Winter 12-4-2016

Information Security Challenges in the New Era of Fintech

Eldon Y. Li
National Chengchi University, Taiwan, eli@nccu.edu.tw

Jong Peir Li
National Chengchi University, Taiwan, johnli8139@gmail.com

Information Security Challenges in the New Era of Fintech

Eldon Y. Li, National Chengchi University, Taiwan, eli@calpoly.edu
Jong Peir Li, National Chengchi University, Taiwan, johnli8139@gmail.com

ABSTRACT

After the recent cyber-attacks on financial institutions around the world, we are faced with a whole new set of challenges never seen before. Traditionally, fraud and theft were conducted in person or through traditional telecommunications such as telephone. However, today we are facing highly sophisticated and intelligent hackers who have the ability to illegally access financial institutions' computer systems from remote locations and even across borders. Therefore, this study will focus on reviewing the information security framework by adopting up-to-date standards as the way to counter financial information theft.

Keywords: Cyberattack, Information Security System, Fintech, Hacker

INTRODUCTION

Information security problems come in various forms worldwide, including the cyberattack on Central Bank of Bangladesh by hackers in February 2016, which hackers used APT (Advanced Persistent Treat) malware to hack i0nto the system of Central Bank of Bangladesh and stole the access to SWIFT system, submitting transfer requests to Federal Reserve Bank of New York and successfully transferred the foreign-exchange reserved of 81 million US Dollars owned by Central Bank of Bangladesh. Later, in August this year, the biggest USD to Bitcoin Exchanger Bitfinex was attacked by hackers and more than 65 million USD was taken. This summer, teller machines in Taiwan was under attack of malware and was robbed of over 70 million NTD. Transnational scams conducted in Kenya occur commonly. These frequently happening information security incidents proved that the measures of cyberattacks are changing nonstop, becoming more destructive, and the amounts of heist are far higher than a conventional bank robbery. Many enterprises and businesses depended on the entire service provided by information security company or use the information system that hasn't been updated for years when it comes to information security management in the past. However, the professionalism of hackers, on many occasions, overwhelms the information security level that information security companies can provide. In the meantime, Fintech has been burgeoning globally recently; nevertheless, many responsible persons investing in angel fund recently have made remarks that without information security, there won't be Fintech. When they review new investment cases, whether these startups are having a wholesome information security mechanism becomes the key factor making determining their investments. In particular, many of the startups are internet companies storing massive amount of client information, frequent trades, even ginormous capital. Therefore, information security is the premise of Fintech's success.

RESEARCH QUESTIONS

After multiple new information security problems have happened, this study intends to research the following three issues to find the information security strategies matching requirements by financial institutes in the future.

RQ1: How to improve the software, hardware, internet and management system of financial industries to prevent attacks by hackers?

RQ2: How to perfect in downside improvement and profiting simultaneously? In other words, how to make information security operating smoothly while Fintech can be well-developed?

RQ3: Information security system can take massive time and manpower inputs. How to consolidate the mutual power of the government and financial industry to develop an information security system catering to people's needs?

CONCEPTUAL FRAMEWORK

Figure 1 exhibits the six important components used to analyze the information security system in this study. These components are mutually related and indispensable, coming as such: (1) Design of information security system, (2) Software of Information Security System, (3) Internet Security, (4) Central Surveillance Institute, (5) Control of Information Security, and (6) Cultivation of Information Security Talents.

Design of Information Security System

The design for Fintech

In the past, the design of system stressed on functionality, thus cost lowering and efficiency facilitation are the main considerations. As Fintech starts to develop rapidly, business models are undergoing a metamorphosis, and designs of information security system should meet the requirements of Fintech era. Firstly, for instance, block chain is an operation model featuring decentralization whose greatest advantage is the high security, and all transactions rely on the dependability of codes and block chain's trait of being unable to manipulate, making a huge difference from the transactions in the past with centralized

managements by financial information systems of Central banks in countries. Many bank applications including trade finance, multinational payment and syndication have been provided with newly developed block chain applications, although the business values of such needs time to tell, the applications have replaced many traditional payments. For instance, in apps Alipay and WeChat Pay, we can find the functions of communications by social media, shopping site, withdrawal and deposit and payment in one application. Each function may involve different information security issue, for example, social media needs excellent personal information protection; payment system needs strong detection of financial crime control. Combining information security features needed by different functions into the same platform is a great challenge to information security developers. Therefore, an information security developer in the financial institute should have a profound understanding with new internet financial environment and Fintech to catch up with the information security level their institute needs.

