Education in IT Security: A Case Study in Banking Industry

TSE W.K. DANIEL, HUI M.H., LAM S.T., MOK Y.C., OEI W.C., TANG K.L., YAU X.L.

Abstract—**The banking industry has been changing incessantly and facing new combination of risks. Data protection and corporate security is now one of the major issues in banking industry. As the rapid changing on technologies from time to time, the industry should be aware on new technologies in order to protect information assets and prevent fraud activities. This paper begins with literature study of information security issues and followed by focused-group interviews with five participants within the industry and survey analysis of "The global state of Information Security survey 2013" which published by PriceWaterhouseCoopers (PWC). Trends and questions were discussed as well as possible solution. The study suggests that IT security education should be made to different level of staffs such as executives, professional and general staffs. Besides, the banking industry should increase company-wide security awareness and the importance of corporate security which keep the information and physical assets secure and in a proper way.**

***Keywords* - IT security education, banking industry, security awareness, data protection, corporate security**

I. INTRODUCTION

Nowadays, banks are implementing different types of practices to protect the information and information systems from fraud attacks. Maintaining information security requires support and co-operation from all employees within the organization.

The research aims to evaluate current information security practices in the banking industry and assess the information security awareness level for the employees in the industry. The research is divided into three levels, executive (C-level staff), IT Professional and general staff, based on business needs.

To do the research, representatives from the financial institutions and organization that provide information security training were interviewed. Meanwhile, analysis on the result, which was published by PriceWaterhouseCoopers (PwC) [1], was performed.

The result showed that there was a lack of well-structured training activities provided for the existing staff. Meanwhile, the employees do not consider information security as part of their responsibilities. To solve the problem, several recommendations (e.g. implementing Information Security Awareness Training Program) were made and suggested the banking industry in Hong Kong to follow.

II. LITERATURE REVIEW

Nowadays, online banking is one of the most popular Internet activities. Customers would use the online banking service to perform different types of financial activities (e.g. money transfer, share trading). Banking systems contain a wealth of private financial information. Certain data such as personal credit file could be used as a shared secret between the banks and the customers at a specific moment. Since the evolution of the banks, there have been some unscrupulous individuals who try to undermine its defense system in order to gain access to the valuables. [2] Smyth found that password recovery is one of the threats in using e-banking facilities. There is an increasing concern on the security level of the online banking systems. [3] McGlasson stated that the most important part of a good bank IT security infrastructure is information security.

In order to protect the information assets and prevent fraud activities, the banking industries should design and implement information security strategies. Two suggested solutions are establishing information security governance framework and organizing information security awareness training program. Meanwhile, [4] Tiow warned that the banking industry should not overlook the security awareness issue under outsourcing environment.

A. *Information Security Governance Framework*

The word "Information Security Governance" has become popular recently, especially for banking industry. The corporate executives start to pay attention on information security and are willing to make investment on establishing information security governance framework to protect the information assets. However, most of the corporations do not have much experience on it.

[5] Ohki et al. conducted a study to review how corporations in Japan performed their risk management processes from the view of information security. The result showed that most of the corporations established information security program from a bottom-up approach by setting up information security policies and procedure as well as security controls. However, this kind of bottom-up approach might not solve difficulties and issues effectively since the alignment and interconnection between the management philosophy and corporate policies were not clear enough.

The main objective of establishing the Information Security Governance Framework is to set up an Information Security Committee which senior management or representatives of board of directors are required. This can help to align the IS strategy with corporate strategy so that the effective Information Security policies as well as its enforcement can be adopted.

In order to adopt Information Security policies effectively, the corporations should recruit Security Managers or Chief Information Security Officer (CISO) to facilitate on establishing Information Security Governance Framework. The main duties of the Security Managers are directing, overseeing, evaluating various kinds of security controls as well as reporting the status to senior management from time to time.

B. *Information Security Awareness Training*

Nowadays, computer misuse and illegal conducts are increasing with the growth of computerization. In order to let the staff familiar with the complicated information security

DOI: 10.5176/2251-3043_3.3.268

issues, [6] Payne suggested that the corporations should also deliver an Information Security Awareness & Training program for all levels of staff members in an efficient and effective manner. [7] Porter pointed the importance of security education to combat with the increasing threats of e-banking security.

[6] Payne stated that there were several ideas on delivering the training, e.g. conducting classroom training, seminars and workshop, distributing information security handbooks, creating online quizzes or games. The committee could also periodically host security websites and issue Security Newspaper. Besides, the Security Committee should alert staff members when a level of risk exposure was reached.

Meanwhile, [8] Chen et al. suggested that the training could be delivered using an e-learning platform. The system would provide rich and interactive content via Internet and Intranet. The content could be provided according to target groups according to their job nature or expertise.

