International Journal of Engineering Materials and Manufacture (2020) 5(2) 62-67
DOI: https://doi.org/10.26776/ijemm.05.02.2020.05

Enhanced Information System Security in Internet Banking and Manufacturing

Saiful Islam

Received: 03 June 2020
Accepted: 22 June 2020
Published: 30 June 2020
Publisher: Deer Hill Publications

ABSTRACT
The internet has contributed significantly by changing the way of interaction among people and the execution of business today. By virtue of the internet, electronic commerce has been developed, enabling business to manage their customers and other organisations inside more effectively and outside their industries. The industry which is applying business transaction using this new communication pathway to reach its business clients is the banking sector. The electronic banking system identifies different emerging trends including providing service to meet customer's demand anytime and anywhere, importance of product time-to-market and increasingly complex back-office integration challenges. The challenges that internet banking is facing are providing information system security and protecting privacy of information. This paper will first discuss the current forms of security threats in the internet banking; secondly, it will investigate weaknesses in the current information security protocols of the internet banking. Thirdly, it will propose an enhanced information system security for internet banking.

Keywords: Information System, Security Risk, and Internet Banking.

1 INTRODUCTION
Banking is one of the oldest businesses known to humankind. Technology however have transformed and transitioned the traditional banking processes and strategies. Banking institutions have heavily invested in information technology in addition to other well-known systems such as telephone and branch banking. According to Rahi *et al.* (2018), banks have claimed information systems contributes to reduced operating costs and competitive advantage over rivals as some of the reasons for adopting information technology. Internet banking is the latest information technology infrastructure and has brought a 360-degree change in the entire finance industry. The adoption of internet banking has helped banks to offer real time financial transactions and helps in attracting and retaining customers. This is because banking institutions are now able to offer services at the comfort of customers that who would otherwise be needed to be physically present for transactions. The impacts of internet banking have been of interest to both business financial researchers and banking management. Ntseme, Nametsagang, and Chukwuere (2016) in a study of risks and benefits of online banking focused on the five advantageous factors of internet banking that is: accessibility, perceived security, self-efficacy, convenience, and usability. Ling *et al.* (2016) identified speed, convenience, 24hours banking as benefits of online banking. Even though banks in several countries have integrated security features, there is several internet security threats and vulnerabilities still continue to persist. As new threats continue to emerge, banks will need to adopt new measures to protect users. Banks can do more by deploying Information Security policies that ensure safer Internet banking experience. The purpose of this report is to evaluate the current forms of security threats in the internet banking, investigate weaknesses in the current information security protocols of the internet banking and propose an enhanced information system security for internet banking.

2 AN OVERVIEW OF INTERNET BANKING
According to Shaikh and Karjaluoto (2018), internet banking is a connection of banking systems that enable customers to get access to their bank accounts and other important banking details through the use of a website and without the inconvenience of attending physically to the bank, sending faxes, letters, or telephone confirmations. Internet banking has also been defined as a technological service which customers can request bank services such as opening of an account, funds transfer, balance inquiry, and online payments over the internet without leaving their homes or

S. Islam ✉
Kent Institute Australia Pty. Ltd. (Kent)
Level 10, Queen Street
Melbourne, VIC 3000, Australia
E-mail : saiful.islam@kent.edu.au

Reference: Islam, S. (2020). Enhanced Information System Security in Internet Banking and Manufacturing. *International Journal of Engineering Materials and Manufacture*, 5(2), 62-67.

organizations (Sundaram et al. 2019). Ramavhona and Mokwena (2016) stated that the key feature of internet banking is that it provides a universal connection from any location globally and it is very accessible from any internet connected computer. The convenience of internet banking is making more and more banks are integrating internet into their services to develop and expand transactional relationships with their customers (Ramavhona & Mokwena, 2016). Novokmet and Tokić (2016) identified three functional levels of internet banking that are currently employed in the banking industry as show in Figure 1.

