security or IT experts. The other 60% or 70% are people in charge of how to communicate with the customer affected, lawyers and human resources specialist if disciplinary actions should be taken.

Timing controls consist of prevention, detection, or correction. Nature controls consist of administrative, technical, or physical. They should measure the probability of an event. Risks are high, medium or low and are assigned taking into consideration the adequacy of related internal controls.

Information Security Strategy

This is a plan to mitigate risks while complying with regulations, standards and rules. Policies are used to guide decisions made by users.

RECOMMENDATION – Policies should be reviewed at least annually.

FINDING - Privileged access have to be controlled.

RECOMMENDATION - IT should allocate those privileges on a need-to-use or an event-by-event basis. Privileges granted should be documented and audited.

REVIEW - These access should be well documented because can affect the segregation of duties policies, standards and guidance. It should exist a formal access request method to grant access. On a one to ten scale, 80% of the cases have proper documentation and documentation on why a privilege access is granted.

Security tokens consist of a generation of numbers randomly sequenced in a certain time frame. After that time frame expires, the sequence of numbers will be randomized again.

FINDING - Weaknesses: guessing the combination of the generated numbers, reverse engineering, cloning the token and man-in-the-middle attacks, theft or loss.

RECOMMENDATION - The use of multi factor authentication.

REVIEW- The token device is strictly assigned to an employee and if the device is lost, it is considered as a security incident. A reverse engineering for a token is rare to occur. On a one to ten chance, barely exist a 10% to an employee loose the token device and from a one to ten chance, exist a 0% chance of a reverse engineering, guessing the combination or cloning the token. The only way to have access to a token device is if a user leaves

unattended the device, loose it or via a social engineering attack.

Biometrics validates user's identity by referencing a unique physical or behavioral characteristic. A physical characteristic can consider finger print or iris pattern while a behavioral characteristic is a unique pattern of key strengths and pauses made on a keyboard when a user types a phrase. Biometric authentication doesn't rely on a user's memory or to have a token to be effective.

NETWORK ACCESS

The information security personnel's role is to lead in the development of policies, standards, procedures, and compliance and incident response procedures. Network administrators implement those procedures, policies and process.

To configure a network, applications, systems accessed and the definition of minimum access requirements for services should be considered. A firewall can be used to control access between security domains. A packet filtering firewall examines all data packets, letting pass or blocking packets based on previously established rules. Packet filtering firewalls are unable to prevent exploitations because the packet filter does not examine packet contents. This firewall is less secure because it is easy to misconfigure.

Stateful firewalls keep track of the state of network connections traveling in them. A proxy server firewalls are the most secure and expensive, but information packets don't pass through a proxy. A proxy acts as an intermediary where computers make a connection to the proxy and it initiates a new network connection based on the request. To enhance firewall security, we can remove unnecessary services, fixing an application's bugs, and giving proper maintenance.

Wireless networks are difficult to secure. They should be treated as untrusted networks.

RECOMMENDATION - Use end-to-end encryption.

Application Access

Access controls for the application should be consistent when assigning new user access, changing an existing user, or removing access. These accesses have to be monitored for unusual activities to ensure if the proper access has been given using event logs.

Physical and Environmental Protection

Information should be kept confidential, with its integrity conserved and has to be protected. In the risk assessment, organizations should include political issues, criminals, flood, earthquakes, fire, smoke, explosives and others.

RECOMMENDATION - Organizations must select a safe zone to locate its internal assets. Guards, fences, barriers and cameras are in place to protect external facilities and control access to restricted areas. Zones like data centers, power supply units, and telecommunications and media equipment should have restricted access.

Encryption

Encryption is a way to protect the information, data, systems and databases. It is important it pass a secret message from one place to another without the information stored in that channel being revealed.

Symmetric encryption consists of a secret key (number, word, piece of text) applied to a message's text to change its content. It can occur by changing a letter from a number or vice versa. The message can be encrypted or decrypted only if the sender and the recipient know the secret key. Asymmetric encryption has a public key and a private key. One key is used to send an encrypted message. The public key is available to someone who wants to send an encrypted message to a certain recipient. To decrypt an encrypted message using asymmetric encryption, the recipient should use his or her private key in which the individual is the only one having access to it to see the message's content.

Security Monitoring

Networks are actively being monitored for unusual logs. Host activities are limited to operating systems and applications. Network activities are

based on network traffic allowed through a firewall or sensors placed on a switch that controls a subnet.