Unlike traditional classroom training, the system would emphasize more on employee involvement and effective communication instead of one-way content delivery. Also, the major purpose of the system was to support business operations instead of the employees' own learning path.

[6] Payne also stated that the Information Security Committee should deliver message aggressively as well as making sure that the message inside was consistent, so that users understood the important messages. The committee should use different angles to restate the most important pieces of message in multiple ways.

C. *Security Awareness under Outsourcing Environment*

In order to minimize cost or leverage expertise from the market, it is inevitable that the bank industry would outsource their IT projects to third party. Outsourcing would make security management more difficult as the ownership or responsibility of an IT function or server is transferred to the suppliers.

[4] Tiow has provided a thorough and decent guideline on how to manage security for outsourced service. This guideline introduced what should be achieved during pre-outsourcing activities, which assessment of security risks, specification of security requirements and assessment of competency of supplier should be included. Once the service was outsourced, the security management staff should establish contractual obligations and assess the supplier continual performance.

One of the most important points of this guideline is that, security awareness should not be advocated only among the internal staffs. The personnel provided by the supplier should also be emphasized. The security management staff should verify whether there are security trainings or awareness programs provided for these external staffs. They can verify these external staffs by interviewing the supplier, checking the personnel credentials such as security certifications or training received. Also, they should examine the external staffs on whether their experience and technical expertise can enable them to work proficiently and competently. The suppliers' past references or present customers can be one of the sources of evidence on the experience or expertise.

In order to have the ability to examine the security awareness of the supplier, the internal staffs should be well-trained on security awareness also. Policy and procedures should be provided in order to facilitate them to manage the security in all stages of the IT services.

D. *Summary*

It is a must for the banking industry to pay more attention to the information security issues within the organization nowadays. The banks should establish information security governance framework and organize information security awareness program. Also, the banks should concern more about security awareness under outsourcing environment. In case these suggestions are adopted and well implemented, it is likely that the information assets would be well protected. Then, customer will have more confidence on the online banking services and thus additional corporate value would be created.

III. RESEARCH METHOD

A. *Interview*

Conducting interview usually a stepping stone to both interviewers and interviewee to build the relationship, once relationship is built, it would be easy for the interviewer to gather true and reliable information. Apart from that, conducting interview not only can get information but also let interviewee identify their knowledge on the topic. For this case, the interviews can identify the staff knowledge on Information Security as well as the corporates policies align with business goals as management is involved.

In order to be familiar with the market practice and provide an effective Security Education Program to the clients, interviews with two financial institutions stationed were conducted.

Bank	Descriptions
Bank "A"	A Foreign bank which has branch office
Bank "B"	A Local Retail Bank

The following are five targeted interviewees with their own professions in the banks

Bank	Descriptions
Interviewee "1"	Head of Sales and Marketing
Interviewee "2"	Head of Human Resources
Interviewee "3"	Head of Legal & Compliance (Barrister)
Interviewee "4"	Chief Information Officer / Security Manager
Interviewee "5"	Firefighters (IT Services Desk Engineer)

A serious of questions that about interviewing the staff mentioned above was set up. The goal is to develop an understanding of the topics that the staff is concerned.

Questions for the interviews:

~ What your role is in relation to IT Security?

~ Which key concern do you have in regarding IT Security as a management or employee?

- What is the level of security knowledge or training do you have?
- What types of security training are beneficial to you?
- How would you rate the level of security awareness training within the bank?
- How effective of security policies is currently in place?
- What suggestion do you have to improve the security awareness training within the organization?

Apart from the interview, advice was sought from a service provider which provides education and information security awareness training as well as helping corporate to setup Information Security as another point of view

Questions for the training expertise:

- What have your company provided for your clients in relation to Information Security?
- What will the level of staff attending your training?
- Why do they need your services?
- What is your challenge in providing such services?
- How effective are your services?

B. *Survey*

The analysis was based on [1] that published by PriceWaterhouseCoopers, CIO and CSO Magazine in which they jointly conduct a worldwide study online from the period of Feb to Apr 2012.

This was used as the analysis sample as it consists of sound numbers of companies and staff in different countries and industries.

The following table shows the survey response levels from different industry.