- **Informational role-** Typically, the bank uses a stand-alone server to send marketing information over the internet to consumers about their products and services. This is usually the basic role of internet banking
- **Communicative level-** This role allows interaction between the consumer and the bank systems. The communication is often limited to loan applications, personal details updates (name and address updates) and electronic mail.
- **Transactional level-** this functional level allows bank customers to directly execute financial transactions. Usually, the most basic transactional system allow customer to only transfer funds between different accounts of bank. Today, the advanced transactional internet systems allow online payments directly to third parties taking the forms of electronic bank check, electronic money transfer, and bill payments.

Kalra and Narayan (2017) in a case study in India defined internet banking as a convenient form of banking where a bank account is usually maintained over the internet. The authors stated that the internet banking has a multi-dimensional advantage, which is both to the consumers and the banking institutions as shown in Table 1. Despite a lot of benefits of internet banking, there are some security threats exist in current internet banking system. Tabiaa et al. (2017) found that internet banking combines a lot of risks. The authors classified the risks into two parts; that is general and operational risks. The general risks are associated with physical equipment such as computers and server tools. The operational risks mean inadequate processes, eternal attacks, and failure of people and system. The operational risks are important to this study as they are a security threat to the provision of internet banking services.

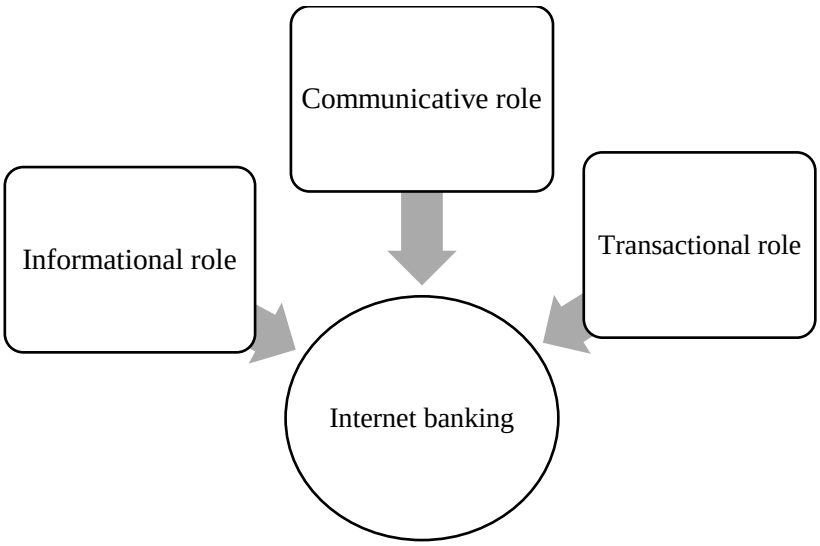

Figure 1: The three functional roles of Internet banking

Table 1: Advantages of internet banking to both customers and banks, Source: Kalra and Nayaran (2017)

To consumers	To the bank
• Ability to operate different bank accounts at the same time • Reduce time in executing different accounts operations • Save operations costs • Accessibility at any time in any geographical area	• Decrease in operational costs thus an increase in profitability • Less paperwork due to computerized administrative tasks • 24 hours income generation • Investment in personnel greatly reduced due to absence of physical agencies and investment in virtual banks

Table 2: Banks that have recently reported cyber-attacks. Source: Bouveret (2018)

Institution	Year	Type of attack	Details
Federal Reserve Bank of Cleveland	2010	Data Breach	Theft of 122,000 credit cards
Federal Reserve Bank of New York	2012	Data Breach	Theft of proprietary software code worth USD 9.5 Million
Sveriges Riksbank	2012	Business Disruption	Distributed Denial of Service (DDoS) attack left the website offline for 5 hours
Banco Central del Ecuador	2013	Fraud	USD 13.3 Million stolen from the account of city of Riodamba at the Central Bank
Federal Reserve Bank of Saint Louis	2013	Data Breach	Publication of the credentials of 4,000 bank executives by anonymous
Central Bank of Swaziland	2014	Fraud	Theft of USD 688,000.00
ECB	2014	Data Breach	20,000 email addresses and contact information compromised
Norges Bank	2014	Business Disruption	DDoS attack on seven large financial institutions, resulting in suspended services during a day
Central Bank of Azerbaijan	2015	Data Breach	Theft of thousands of bank customers' information
Bangladesh Bank	2016	Fraud	The SWIFT credentials of the Bangladesh Central Bank were used to transfer USD 81 Million from its account at the FRBNY. Hackers tried to steal USD 951 Million
Bank of Russia	2016	Fraud	21 Cyber-attacks aimed at stealing USD 50 Million from correspondent bank accounts at the central bank, resulted in a loss of USD 22 Million
Bank of Italy	2017	Data Breach	Hacking of email accounts of two former executives