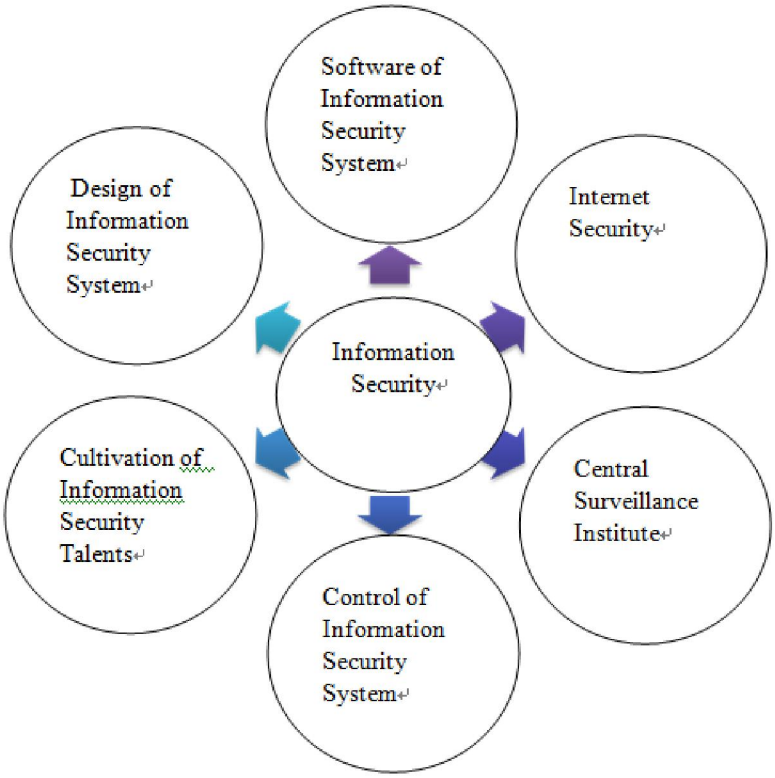

Figure 1: Conceptual Framework

System update

The ATM involved in this ATM attack incident is the 1500 model by Wincore, a model used for a long period. Besides the incapability to respond to intelligent and automatic transaction model in the future, it is also in need for major improvement in information security level. ATMs in the future will be evolved into VTM. More transactions will be completed directly via ATM, and identification and transaction features including verification needing signatures of clients, immediate renewal of passbooks and instant confirmation of purchase of financial products will be the priority for banks to stride into the Fintech Era. As the surge of WeChat and Alibaba strikes in the internet finance, most banks respond to such phenomenon by evaluation the values of branches meanwhile knowing the degree of acceptance by clients on Fintech. Should a branch be conserved after evaluation of its value, the functions for new models can be less wholesome; however, if the area of land is massive, for instance, the market in Mainland China and India, then using intelligent teller machines to offer more universal financial services will be the future trend, and remote security protection will become more important. Every bank is having its international finance development work in progress. New international finance will surely result in massive information security pressure to financial industry. Therefore, upon system updates, a more prospective planning is needed to cover the development of new technologies in the future.

System space

Although cloud storage for information and transaction processing becomes more and more common, however, as the advent of big data era comes, the information increases exponentially, additional to enough space, sufficient power as well as fireproof and quakeproof safety measures should be considered. Take Bitcoin as instance, during the data mining process, a great deal of power consumption can be expected, and each nation rushes to expand its mining capacity to claim their rights to keep accounts on block chains. For example, Mainland China locates their virtual coin mining center at regions with ease of access to solar power to offer the center cheap and sufficient electricity. At the same time, system temperature control and prevention to unnecessary loss caused by system interruption brought about by power interruption and natural disaster should be taken.

Process of system maintenance
As the information confidentiality in the future and security of system are the most important parts of information security, even an ordinary routine system maintenance should be treated with the high-class measures equivalent to semiconductor entering and exiting facilities and company by IT personnel in the company.