Survey response levels by industry

Industry	Number of responses this year
Technology	1,469
Financial Services	1,338
Retail & Consumer Products	1,169
Industrial Products	775
Public Sector	730
Telecommunications	511
Healthcare Providers	467
Entertainment & Media	378
Aerospace & Defense	242
Automotive	218
Power & Utilities	201
Energy (Oil & Gas)	136
Pharmaceutical	112

Source: Global State of Information Security Survey 2013, by PwC

The following graphs show the response from different countries, titles as well as the size of companies that are reliable for the research:

Respondents by Region of Employment

Asia	Europe	Middle East & South Africa	North America	South America
18%	26%	2%	40%	14%

Respondents by Title

CIO, CEO, COO	CISO, CSO, CIO	Compliance, Risk, Privacy	IT & Security Management	IT & Security (non-MGT)
21%	14%	13%	21%	31%

Respondents by Size of Companies

Small (<$100M US)	Medium ($100M – 1B US)	Large (>$1B US)	Non-profit/Gov/Edu	Do not know
33%	20%	25%	7%	15%

Source: Global State of Information Security Survey 2013, by PwC

IV. RESULTS ANALYSIS & PRESENTATION

A. *Interview Result*

The following are the results of interview

1) *Head of Sales and Marketing*

	Bank A	Bank B
Question 1	No relation to	User
Question 2	Helps to protect customer information	Ensure operation efficiency although tons of security controls are in force
Question 3	Security Awareness Training provided by Head Office when I join the bank	Not really
Question 4	Fulfill Regulators' requirement	Not much actually
Question 5	OK	Not sure
Question 6	Strong enforcement as required by Head Office, regular inspection will	This is a must to comply with policies and standard as required by Hong Kong Bank Regulators

	be carried out	
Question 7	Force the staff to attend the security awareness training	As a user, I am not concerned in Information Security, as I think this is not my job. So, better to arrangement workshops to promote it.

2) *Head of Human Resources*

	Bank A	Bank B
Question 1	Partially, as appointment of Privacy Officer	Partially, as I am in charge of staff development
Question 2	Protection of employee information	Privacy
Question 3	Not much	Nil
Question 4	Importance of information security	Nil
Question 5	Not enough eventually	Can do better
Question 6	High as required by Head Office	So far so good
Question 7	In a centralized manner, all branches use the same set of materials	Having workshops or promote an Information Security Awareness Function

3) *Head of Legal & Compliance (Barrister, Hong Kong High Court)*

	Bank A	Bank B
Question 1	Partially, as appointment of Privacy Officer	Partially, as I am in charge of staff development
Question 2	Customer Data Protection	Customer Data Protection
Question 3	Not much	Not much
Question 4	Importance of information security	Importance of information security
Question 5	Not enough eventually	Can do better
Question 6	High as required by Head Office	Enforcement has been done
Question 7	Can have quizzes or test to make sure staff are aware of this	Promote more by having workshops or activities

4) *The Chief Information Officer*

	Bank A	Bank B
Question 1	My Job	My Job
Question 2	Protection of company assets and maintain a stable system environment	How to increase the security awareness of employee
Question 3	Information Security as well as IT Governance	Information Security Profession and governance
Question 4	To execute my job	One of my job is to promote information security awareness
Question 5	Not just only for new joiner	Can do better
Question 6	In place as regular inspection will be taken place	OK
Question 7	Promote the awareness of Security instead of just comply with policies	Can try to source some vendors in providing awareness training

5) *Firefighters (IT Service Desk)*

	Bank A	Bank B
Question 1	Enforcer	User as well as "policeman"
Question 2	Staff didn't aware on Information Security	Can't control all the staff as some of them are contractor
Question 3	Basic Security training for system support	Basic training
Question 4	To promote information security as a frontier	Not much
Question 5	Can be more	Not really enough

Question 6	OK	OK
Question 7	Now only cover general concept, better enhance to cover more topics	Put more effort in controlling contractor

6) Information Security Education Service Provider

	Bank A
Question 1	Our company provide Information Security related service such as helping the corporate to setup Information Security Framework, Governance as well as providing awareness training to end user
Question 2	All level of staff. However, different topics will be covered to different levels
Question 3	The company lack of resources or talent to provide such training. The management would rather pay money to ask for service.
Question 4	Need to familiar with the corporates' internal policies and procedures before we provide service. However, we prefer the corporates provides awareness training by them, as they will be more familiar with the company culture. We prefer to train up the security personnel to provide such training
Question 5	Keep on going as some of the corporates, especially financial institutions are required to have such kind of awareness training in complying with the bank's regulator

B. Survey Result

The following are the results of survey that are useful stated in [1] by PwC:

1) How confident are you that your organization has instilled effective information security behaviors into the organizational culture?

	2009	2010	2011	2012
The company requires third parties (including outsourcing vendors) to comply with our policies	37%	33%	27%	30%
The company has an incident response process to report and handle breaches to third parties that handle data	37%	32%	29%	27%

2) How confident are you that your organization's information security activities are effective?