3 CHALLENGES OF INTERNET BANKING

Internet banking has been emerged as one of the fastest and easiest way of banking. The threat of cyber security attacks become a great challenge for the Internet banking and electronic commerce (E-commerce) industries. Therefore, the security of this information system infrastructure is a major concern in the provision of effective banking services. The BBC News reported on 27 March 2015 that internet banking fraud rose by 48 percent in 2014 as compared to 2013 in the United Kingdom (More, Jadhav, & Nalawade, 2015). The rise was due to increased development of computer malware and con artists tricking online banking users to give personal details that is common online threat known as phishing. Another report by Business Insider India (Jan 5, 2015), revealed that the number of cybercrimes in India increased from 22,060 in 2011 to 71,780 in 2012 (More, Jadhav, & Nalawade, 2015). The report also noted that the increased use of mobile phone in financial transactions will increase the internet banking security vulnerabilities to a great extent. International Monetary Fund (IMF) in 2018 reported that more financial institutions around the globe are reporting cyber-attacks, data breaches, and frauds on their online services as shown in Table 2 (Bouveret, 2018). From this context, creating an information technology infrastructure that ensures optimized security of internet banking is critical.

The current internet banking system relies on Personal Identification Number (PIN) authentication and unencrypted short messages (SMS) and emails as the only security features in their Internet banking systems. Sundaram et al. (2019) further studied the current security protocols in internet banking and found that financial institutions use similar methods of authentication for all users. The measures employed ranged from telephone number, PIN, mother's maiden name, and simple passwords only systems. The problems with the structures now-a-days are inherent inside the setup of the communications and additionally within the computer systems itself. Hackers have many unique methods that they can access these security protocols of internet banking. Therefore, even though banking institutions have integrated security features in internet banking, the existing security protocols are not efficient.

While a significant number of Australians use internet banking, a large number continue to use bank conventionally. According to Australia Bureau of statistics (ABS, 2016), only 21 percent of Australian citizens are comfortable using the mobile banking despite having many benefits of online banking. Moreover, age is a determinant of using internet banking. ABS (2016) reported that 61 percent of Australian citizens age 15 years and above used internet in 2014 and 2015 and 72 percent of them used the internet for conducting banking transactions. On the other hand, only 49 percent of Australians aged 65 years used the internet and only a half used the internet for banking services. Security concerns are the core reason for lower adoption of internet banking in Australia. The groups who do not engage in internet banking have cited low trust in the system. At the same time, security remains a main concern for those who use the services in Australia. Given the many benefits of internet banking such as convenience, non-physical handling of money, speed, and cost reduction, this study will evaluate the current forms of security threats in the internet banking, investigate weaknesses in the current information security protocols of the

internet banking and propose an enhanced information system security for internet banking. As a result, individuals will trust internet banking and ensure many Australians benefit from the new technology.

4 SECURITY RISKS IN INTERNET BANKING

Khan *et* al. (2016) stated that internet banking infrastructure can be attacked with different skills and persistence. Communication and transitional roles of internet banking has been termed as the most vulnerable to security attacks. According to Reserve Bank of Australia (2018), the most common cyber threats in Australian Banks are data breaches by stealing sensitive data by means of phishing, system disruption such as denial of service (DoS) attack and financial attacks either through fraud or ransom. HSBC Australia stated in their website that the most common cyber-attacks in Australian Banks are phishing, Malware, Business Email Compromise, Text and phone scams. Australian Cyber Security Centre reported in 2016 that the most common threats in financial institutions are phishing and denial of service (DoS) attack. Internet Banking may face some security threats including Phishing, Denial-of-Service (DoS) attack, password cracking, Social Engineering attack, Man-in-the-middle attacks, and Man-in-the-Browser attacks.