System outsourcing
To save costs, many enterprises outsource their information system-related affairs to information company of the external, from setup to maintenance. Nevertheless, since various information security issues have happened, contents of contracts should be under scrutiny once again. Firstly, whether the outsourced company with excessively small amount of capital can indemnify when major information security issues happen should be the important consideration factor a company determines their system outsourcing company, more than just cost and effectiveness consideration. Besides, the outsourced company, in most of the time, complies with access controls but has loose management on information of clients, which faces possible embezzlement or backup. Besides, time needed by the outsourced company to recover system operation should be regularly reviewed. Meanwhile, audit departments should perform irregular checks to outsourced company to ensure the operation quality of system.

Insurance for information security system
Cyber-attacks and risks of theft have become crucial risks for financial institutes. Besides facilitating information security clearances, obtaining insurance can be the extremely important part to prevent possible losses.

Software of Information Security
Instant checks performed anytime
Most attacks by hackers are personal information theft or access to users' accounts for deposit heist. After the ATM attack, Investigation Bureau, Ministry of Justice released the four APT Attack malwares (cnginfo.exe, engdisp.exe, sdelete.exe, cheanup.bat). The financial industry should, besides scanning their systems for the four released malwares, always stay alert with the new malware attack incidents occurring worldwide. The malware involved should also be listed on the program list for scheduled system scan. Current APT attacks remain latent in the company's system for some time and activate when suitable. Such period of time is the prime time for information security personnel to capture the attacking program. The bank industry can perform overall check to tens of thousands of computers via EDR (EDR, Endpoint detection and response).

White list
Programs and applications passing scrutiny and can be remained in the computer must be compared with system programs. The information security team should delete the rest of the programs excluded from the white list. Take ATM as instance, except for programs on the white list such as withdrawal, deposit and transfer, other programs aren't allowed to be stored on the ATM. In addition, the process of white list review should not be limited to ATM. The review should be performed on domestic and overseas systems of the bank and a list should be compiled for control. Plus, automatic scanning process shall be established. Programs not on the white list after scanning should be blocked and reported. Should a new program need to be added to white list, an official review process must be taken.

Validity of software
The operating system used in the teller machine involved in the ATM heist is Windows XP by Microsoft. In addition to the old system, the software developer has also suspended its system maintenance; hence, in the phase of system design, not only the hardware but also the software update and ability to protect the system should be taken into consideration.

Anti-virus software
Malwares usually go through steps of intrusion, diffusion, waiting and execution. Anti-virus software should build up strong firewall before the occurrence of intrusion and diffusion to prevent malware intrusion. And virus scanning software should detect and clean the intruded malwares in phase of waiting and execution. Usually, after the malware has accessed to the company's system, it will stay latent for a certain period of time, observe the operation of the company's internet security mechanism, find out who has been authorized and record the password of whomever has been authorized, which is the best timing for cleaning these malwares. Some companies use virus scanning software whose version is utterly old due to their lack of hacker encounter experience or reason of cost saving. No matter outsourcing to software company or system fortification by internal IT personnel, all needs to be sped up in the process. According to Symantec's internet threat analysis report, in the past 6 years, the number of mutated malware has multiplied by 184 times. Therefore, the information security in traditional concepts contains no capacity to react to new alien threats.

Internet Security
Auto sandbox
For external Email and internet uses, auto sandbox should, other than passive processes of screening and more, take actions to know what abnormal transactions are, such as abnormal magnifying of trading volumes in a short period and uses of internet or

external Email systems. It is found in the ATM attack incident that internet hackers constantly seek for opportunities to intrude into company systems via use of internet and Email. Once the original attached file goes on the black list, hackers will change the attached file into the normal names of attached files hardly recognizable. Thus, as hackers relentlessly change attack patterns, if we merely perform screening based on name of attached files and high-risk terms, we may fall into risks of being unable to follow hacker's techniques. From time to time, hackers will entice company users to open attachments containing malwares on social media platforms; thus, should one open the external attachments, the action shall be authorized and screened. Auto sandbox should screen the so-called "abnormal data", for instance, abnormal transactions inclusive of abnormal cash dispensing in a short period and uses of system at abnormal time by privileged users, and take those as points for intensive monitoring and management.