	2009	2010	2011	2012
Confident	84%	78%	71%	74%

3) What business issues or factors are driving your company's information security spending?

	2010	2011	2012
Regulatory compliance	22%	22%	27%
Internal policy compliance	27%	27%	31%
Business continuity/disaster recovery	30%	32%	42%
Change & business transformation	32%	33%	32%
Economic conditions	46%	46%	48%

4) What process information security safeguards does your organization currently have in place?

Information Security Safeguards	2009	2010	2011	2012
Have employee security awareness training program	54%	47%	43%	47%
Have people dedicated to employee awareness program	58%	57%	49%	49%

V. Case Study

A. Case 1: The Banks' interview

According to the interview done previously, the following issues have been identified:

1) Information Security Governance

The level of Security is high as required by bank's regulator. However, Bank A has a strong enforcement of policies and procedures as bank's culture as well as the enforcement of their Head Office. As Bank B is a local bank, it requires setting up strong security framework as they don't have a strong background in order to govern the bank.

2) Training / Education

The Information Security Awareness Training is provided, however only for new joiner, as a result staff may not be aware on new threats or policies set by Information Security Committee. It is recommended to provide workshops, slogan, etc. to increase the awareness of Information Security, educating staff not only have to fulfill the requirement of bank's regulator but also the importance of protection of company assets and customer information.

3) Challenge

The most challenge for both banks are increasing staff Information Security awareness, non-IT staff thinks that Information Security is not their business, they just fulfill the requirement set by the bank and regular. Besides, there has a challenge on managing outsourcing vendor as well.

B. Case 2: Services Provider's interview

1) Information Security Governance

Help the corporations to set up Information Security Framework, Governance as well as providing awareness training to all level of staff. However, different topics will be covered to different levels.

2) Training / Education

The Information Security Awareness Training is provided, however only for new entrant, as a result, staff may not be aware of new threats or policies set by Information Security Committee. It is recommended to provide workshops, slogan, etc. to increase the awareness of Information Security; educating staff not only have to fulfill the requirement of bank's regulator, as well as the importance of protection of company assets and customer information.

3) Challenge

The company is lack of resources or talent to provide such training. The management would rather pay money to ask for service. The service providers need to be familiar with the corporations' internal policies and procedures before the vendors provide service. However, they prefer the corporations provide awareness training by themselves, as they will be more familiar with the company culture. They prefer to train up the security personnel to provide such training.

C. Survey Findings [1]:

1) Finding 1: Many respondents are over confident on their security program

74% of respondents are confident that they have effective security, yet many do not have a process in place to handle third party breaches. Only 30% require third parties to comply with privacy policies.

2) Finding 2: Over confident on security program

Most of the respondent saying that their information security activities are effective, but confidence has eroded.

Although 1/3 of the respondents are confident that their company's security activities are effective, they probably don't realize that assurance has dropped since 2009.

3) Finding 3: Security budgets are not driven by security needs

The spending on security investment is not driven by the needs, at 46%, followed by change and business transformation. Business continuity and disaster recovery is the highest-rated security-specific response as required by the regulators or others requirement.

4) Finding 4: Less than half have security training programs for employees

Only 47% of the respondents have an employee awareness training program in place, which is not enough.

VI. Discussion

A. Training for IT Budget control on Security Program

For security program, rate of budget increase is slowing down after recovery from the global economy crisis. It is dropped from 51% in 2011 to 45% in 2012. Most companies think those resources should be used in better way such as generating more revenue. However, [9] if the security program is ignored, the loss in company will be greater than they have earned. For example, Madoff Loss, Money Laundering, fake on-line banking website, etc.

Thus, the training for executives for calculating the IT budget on security program was organized. [10] How to find out the benefit which is greater than the cost and how to find out whether it is worth to invest are the two questions to solve.

For above enquiries, the formula to explain [11] was used.

First step is to find out the loss. There is the calculation of expected loss per risk.

Annualized loss expectancy (ALE) = Single loss expectancy (SLE) x annualized rate of occurrence (ARO)

For SLE, it should be asset value x exposure factor (EF)

Second step is to compare the cost and the loss (ALE). Cost Benefit Analysis (CBA) formula will be used as below

$$\text{CBA} = \text{ALE (prior)} - \text{ALE (post)} - \text{ACS}$$

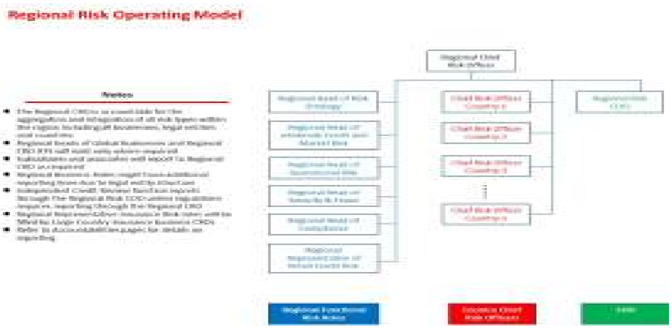
ALE (prior) is the ALE prior to have the controls and ALE (post) is the ALE after the treatment of controls. The difference between the two ALEs represents the less loss saved, i.e. the benefits obtained after implementing the controls. ACS is the annualized cost of the safeguard.