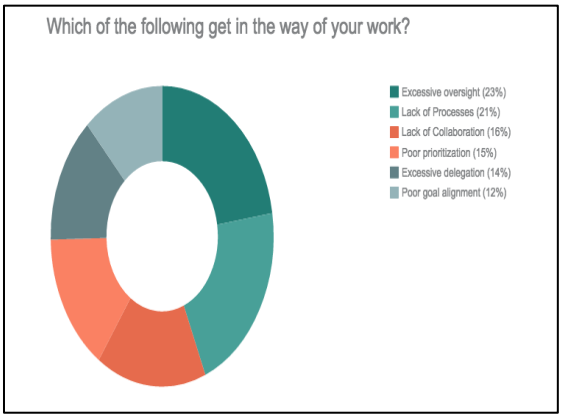

Figure 2
Which of the following get in the Way of your Work?

SYSTEMS RISK ASSESSMENT

Security Issues Banks are Facing Today

Risks for mobile devices include: loss and theft, mobile malware, and mobile units accessing non-secure networks, and the lack of security for the BYOD (Bring Your Own Device). Not updating a mobile operating system allows vulnerabilities to be exploited. Malware intrusion can install a backdoor through the system and if the device is connected to a bank's network, it can lead to critical security issues.

Public networks are not recommended if sensitive information such as paying bills, accessing bank accounts, credit cards, email, etc. are involved. "Rooting" or "Jailbreaking" a device is risky and information, data, photos can be targeted.

FINDING – Not updating mobile devices.

RECOMMENDATION - Encrypt the mobile device.

REVIEW - IT department is in charge to update the device as soon new definitions are available. Network Admin have the power to disable the network access to an outdated device. Chances drop to a 10% to 20% since definitions are installed as soon they are released and tested in current systems.

FINDING - Theft or loss of mobile devices.

RECOMMENDATION - The complete wipe process of the device.

REVIEW- These events are very common in a bank industry. On a one to ten chance, it can happen 80% to 90%. Senior management is responsible for these incidents. All devices are encrypted prior to be assigned. Device theft comes when a user left it unattended in desks, lunch rooms, car, or they lose them. Another incident is, hard drive theft. A user don't stole a computer but try to get access to information by stealing the drive. PC hard drives are encrypted as well. PC stealing come when it left unattended in a desk. Most banks use safety cables to protect their equipment.

FINDING - Allowing your device to auto connect to networks and keeping the Bluetooth device turned on.

REVIEW- On a one to ten scale, this happen 100%. User let their devices auto-connected for several reasons: public Wi-Fi available, known Wi-Fi password for a bank private network or they forget to turn it off. These issues happen for Bluetooth devices as well. We can include the use of smartwatches. An attacker can get access to the device inspecting all the information stored.

What is Tokenization?

Tokenization is the process of replacing non-public personal information (bank accounts, names, social security numbers, dates of birth, etc.) with a cardholder' non-relevant information. With credit card numbers, the merchant acts by using the same 16-digit format, matching it and hiding it.

Advantages for Merchants

Merchants are not required to make major changes to their current payment acceptance systems. They can use a token system to track transactions, handle refunds, returns and many other transactions. Mobile wallets (Apple Pay, Samsung, etc.) can be used physically in stores or via the Web. Protocols are used and store one-time tokens in the mobile wallet to protect the information.

Tokenization is handled at the merchant level. It is usually given by a service provider, issuing banks, card networks (VISA, MasterCard, Discover, AMEX) or even by a wallet provider. When the

merchant implements a token, it gets the account number but doesn't save it. Card information is secured via encryption and the merchant processor decrypts it.

In the case of an issuer or any card network, the issuer is authenticated by the wallet service and the token is sent to the merchant. The token is replaced with the appropriate cardholder data for authorization by the issuing bank. Apple Pay works similarly, but the difference is that it has a different token assigned to each smart phone. Instead of using the security code from the back of the card, Apple Pay creates a dynamic security code to securely validate each transaction.

Token Encryption

Data that is replaced with a token is also encrypted with point-to-point encryption at the POS terminal and decrypted when the payload reaches the application. The transaction is secured at the beginning and at the end. Many point-to-point encryptions are not end-to-end, but the encryption occurs at the point-of-swipe, and decrypted by the merchant acquirer. A tokenized account number is not valuable to anyone outside the merchant.

Vulnerabilities

FINDING - Attackers can get access to databases where card information is stored along with the tokens.

FINDING - Attackers are also buying credit card numbers online. They load that information onto systems like Apple Pay, giving them the opportunity to create a physical fake.