4.1 Phishing

Khan et al. (2016) focused on phishing where fraudsters use the communicative level of internet banking to send fraudulent emails that are created with the intention to deceive the systems users to disclose personal information. Information including user passwords, PIN, social identification, and date of birth, and credit card details have also been critical details for phishers. The study reported that one-way fraudsters are phishing is done by developing a website that exactly resemble the original bank site. Once the customers enter their username and password, the attacker's systems store the details for use in the original website of the bank (Khan et al. 2016).

4.2 Denial-of -Service Attack (DoS Attack)

Tabiaa et al. (2017) stated DoS attack as the most common type of internet banking security risk after phishing. The authors described DoS as an attack where the cyber criminals make internet banking network unavailable to its intended users. They temporarily or indefinitely disrupt services of a host connected to a bank computer (Tabiaa et al. 2017). Khan *et al.* (2016) further stated that DoS attacks significantly degrade the internet banking service quality experienced by the legitimate users. The attackers inject and execute arbitrary code when performing a DoS attack to give commands to the server and access critical information from the systems.

4.3 Password Cracking

Veras, Collins, and Thorpe (2014) stated in a study of semantic patterns of passwords that cyber attackers can involve a guess work to obtain personal information from internet. The attacker often tries many passwords and passphrases with the hope of eventually guessing the password correctly. In password cracking, Tabiaa et al. (2017) revealed that cyber attackers check all possible passwords systematically until a correct one is found. Veras, Collins, and Thorpe (2014) stated dictionary attacks, pattern guessing, and word list substitution as the most common types of password cracking.

4.4 Social Engineering Attacks

Mouton *et al.* (2015) revealed that social engineering attack is more common with global connectivity of internet. This is the science of using social interaction to persuade an internet banking user to comply with a specific request from the attacker and the request involves a computer related trick. Airehrour et al. (2018) in investigating social engineering in the New Zealand banking system stated that cyber attackers use relationships and friendships to obtain information from their victims. The authors explored social engineering attack cycle which was first described by Kevin Mitnick (2002) as show in Figure 2.

4.5 Man-in-the-Middle Attacks

Kimwele *et al.* (2014) focused on studying threats associated with man-in-the- middle attacks in the mobile banking system. They found that this type of attack often targets the communicative level of internet banking which is normally achieved through SMS and emails. The attacker will intercept messages in a public communication server and then retransmits them, substituting the message to a new but related version so that the two original parties appear to be communicating with each other. Tabiaa *et al.* (2017) stated the attacker is usually a third party who has access to the communication channel between two end users. The attackers convince the two communicating parties that they have a secure channel but instead they access to all the encrypted messages.

4.6 Man-in-the-Browser (MitB) Attacks

A Man-in-the-Browser attack is performed by infecting a user browser with a browser add-on, or plug-in that executes malicious actions. Generally, the attacker can perform anything the user can and can act on their behalf once user's machine is infected with malware. The attacker can perform any bank transfer that the user does while infected if the user logs into their bank account at that time. By the virtue of being invoked by the browser during Web surfing, that code can take the control of the session and perform malicious actions without the user's knowledge.

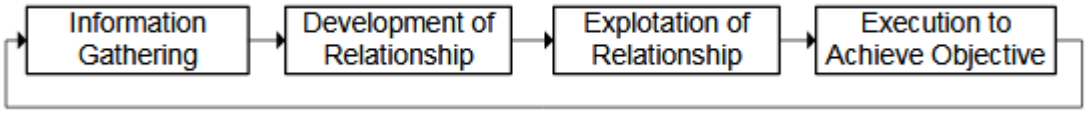

Figure 2: Social engineering attack cycle. Source: Airehrour *et al.* (2018)

5 RESEARCH METHODOLOGY

In this study, a survey was conducted in Australia as the research methodology. The targeted participants were bankers and internet banking users. The bankers were considered the most suitable informant, especially if these bankers also at a senior level in the overall organizational hierarchy. The questionnaires were sent to 200 participants and the response rate was good. 123 participants responded to this survey. The participants were asked about current forms of security threats in the internet banking, weaknesses in the current information security protocols of the internet banking and they were asked to propose an enhanced information system security for internet banking. Based on the survey's positive and negative responses, the security threats, and weaknesses in the current information security protocols in internet banking have been identified. Finally, an enhanced information security for internet banking has been proposed.