If the CBA is positive figure, the security program will be worth to invest. From this, it can be easy for company to evaluate whether security program (as a kind of security controls) is worth to invest.

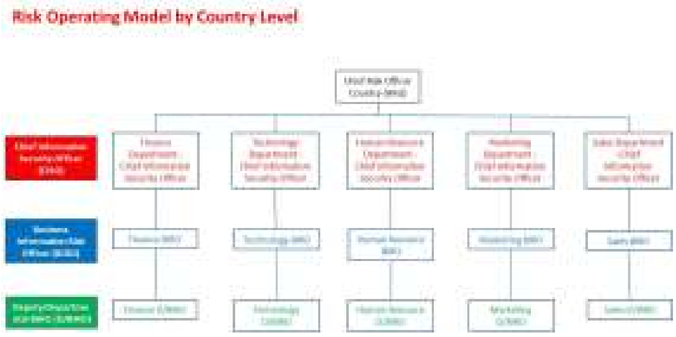
From now, more banks were found unwillingly cut spending on security program. [12] Based on the 2012 Financial News Publishing Ltd, 43% of banks are planning to make significant changes to their IT systems in the next four years to improve management information, regulatory compliance and risk management. 21% are planning immediate changes. Overall, 54% of banks will involve data warehouses and 46% of banks will involve Business Intelligence applications.

B. Training for Implement Risk Operating Model

How to build the Risk Operating Model in the company? Actually the training will be held for the executive to develop the operating model [13]. The training will let the executive know the work flow, structure, job role and job duties in the Risk operating Model. Below is the structure chart of the Regional Risk Operating Model in bank [14][15].



Refer to above diagram -Regional Risk Operating Model, the scope will be minimized and focused on the country level. In country level, it will start from the Chief Risk Officer Country [16].



Role

CISO: ensuring the security of all information within their line of business/department.

BIRO [17]: Responsible for overseeing the management of all Information Security Risk policies, process and projects within their respective line of business [18]

D/BIRO: Responsible for assisting the BIRO and ensure that proportionate and effective information security controls are established

Based on the above information, it shows that it involves many employees, who should be skilled and experienced in risk and compliance, to implement and maintain the information security risk (ISR). After financial crisis in 2008, the government/ monetary regulators (HKMA) is stricter to monitor the banking operation and information security. It makes the emergent need for the talent of risk controller.

Actually if more ISR training can be delivered within colleagues, it can increase their ability and awareness on ISR. Also the employees are encouraged to attend the courses from ISACA (Information Systems Audit and Control Association), BSI (British Standard Institution) and BCS (British Computer Society), then assign the role of D/BIRO to colleague in each department and reduce the pressure of talent people needs.

C. Security Awareness under Outsourcing Environment

Even in banking industry, outsourcing IT projects or services becomes an inevitable trend, as the company can leverage expertise in the market and minimize the operation cost. On the other hand, there is more concern on the security issues from the management which comes from outsourcing.

There are many additional challenges from outsourcing IT projects and services. First of all, it is more difficult for the organization to ensure the outsourcing staffs are qualified for their security awareness level. Next, the IT assets are not necessarily to be inside the location of the company. Especially, in the utilization of cloud computing technologies, the IT assets may be located outside the country. Moreover, according to the support model, remote access may be required for some vendors. This may become a backdoor for outsider's authorized access. Lastly, the globalization of business requires a 24x7 support from anywhere. All these factors can become a missing link in security awareness.

In order to ensure the security awareness under outsourcing environment, a few steps will help the company's decision: 1. categorize the data to be protected; 2; choose the right activities to be outsourced and 3. Choose the right vendor.

1) Step 1: How to categorize the data?

Staffs should aware what efforts should be made in order to protect enterprise data. [19] Different category of data may have different decision. Data may be mission critical, so that any failures made cause a potential loss. Data may represent private customer information; leakage of such information may cause compliance issue or legal actions. Data may include company secrets or confidential formula; the competitors may get advantage when such information is leaked to them. All these factors are needed to be considered in order to perform an appropriate risk analysis or impact analysis. Company staffs should be aware of the risks or impacts when outsourcing the projects and let vendors to access those data.