Standards

- VISA on July 10, 2014: VISA Tokenization Best Practices for tokenization uses in credit and debit card handling applications and services [3].
- MasterCard and other brands in October 2013: Introduced a proposed framework for a new global specification for enhancing the security of digital payments using payment tokens [3].
- EMVCo LLC in March 2014: Released its first payment tokenization specification for EMV [3].
- Clearing House on July 1, 2013: Pilot program aimed at fostering standards to implement tokenization [3].
- ANSI X9 as X9.119 Part 2: The effort is for developing standards definitions for tokenization and for generating and validating tokens [3].

Standards often lag behind technology advances with the common practice being that the technology is introduced followed by standards. Security especially is comprised of a series of steps, where timing is very important, as well as understanding how changes benefit all parties determining whether new technologies are adopted. Furthermore, just because standards are developed by an accredited standards body (e.g. ANSI and ISO) does not mean it may not contain proprietary technology that includes the use of an essential patent claim [3].

Risk of Remote Access: Merchant Card Payment Systems

FINDING - Criminals have exploited databases and payment processing systems.

RECOMMENDATION - Multi-factor authentication.

POS Malware Family Names

- Alina is a POS malware that targets applications containing track data. It applies basic encryption and exfiltrates the information. This malware allows for searching and installing automatic updates when they are released [4].
- Backoff POS malware consists of scraping memory for track data, logging keystrokes, command & control communication and injecting malicious stub into explorer.exe to crash or forcefully stop events. In addition, it also uses a key logger functionality [4].
- BlackPoS/Kaptoxa infects the computer running a Windows environment. The malware identifies the running process associated with

the credit card reader and steals payment card Track 1 and 2 data from its memory. BlackPos is a RAM scraper that grabs encrypted data when it travels through the live memory of a computer. The captured data is uploaded to a remote server via FTP [4].

- Chewbacca is a Trojan virus that logs all keystrokes and sends the data to the botnet controllers via Tor [4].
- Decebal is a Romanian PoS malware capable of checking if the computer on which it is installed is running any sandboxing or reverse engineering software. It also can validate if the stolen card numbers are legitimate [4].
- Dexter steals the process list while parsing memory dumps of specific POS software-related processes, looking for Track 1/Track2 credit card data [4].
- Fighter PoS uses keylogging techniques and also can get full control of the infected machine [4].
- JackPoS is inspired by the Alina PoS Malware and is masked as the Java Update Scheduler [4].
- Log PoS avoids a traditional detection mechanism of scanning files for unencrypted credit card information by instead writing to a mailslot. A mailslot allows communication between processes both locally and over a network [4].
- NewPoSThings looks for credit card track data then exfiltrates the spoils to a command and control server [4].
- NitlovePOS can capture ex-filtrated Track 1 and 2 payment card data by scanning the running processes of a compromised machine. Data is sent to a Web server using SSL [4].
- FindPOS/PoSeidon can be detected by an antivirus. It has a key logger function. The malware searches memory for credit card track data and verifies any logged numbers through the Luhn algorithm. A Luhn algorithm is a simple checksum formula used to validate a variety of identification numbers [4].
- vSkimmer searches program memory for track data. It only looks for data matching the Track 2 format. It can be configured to copy data to a specific USB device if it is unable to connect to the Internet [4].

Applications

FINDING - Consider if the system information could be accessed using other utility programs (MS Access, Excel, etc.).

RECOMMENDATION - Minimizing the use of these applications.

REVIEW- On a one to ten scale, this can occur 100% of the time. Applications such as Excel and Access are used to data management. These applications can contain NPI information, policies, internal data and many other information.

FINDING - Backups in systems are critical.

RECOMMENDATION - Application data should be backed up and retained according with the retention periods stated by the bank regulation. Backups needs to be encrypted.

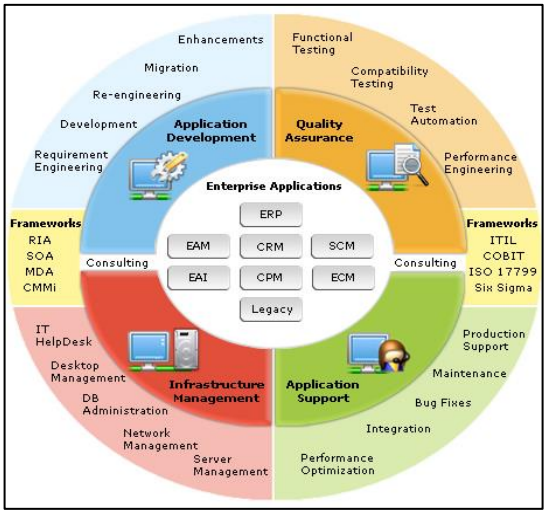

Figure 6
Applications & Systems

Applications must have testing environments. This is important because testing process can never be executed with real customer information and can affect information confidentiality and reliability. Any information security assessment should be performed at least annually. This can include threats and vulnerability assessments, risk assessments,

GLBA assessments, penetration tests and many others. It is important that the application or system owner complies with every regulation stated. Systems should have a fraud detection and monitoring systems in place which consider customer history and behavior and enable a timely and effective institution response, policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud.