6 RESULTS AND IMPLICATIONS OF THE STUDY

The most common security threats in internent banking are not pure technical attacks. 71 participants mentioned that phishing is the main threat in internet banking and they mentioned that password stealing, identity theft, Denial-of-Service (DoS) attacks and Man-in-the-Browser (MitB) attacks are the other security threats. 52 respondents stated that Denial-of-Service (DoS) attack is the main security threat in internet banking while phishing, password stealing and identity theft are the other types of cyber attack in intenet banking. Therefore, the most security threats that are identified for internet banking in this study are phishing, password stealing, identity theft, Denial-of-Service (DoS) attacks and Man-in-the-Browser (MitB) attacks. Cyber attackers often steal and accses to personal and bank security details. Currently, banks have developed authentication protocols to mitigate cyber attacks in internet banking. An authentication is a method and a piece of information used to verify the identity of a person or organization when accessing networks with security constraints. The most common types of authentication in current online banking systems include, PIN, passwords, identifiable picture, one time password (OTP), finger and palm print, voice, signature, and facial recognition. Kayode *et al.* (2017) stated that the most common methods of authentication using in current internet banking have low to medium security strength. The authors revealed only Iris pattern have high security strength. Sheikh and Rajmohan (2015) stated now-a-days CAPTCHA is a common authentication protocol in internet banking. The authors however stated that the images used are too simple, making it very possible to obtain desired banking information using the OCR sofware.

This study recommends that Biometrics-based authentication is the enhanced security solution to address security issues in online banking. This is the use of personal physical and behavioral human features to identify the identity of internet banking user. Some common features used include voice, fingerprints, facial paaterns, and typing cadence. This type of authentication is not transferable as with the case in passwords, PIN, and mother maiden name. The findings of this study will challenge banking management to rethinks about their current authentication methods in online banking. The findings are also important for system developers who design and develop internet banking information technology infrastructure.

7 RELEVANCE TO MANUFACTURING INDUSTRY

Industrial production relies upon secure digital connections with vendors, partners, and customers to stay relevant and competitive. These digitally connected industry has significant amount of cyber risk. All that sensitive data, communication channel and automatic processes multiply the opportunities for hackers by expanding the "surface area" exposed to cyber-attack. Since digital systems are very much embedded in daily operations, the significant damage can be magnified from even a single security incident. Industrial business processes are automated, digitized and streamlined. This data-driven, real-time operation creates more risks from autonomous machines and processes. These risks could occur from robots to automatic warehouse equipment to information systems that automatically carry out work with outsiders. To manage risks, industry need to develop pervasive cyber resilience that weaving cyber protection into all operations they perform at present and plan to perform in future. This paper recommends cyber security solutions that can help industry to make them cyber resilient. Cyber resilient enterprises can operate safely under persistent threats and sophisticated attacks. They can strengthen customer trust and boost industrial production.

8 CONCLUSIONS

The number of cyber attacks have increased dramatically as more banks adopt internet banking. The technology have been adopted due to its benefits in increasing convinience of banking services, the potential to reduce operations costs in bank, and the perceived security. However, the current security models in mobile banking have some

weaknesses due to the persistent number of attacks. Common types of security attacks in online banking systems include phishing, denial of service attcks, password cracking, social engineering attacks, man-in-the-middle attacks and man-in-the-browser attacks. It is important that banks rethink their authentication strategies. The limitation of this research is that this study was conducted in a single country only. The future research may be conducted in broad geographical areas in the world.

ACKNOWLEDGEMENT

The author is grateful to the bankers and the internet users in Australia who participated in the survey as part of this research study.