2) Step 2: How to choose the right activities to be outsourced?

Activities which requires professional specialty, especially those requiring significant personal investment in skills or tools, are good candidates for outsourcing. Hackers and criminals are usually more reluctant to become certified professionals. The certification authority is one of the proofs on the proficiency or ethnics of those professionals. Therefore, one of the criteria of pick up the activities to be outsourced is whether the professional required can be proved by a public certificate. IT staffs involves outsourcing should be aware of the security related certificate and organization. This will help in their outsourcing decision.

3) Step 3: How to choose the right vendor?

To choose the right vendor for outsourcing, the vetting process is the vital important procedure. There are several criteria which will help the company to ensure the vendor has enough security awareness. First of all, the vendor can be requested to provide an external security audit for their company. Also the direct contacts at the vendors' customer can be requested in order to examine their track record. They can be examined on their experience to encounter any material security breaches. On the other hand, they can be requested to provide professional certificate profiles on outsourcing staff in order to prove their security awareness. Any hesitation on providing the information by vendors as mentioned may be a clue of the incapability on security awareness.

D. Security Awareness and Training Activities

In order to increase the information security awareness level of the existing staff, Security Department of the banks should organize a formal security awareness program. It includes developing and implementing an Information Security Awareness (ISA) System in e-learning platform. The system would provide training materials on different topics [20] like password management, social networking safety and data loss prevention. The security threats and the prevention method should be discussed for each of these topics. The system should consist of an online assessment which includes a number of multiple-choice questions regarding the information security issues. This aims to ensure the employees do gain some security knowledge from the materials.

According to the lesson learned from other financial institutions about their ISA system [21], some of their colleagues replied that they were not willing to use the system because the amount of the training materials was too large while the employees themselves had heavy workload and therefore did not have extra time spending on the system. Hence, it is suggested that the training materials can be divided into two modules – core and elective.

The core module shall include all must-known security topics, which may differ among the employees based on their main job responsibilities. For example, staffs from customer services team have a greater chance to get in touch with the sensitive customer data so data loss protection should be included in their core modules. Meanwhile, staffs from infrastructure team staff would usually access the servers in production and testing environment, so firewall and network security issues should become their core module. To ensure the content and the difficulty of the training materials in the core module is appropriate, the Security Department should invite the representative of each team to share their opinions during the program development phase.

Security Department should make the core module compulsory and hence the employees are required to read the training materials and pass the test before deadline. The expected time of completion for the core module should be within 30 minutes so that even the busier staff could find time to complete without affecting their normal duties.

The remaining topics would become the elective modules. Although it is not compulsory, the management should still encourage their subordinates to access the materials when they have spare time or the management gives motivation by granting both extrinsic and intrinsic awards to those who have read the materials and passed the internal test.

Security Department should consider present the materials in multimedia format, e.g. video clips and games, to increase the attractiveness. It is also suggested the department should use real-life examples to explain the security issues so the employees can have a better understanding on how the security topics can apply to their work or even personal life.

However, [22] Ispitzner considered that the Security Department cannot just rely on this e-learning system to promote the information security awareness. It is because the employees would forget the details they have learnt in the e-learning session after a period of time. Also, new types of threat would be exposed with the evolving technologies. The skills and knowledge the employees learnt in the e-learning sessions may not be enough to solve these problems. Hence, the Security Department should update the training materials in the system from time to time and require the employees to take the e-learning sessions annually to remind them the critical security items. In addition, Security Department could issue Security Newsletter which reports the latest security news around the world or within the organization.

Meanwhile, [23] the Security Department should promote the atmosphere for the employees sharing knowledge regarding to information security issues. This can be achieved by setting up a discussion forum in the ISA system, which allows the employees to discuss the newly-discovered security threats and the ways on preventing them.

E. New Technologies on Mobile Banking

The growing popularity of smartphones, mobile banking allows consumers to check balances, transfer money and pay bills. You can access most of the services through the smartphones. This kind of technology has simply made lives easier.

1. Mobile banking services is free of charge to their customers. It means customer can handle transactions without extra cost while saving time.
2. Mobile banking provides three ways of service available to everyone.
   - ~ SMS, user balance information and banking passwords have been easily sent to customer through SMS. It provides fast method.
   - ~ APPs, some banks have dedicated software Apps downloadable in Google “Play Store” or Apple IOS “Apps Store”. These banking mobile Apps can enable their customers gain access to their bank account.
   - ~ Web browser, the smartphone have internet browser facility. This can help people to login their account same way as ordinary computers.
3. In bank, their servers are encrypted for wireless transactions. This means that such transactions may actually more secure than wired connection.
4. The account information (account number) is not displayed on the wireless connection. This contributes to the data security.