View of internet framework

The original design of internet framework is supposed to burden the responsibility of transmitting the company's internal information and documents and undertaking transaction. However, as the methods of transaction change, the connecting body, time, country and joints of internet framework should be redefined. For instance, whether the connection time among different systems should be available for 24 hours should be reassessed. Divisions on the internet and segregation are crucial. Segregations are as flooding in a ship's cabin, once segregated properly, cruise of the ship won't be affected; hackers won't be granted full access even after they hacked in. Segregation of host and setup of firewall are especially important. New connections to the host should be assessed with prudence and old connections should never be opened. For the one with greater influence, for instance, the emergency exit in the ATM Heist, the authorization level should be massively heightened and cannot be opened without grants by two or more authorization managers.

Authorization

To companies, different levels of authorized systems and authorization personnel of companies, meaning by whom can what system be used and authorization occasions should be regulated. For example, software companies usually leave a backdoor, and the backdoor cannot be opened except for emergency. Consequently, besides the manager of information security, COO and CRO of the company should be managers owning authorization rights to backdoor so as to open in proximity, to supervise the use of backdoor, and to ensure its closing. Moreover, the authorization occasion cannot be accessed via the Blackberry at home to prevent employees from exploiting the window of management in managers' leaves or typhoon day-off to open the evacuation exit and execute malware. Furthermore, the authorized personnel and password should be changed constantly.

Information security dashboard

For important data of information security, an information security dashboard should be established. The dashboard contains the overall information security status a manager needs for control, for example, risk index and information security early warning, and central monitoring institute needs monitoring marquee for instant display of information security incident. Take ATM as an example, since the machines are distributed in a vast area, the monitoring of abnormal volume and white list programs have strong remote monitoring effects.

Use of remote equipment

It becomes widely common for people to work at home, have flexible hours, attend a meeting via tablet computer and to read encrypted data through cellphone. As the equipment enhances convenience at work, it adds burden to information security tasks. When a company is faced with situation that numbers of employees using mobile devices of laptops, cellphones and tablet computers outside of the company, special regulations shall be made to lower the loophole and risks created by use of mobile device outside of company.

Central Monitoring Institute

Detect abnormal transactions

Abnormal transactions include fraud, false claim, manipulation of account information, financing terrorists, money laundering, client information theft, etc. Each abnormal transaction takes different ways to avoid. For instance, fraud usually involves finding management loopholes from shopping platforms including e-commerce and TV shopping for information theft and setting scams via overseas calls to complete the process. At this moment, to detect the abnormal action like information theft, the information security system should be equipped with extremely advanced identification capacity; what's more, in respect of anti-terrorist-financing and anti-money-laundering which attract banks' attention recently, the system should have the ability to have a clear hold on clients' cash flows and complex transaction type. For example, should a client's cash flow comes from sanctioned nations such as Syria, how the system can detect effectively and the ways to define valid parameters are utterly important. Once an abnormal transaction is found, an UAR (Unusual Activity Report) should be submitted and the Compliance should review the abnormal transaction. Even more, a report to Investigation Bureau, Ministry of Justice should help with detection of abnormal transactions to fully prevent financial crime from occurrence.

Stop abnormal transactions

When the system is hacked or the abnormal transaction is underway, whether the central control institute can immediate detect

and stop the abnormal transaction is important. For example, in the ATM attack, the malware has been hiding in the company's network for a long time, finding the perfect timing to commit crime. They were able to choose the typhoon night and period of card-free service system updates for commit due to observations for a long time. As tens of teller machines dispense bulk amount of cash simultaneously, whether the central control institute's system detects such abnormality and whether the notification is sent to manager's phone immediately are the highlights to be improved in the future. The prime guideline of immediate stops to handle abnormal transactions without affecting normal transactions online or via ATM by clients should be taken when the system abnormality is spotted. Otherwise, should a mega-sized international bank halt all transactions once it encounters system abnormality until the cause is found, rights and interests of clients as well as convenience brought by transnational system use will be massively affected.

Setup of surveillance system

The ATM attack case cannot be solved rapidly without the great help from surveillance system. The surveillance system we refer to here doesn't only contain cameras, it also includes monitoring mechanism surveilling abnormal access, abnormal use and abnormal program.

The information security management issue on software/hardware and internet contained in Research Question 1 can be solved with the above four components.