CONCLUSION

The weakest link in a company is the people (staff), giving a lot of opportunities of improvement. Awareness programs are created and reviewed constantly to ensure employees have full knowledge of new trends in the information. Banks have in place systems and security profiles that give help to users to avoid security flaws.

Internal policies and regulators state measures to safeguard the information. Bypassing rules will make them null. Human error are hard to avoid even with the most expensive security and monitoring methods. A good recommendation is that internal audit evaluate that the application and procedures are performing well according to policies, but they can give recommendation on how an employee do his tasks and if he follows the stated procedures and policies. Bank's issues can be addressed with full knowledge users, not only giving awareness training but visiting business unit and performing a checklist on how they are handling and implementing policies and procedures. They can give recommendations avoiding future audit's findings.

With Payment Card Industry (PCI), banks rely on outsourced service providers for merchants and transactions. A failure in these systems will cause customers to loose trust in merchants or financial institutions. Banks have to be sure on who they rely that kind of communication and how it will be affected if these systems are targeted by an attack. With past events, banks incurred in costs replacing customer debit/credit cards because information was targeted via merchants. Merchant provider is responsible for updating his systems and hardware to ensure maximum protection. What can happen if a merchant system is affected by attackers or by a failure? Customer can choose between different merchant providers, decreases in sales, cost in replacing cards, losses from frauds, compliance fines and penalties, legal costs, going out of business and loss of jobs [5].

Most system failures occur because wrong deployment performed, a particular process was not performed on time, user testing environment was not used properly or was not used at all, and a device was unplugged for certain procedures. Even if a system was accessed externally by a hacker, there was a factor that lead that attacker to enter the network. Most of these factors includes a not well configured firewall, a network was not well segmented to avoid traffic, and systems updates were not performed on time. Most updates have to be tested before implementing them for compatibility and stability matters. Network vulnerabilities and penetration tests are performed by a third party. Common findings in this report are: unpatched applications, outdated servers, logging to a terminal using TELNET client, the use of man in the middle attack, SQL injection and others. Not well configured and unused sections of a network includes unknown domains and testing domains as well.

The use of third party solution tools are helpful on a day to day basis. Banks must avoid the use of these tools usage, especially if the tool is going to be connected to the network, databases (ODBC) or if the tool is accessed via internet.. ODBC connection are helpful for that job but can affect server stability and the system can fail. A human factor error could be a server failure because multiple ODBC logons at the same time or constantly pulling data. Another human factor is letting the computer unattended while using these tools. Banks have in place a 15 minutes automatic lock in computers if the computer became idle.

We can conclude that employees have to be capable of detect their own mistakes and correct them. Employee awareness material should be included in the employee manual. Awareness,

should be given at least twice a year, recommended to be trimestral. Supervisors or managers can include clean desk policies and information security measures discussed here as the employee annual performance requisites.

Employees are responsible of running a bank and they are going to be a challenge in the near future. Employees with several years working in a bank are less likely to accept changes. They don't take information security measures as an important matter. With these kind of employees, banks have to take actions to ensure all policies and regulations are being followed as stated.

REFERENCES

[1] Nopsema. (2014). 'Human Error'. [Online]. Available: http://www.nopsema.gov.au/resources/human-factors/human-error/. [Accessed: 5-Oct-2014].

[2] K. Parsons et al. (2010). 'Human Factors and Information Security: Individual, Culture and Security Environment. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf. [Accessed: 5-Oct-2014].

[3] D. Schutzer. (2015). 'Tokenization in Financial Services'. [Online]. Available: http://fsroundtable.org/cto-corner-tokenization-financial-services/. [Accessed: 22-Apr-2015].

[4] FS-ISAC et al. (2015). 'Alert and Recommendations: Securing Merchant Card Payment Systems from the Risks of Remote Access'. [Online]. Available: https://www.fsisac.com/sites/default/files/news/Alert%20--%20Securing%20Merchant%20Terminals%20Remote%20Access%20FINAL%207%20July%202015.pdf. [Accessed: 25-Sep-2015].

[5] PCI. (2016). 'Why Security Matters'. [Online]. Available: https://www.pcisecuritystandards.org/pci_security/why_security_matters. [Accessed: 6-Jan-2016].