On the other hand, new technology also has disadvantages.

1. The biggest security risks in mobile banking are, mobile phone service provider’s server are not encrypted. This makes expert hacker easy access/obtain to user account information or credit card information.
2. The message received from the bank is not encrypted. This means that the information can be easily breached through mobile carrier.
3. If the mobile phone is being stolen / lost, the information stored in the message can be used easily by another person.
4. Using an Internet browser in mobile phone but do not install anti-virus in it. This is in a very high risk of sensitive information being attacked by hackers.

With the increased usage of smartphones and high-speed wireless communication for mobile phones, mobile banking is the obviously the next trend. There is no doubt that it provides a comfortable and easily accessible to their account. However, according to information security, it is absolutely unsatisfactory. Unless the banks come up with full security on mobile banking, it is best to use mobile banking when necessary.

F. USB / Portable Device

Nowadays, Data Lost Prevention (DLP) strategies are one of the major challenges to the IT security industry. According to the survey conducted by [24], 70% of businesses have traced the loss of confidential information to USB devices and 55% of those incidents are likely related to malware-infected devices. How to management the use of USB device is a key area of concern.

Any type of solution which aims to protect the data and prevent data loss cannot immune from untrusted and wrong user input. For the banking sector, ATM devices and HSMs now allow the use of USB. Sensitive data may be stored in the portable devices. Traditional threat such as the data recovery of USB devices still exists. Thus, without a proper management, there will be a high probability of data loss which may lead to financial fraud. Therefore, it is important to manage carefully about the level of access where which levels of staffs are allowed to plug a USB device into the USB ports.

There are other threats pop out alone with the use of USB device, such as loss of data from the USB device and malware attack against the bank operating system via an infected USB device. The use of portable devices may also let the attacker bypass the restriction set by the regular DLP system. These threats associate with the use of USB devices. Any systems which allow the plug-in action have high exposure factor to the risk.

Thus, there is a need of improvement to the design of current DLP solution and the use of portable devices. The solution should be able to protect the system from the risk associated with USB technology. As mentioned in the previous part, the access of enabling USB port should be carefully managed. There should be a tight and enforced policy about the definition of acceptable and unacceptable uses of USB and procedures to recover lost USB drives. The policy should also state clearly that the employees who have access to sensitive and confidential data only use secure USB drives. In order to prevent the use of a virus infected device, employees must scan the device before use.

It is also considerable for any company to provide approved portable devices to the employee. This can ensure that there is no malicious code inside the devices. Meanwhile, it is a must to determine USB drive's reliability and integrity before purchase and the devices should be purchased from trusted vendor with leading security standards.

G. Importance of Senior Executives on the Education on Security Awareness

The participation and buy-in of executives is a critical success factor in any education of security awareness. First of all, getting resources will be easier if the security team is getting buy-in from executives. Secondly, lower level staffs usually follow behavior of their managers or senior executives. If the senior executives do not follow the practice of security, then any security awareness training will be in vain. Therefore, the senior executives will have the highest priority to be educated in security awareness.

There are some themes that can be considered in the education module. First of all, there will be a need to have a thorough explanation to these executives on why they are targets. The discussion can be in a small group, or most appropriate a one-on-one section. The key point is to explain that security incidents can happen to them. Also as they will have more administrative rights, they will eventually be the root cause of problem and the impact will be much larger when comparing the same cases happened to a lower level staff.

Another main point in training the executive is the importance of inclusion of the executive's key staff. These executives' assistant will have access to their email or calendar and they may have rights to access executive's workstation. When this key staffs are trained, they can act as the key person to remind the executive on any potential issue so training on these potential candidates is important in order to mitigate the potential threats.

VII. Conclusion

As indicated from the research result, the current employees in Hong Kong banking industry do not receive enough training on information security training. Most of them are not aware of the potential security flaws and loopholes within the organizations and do not know how to prevent these incidents from occurring.

Several methods, which can increase the information security awareness among the employees, were recommended. An information security training program should be designed and implemented to let the employees have a better understanding on different type of security issues. The management should allocate enough financial and human resources to implement this program. Moreover, the management should also keep an eye on the information security under outsourcing environment.

Once these suggestions are implemented in the bank, it is believed that the banks will increase company-wide security awareness and the importance of corporate security which keep the banks information and physical assets secure and in a proper way. As a result, the employees and the organization would be in a win-win situation.