Control of Information Security

The structure of information security control

As shown in Figure 2, the level of information security control should reach the Board to obtain sufficient resources and attention. In the past, information security couldn't enter the main agenda in the board meeting. In the future, besides the classification of information security as important issue by the board, the risk management committee hosted by independent directors should regularly review the system validity and execution status of information security. The institute in charge of execution should be mutually hosted by COO who manages information system and backstage operations along with CRO, and management items should stress on internet security, credit risk, financial crime prevention and Fintech.

(1) Internet security: this has been fully discussed in this study.

(2) Credit risk: After many non-structured information has been transformed into the basic information of big data analysis, information security issues come along. Internet businesses utilize kinds of trading data in its ecology to provide credit line to banks through algorithm, which is totally different from the banks' existing credit method fetched by scoring of clients' financial statements. Nevertheless, as the internet businesses can serve multiple clients with rather little manpower, for example, the online commercial bank by Alibaba can process 200 thousand credit transactions and serve 2 million clients with 400 people, the similar credit technology will be used by banks undoubtedly. Nevertheless, as banks cannot obtain sufficient information for analysis, if the same algorithm is taken for credit, the other type of credit risk caused by information security issue will therefore come to existence. Thus, to prevent this type of risk, when a bank is undergoing the change of credit mode, it is advised to perform in both new and old methods and react with prudence.

(3) Financial Crime Prevention: Since transactions with alleged intention of money laundering have taken place in large financial institutes in domestic and foreign territories and they were penalized by U.S. government, financial crime prevention have become the emphasis of the other type of information security. When creating information system for fighting financial crimes, the required KYC (Know Your Customer) has a rather high standard. Information inclusive of clients' capital whereabouts, understanding of end beneficiary and past criminal records are the basic conditions for bank to effectively fight financial crimes. In the meantime, for suspicious transactions, the system shall be able to automatically report warnings, and enter the anti-money-laundering and anti-information-terrorism scrutiny before the transaction performs. In the phase of system design and function advancement, setup of relative features for fighting financial crime is a cardinal part of information security.

(4) Fintech: Information security should be able to keep up with the Fintech trend. In the information security control trend, Fintech is particularly set as emphasized item and needs full cooperation by sales manager in charge of Fintech and horizontal function managers with hopes to keep the pace with the trend, no matter it's information security issue generated by new internet platform, new product, bag data analysis technology, transnational payment or trade finance.

Based on the ways to "perfect in downside improvement and profiting simultaneously" raised in research question 2, we can refer to the control structure as shown in Figure 2. With the full cooperation by the managers of four major functions, COO, CRO and CCO can understand latest progress of Fintech development and therefore able to advise effective internet security control mechanism for cooperation and performance.