REFERENCES

1. Airehrour, D., Vasudevan Nair, N. & Madanian, S. (2018). Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. *Information,* 9(5), 110.
2. Australia Bureau of Statistics (ABS, 2016). 8146.0 - Household Use of Information Technology, Australia, 2016-17. Retrieved from: https://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0
3. ACSC Threat Report. (2016). Retrieved from: https://www.cyber.gov.au/sites/default/files/2019-04/ACSC_Threat_Report_2016.pdf
4. Bouveret, A. (2018). Cyber risk for the financial sector: a framework for quantitative assessment. International Monetary Fund.
5. HSBC Bank Australia. (2020). Protecting Your Business, Cybercrime. Retrieved from: https://www.business.hsbc.com.au/en-au/cybercrime
6. Juraj Dobrila University of Pula. I. (2016). Adoption of Internet Banking Service within the Corporate Sector: Evidence from Newly Acceded EU Country. In the EU Economic Environment Post- Crisis: Policies, Institutions and Mechanisms. Juraj Dobrila University of Pula.
7. Kalra, R. & Narayan, B. (2017). E-Banking: Advantages, Challenges and Opportunities in the Indian Context. *Journal of management and technology*, 7(1).
8. Kayode, A., (2017). Internet Banking In Nigeria: Authentication Methods, Weaknesses and Security Strength. *American Journal of Engineering Research,* 6(9), 226-231.
9. Khan, M., Khan, K., Raza, A., & Khan, E. (2016). Analysis of Electronic Banking Services & Its Issues in Pakistan. *European Journal of Business & Management*, 8, 1-8.
10. Ling, G. M., Fern, Y. S., Boon, L. K., & Huat, T. S. (2016). Understanding customer satisfaction of internet banking: A case study in Malacca. *Procedia Economics and Finance*, 37, 80-85.
11. Luvanda, A., Kimani, S. & Kimwele, M. (2014). Identifying threats associated with man-in-the-middle attacks during communications between a mobile device and the back end server in mobile banking applications. *IOSR Journal of Computer Engineering* (IOSR-JCI), 12(2), 35-42.
12. More, M., Jadhav, M. & Nalawade, K. (2016). Online Banking and Cyber Attacks: The Current Scenario. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5, 743-749.
13. Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. *Computers & Security*, 55, 114-127.
14. Novokmet, A. K., & Tokić, I. (2016). Adoption of Internet Banking Service within the Corporate Sector: Evidence from Newly Acceded EU Country. In The EU Economic Environment Post-Crisis:Policies, Institutions and Mechanisms.
15. Ntseme, N., Chukwuere, J. & Onneile, J. (2016). Risks and benefits from using mobile banking in an emerging country. Risk Governance and Control: Financial Markets & Institutions. 6. 10.22495/rgcv6i4c2art13.
16. Rahi, S., Ghani, M. & Ngah, A. (2018). A structural equation model for evaluating user's intention to adopt internet banking and intention to recommend technology. *Accounting*, 4(4), 139-152.
17. Ramavhona, T. C. & Mokwena, S. (2016). Factors influencing Internet banking adoption in South African rural areas. *South African Journal of Information Management*, 18(2), 1-8.
18. Reserve Bank of Australia (Financial Stability Review). (2018). Box D- Cyber Risk. Retrieved from: https://www.rba.gov.au/publications/fsr/2018/oct/pdf/box-d.pdf
19. Shaikh, A. A. & Karjaluoto, H. (2015). Mobile banking adoption: A literature review. *Telematics and informatics*, 32(1), 129-142.
20. Sheikh, B. A. & Rajmohan, D. P. (2015). Internet Banking, Security Models and Weakness. *International Journal of Research in Management & Business Studies* (IJRMBS 2015), 2(4).
21. Sundaram, N., Thomas, C. & Agilandeeswari, L. (2019). A Review: Customers Online Security on Usage of Banking Technologies in Smartphones and Computers. *Pertanika Journal of Science & Technology*, 27(1).
22. Tabiaa, M., Madani, A. & EL KAMOUN, N. (2017). E-Banking: Security risks, previsions and recommendations. *International Journal of Computer Science and Network Security*, 17, 189-196.
23. Veras, R., Collins, C. & Thorpe, J. (2014). On Semantic Patterns of Passwords and their Security Impact. In NDSS.