References

[1] "The Global State of Information Security Survey 2013". [online]. Available http://www.pwc.com/giss2013 [Accessed 2012, 12 Nov]

[2] Ben Smyth, (2010), "How password recovery threatens banking security"

[3] Linda McGlasson, (2007), "Key To Your Information Security Training - Policies and Standards"

[4] Bee Leng Tiow, (2003), "A Security Guide For Acquiring Outsourced Service"

[5] Eijiroh Ohki, Yonosuke Harada, Shuji Kawaguchi, Tetsuo Shiozaki, Tetsuyuki Kagaua, (2009), "Information Security Governance Framework"

[6] Shirley Payne, (2003), "Developing Security Education and Awareness Programs"

[7] Chris Porter, (2011), "Security in e-banking also comes with education"

[8] Charlie C. Chen, R. S. Shaw and Samuel C. Yang, (2006), "Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System"

[9] Ellen Rosen, Bloomberg, (2012),"Money Laundering, Prince Gouging, Bank Suits: Compliance". [online]. Available http://www.bloomberg.com/news/2012-11-06/money-laundering-price-gouging-bank-suits-compliance.html [Accessed 2012, 12 Nov]

[10] Matthew Rosenquist, Intel Corporation, (2007), "Measuring the Return on IT Security Investments". [online]. Available http://www.intel.com/it/pdf/measuring-the-return-on-it-security-investments.pdf [Accessed 2012, 12 Nov]

[11] Andy Good, (2011), "How Information Security expense can provide IT Business Value". [online]. Available http://communities.intel.com/community/openportit/blog/2011/03/02/how-information-security-expense-can-provide-it-business-value [Accessed 2012, 12 Nov]

[12] Financial News Publishing, (2012), "Banks set to increase IT spend to improve risk management". [online]. Available http://www.vrl-financial-news.com/retail-banking/retail-banker-intl/issues/rbi-2011/rbi-659-660/banks-set-to-increase-it-spend.aspx [Accessed 2012, 12 Nov]

[13] DBS Bank Annual Report, (1998), "Corporate Governance. Risk Management Committees"

[14] "Business continuity management", http://www.business-competence.com/business-continuity-management.html

[15] EDGAR Online,Inc, "Credit Risk Management". [online]. Available http://sec.edgar-online.com/j-p-morgan-chase-co/10-k-annual-report/2004/02/18/section22.aspx [Accessed 2012, 12 Nov]

[16] DBS Bank Annual Report , (1998), "Corporate Governance. Committee Structure", [online]. Available http://www.dbs.com/dbsgroup/annual98/Pages/riskman_comm.html [Accessed 2012, 12 Nov]

[17] Chicagojobs.com, (2009), "Business Information Risk Officer". [online]. Available http://cj.chicagojobs.com/candidate/processcandviewjob?docid=A3334-05NL&source=search [Accessed 2012, 12 Nov]

[18] Docstoc.com, (2011), "Business Information Risk Officer". [online]. Available http://www.docstoc.com/docs/68990124/Business-Information-Risk-Officer [Accessed 2012, 12 Nov]

[19] John Landwehr , (2007), "Information Classification – What does "Confidential" mean?"

[20] William Lassiter, (2003), "What Users should know about online banking security?"

[21] Janne Hagen, Eirik Albrechtsen, Stig Ole Johnsen, (2011),"The long-term effects of information security e-learning on organizational

learning", Information Management & Computer Security, Vol. 19 Iss: 3 pp. 140 - 154

[22] Ispitzner, "Top 3 Reasons Security Awareness Training Fails". [online]. Available http://www.securingthehuman.org/blog/2012/02/15/top-3-reasons-security-awareness-training-fails [Accessed 2012, 12 Nov]

[23] K. Thomson, J. van Niekerk, (2012),"Combating information security apathy by encouraging prosocial organisational behaviour", Information Management & Computer Security, Vol. 20 Iss: 1 pp. 39 - 46

[24] Ponemon Institute, (2011), "The State of USB Drive Security". [online]. Available http://media.kingston.com/images/usb/pdf/MKP_272_Ponemon_WP.pdf [Accessed 2012, 12 Nov]

TSE W.K. Daniel (DBA, CEng, CITP, MBCS, CISA, CISSP, CISM, MHKIE) Before Dr. Tse taught in City University of Hong Kong for over 10 years, he had been in IT industry for many years. He had once had his own IT consulting company right before he worked for City University of Hong Kong. His research interests are in information systems security, audit & management, systems development & consulting, enterprise systems integration, and artificial neural network. His personal web site is www.wktse.com HUI MH, LAM ST, MOK YC, OEI WC, TANG KL and YAU XL are his postgraduate students in City University of Hong Kong. They are the IT practitioners.