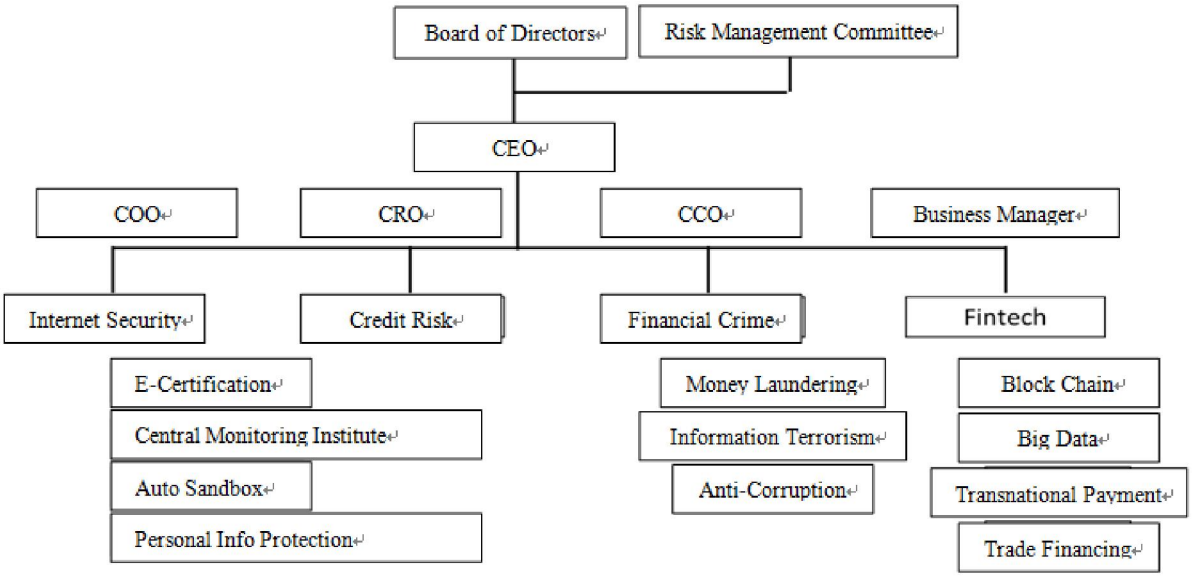

Figure 2: Control Structure of Financial Institutes

Audit

At the aspect of internet security, financial institutes should set three defenses. The first shall be system engineer responsible for instant checks and thorough records focusing on software, hardware and internet abnormality. The second is the defense by CRO, COO and CCO reviewing the check records compiled by the first defense anytime to understand whether there are new abnormalities. What's more, the reports shall be performed in the monthly risk management committee meeting. The last one is audit. The traditional audit shows limited capability to information security due to their non-information learning background. Nevertheless, as the information security incidents emerge nonstop and have become the operation risk of financial business owners, the audit authority should consider the possibility of employing audit employees with information background to ensure the audit quality. Meanwhile, the audit personnel should perform permeation testing to the system and the network for weak spot finding to ensure information security personnel will remind themselves of improving disadvantages.

Handling after attacks

After the occurrence of incidents, a set of full handling standards including evidence keeping and immediate report to authorities as well as internal managers in charge should be established, and drills shall be taken at all times.

Cultivation of Information Security Talents

Information security engineer

In a financial institute, IT personnel mainly take charge of system repairs. Soon, as information security becomes the main risk of financial industry, the specialized information security engineer should take regular views to every part of information security loopholes that may take place. Information security engineer should not burden other jobs and should focus on protecting the company's system and information security. Taiwanese system companies tend to provide free post sale services for business, which will majorly affect repair quality and working willingness of engineers. Businesses should change their mindset of "Free of Charge means Money Saving", after all, once the system is hacked, clients will lose faith to their system providers thus sabotaging the goodwill of system provider, causing losses greater than gains.

Cultivation of information security personnel

Besides the basic knowledge of software and hardware as well as internet, the company shall send their personnel to top-notch information security companies overseas or to banks with great information security measures for visits or on-the-job training. Knowing all types of emerging financial crime and different attack patterns by malware will enable the personnel to provide the best guaranteed information security.

Role of government

With regards to the role of government mentioned in research question 3, besides providing solid training and licenses related to information security to Academy of Banking and Finance Institute, Institute for Information Industry and more, the additional responsibility is to conglomerate the public's strength and resources. "Department of Cyber Security" of Executive Yuan was officially established in August, 2016 under the circumstances that information security issues result from miscellaneous factors and methods are renewed constantly, which a single institute cannot build a holistic information security system with its own strength. Therefore, the study intends to provide the government with advices to step up for compilation, enabling all the publics and financial business owners to live in a safe information environment.

CONCLUSIONS

Fintech changes over time, and new modes for financial crime have been renewed nonstop. The study discusses the six major components of information security, advising items the information technology can be improved. The most important thing shall be the change of managers' mindset. If information security is not well established, great harms to the goodwill of financial industry and clients' rights and interests will be made. To face the menacing internet business owners' competitions and development of Fintech, if relative information security prevention is taken into consideration, both can be handled, leading financial industry to embrace the new internet era with joy.

REFERENCES

[1] Chandrasekharan, B. (1986) 'Generic tasks in knowledge-based reasoning: high-level building blocks for expert systems design', *IEEE Expert*, Fall, pp. 125-164.

[2] Raychaudhuri, D. (1996) 'Wireless ATM networks: architecture, system design and prototyping,' *IEEE Personal Communications*, Vol. 3, No. 4, pp. 42-49.

[3] Johnson, A. L. (2016) 'Cybersecurity for financial institutions: the integral role of information sharing in cyber attack mitigation,' *North Carolina Banking Institute*, Vol. 20, pp. 277-310.

[4] Nakamoto, S. (2008) 'Bitcoin: a peer-to-peer electronic cash system,' Available at http://www.cryptovest.co.uk/resources/Bitcoin%20paper%20Or