Data and Information Security Issues and Challenges for Banking Sectors in Fiji

Goel Aman Lal
School of Information Technology, Engineering, Mathematics & Physics, The University of the South Pacific
Suva, Fiji
Goel.Lal@usp.ac.fj

Manpreet Singh
National Training & ProductivityCentre, Fiji National University
Suva, Fiji
Manpreet.Singh@fnu.ac.fj

Jashvir Bir
School of Information Technology, Engineering, Mathematics & Physics, The University of the South Pacific
Suva, Fiji Suva,
Jashvir.Bir@usp.ac.fj

2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE) | 979-8-3503-4107-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/CSDE59766.2023.10487755

***Abstract*— The Internet has played a key role in changing how we interact with other people and how we do business today. As a result of the Internet, electronic commerce has emerged, allowing businesses to more effectively interact with their customers and other corporations inside and outside their industries. The internet can be seen as a truly global phenomenon that has made time and distance irrelevant to many transactions. One industry that is using this new communication channel to reach its customers is the banking industry. The transformation from traditional banking to e-banking has been a leap change. The electronic banking system addresses several emerging trends such as 'customers' demand for anytime, anywhere service, product time-to-market imperatives and increasingly complex back-office integration challenges. However, the increase in the use of ICT facilities results in the increase of criminal activities like spamming, credit card frauds, ATM frauds, phishing, identity theft, denial of service and other security bridges have lent credence to the view that ICT is contributing to crime in the banking sector. The challenges that oppose electronic banking are the concerns of security and privacy of information. This study discusses security issues associated with internet connectivity, focusing on three main areas: confidentiality, integrity, and availability of information. Vulnerabilities that companies are exposed to, such as a virus, malware, phishing, Trojan horse, exposes a 'company's information assets to attacks. It also discusses preventive measures that organizations should implement in order to protect a company from such threats. Finally, recommendations are made for the decision-makers to consider when making decisions regarding data and information security on financial organizations.**

Keywords— Confidentiality, Integrity, Availability, Online Threats, Computer Crime, Information Security, Formulate Policies.

I. INTRODUCTION

The 21st century is invariably been equated to the Digital era which has witnessed high proliferation and permeation of ICT in all aspects of human livelihood, endeavors and aspirations. ICT continues to bring about new initiatives, innovations, tools and technologies covering a wide spectrum of areas such as robotics and automation [1], [2], education [1], [3], [4], [5], rescue missions [6], finance and security [7], [8], intelligent vehicle and transportation systems [9], [10], [11], [12] , gaming and simulations [13], [14] to name a few prominent ones. Organizations today also know that information technology is essential for not only the missions and advancements from such domains mentioned but also for gaining a strategic advantage in the marketplace. These have also placed a huge importance on the need for ICT skills and competencies world-wide, with academics and researchers investing a lot in designing and implementing the best suited programs, curriculum and interventions to educate and upskill the especially the students and the workforce [15]. However, the growing usage of ICT and growing ICT competencies of people has brought to light another related attribute [3]. It is argued that the importance of information technology invariably means that information security has also become very important. According to [16], [17], and [18], breaches in information security can result in litigation, financial loss, damage to brands, loss of customer confidence, loss of business partner confidence, and can even cause the organization to go out of business [19].

Data breaches and cybersecurity crises are top concerns for today's larger organizations. Unfortunately, small and medium-sized businesses are not safe from such attacks, either. [20] and [16] mentioned in the Cybercrime Magazine that sixty percent of small companies go out of business within six months of falling victim to a data breach or cyber attack. These businesses have failed to adequately protect themselves from online threats. With both the financial security and future of the business on the line [21], it is crucial for organizations of all sizes to have measures in place to monitor suspicious network activity.

Security issues or threats to an organization cannot be avoided. [22] and [23] state that threats comprised of motive, access, and opportunity or outsiders having a desire to cause damage as well as a means of affecting the target system. While an organization's exposure to risk can never be completely eliminated, all steps should be taken to minimize exposure and limit the scope of the damage.

Tom Keenan, a professor at the University of Calgary, stated that threats could come from anywhere and anytime. For instance, in the United States, three North Korean hackers [24] were indicted for allegedly creating and deploying multiple cryptocurrency applications to steal and extort over $1.3 billion cash from financial institutions and businesses [25]. Another prime concern was when [26] reported that a hacker tried to poison the water supply of Florida city by remotely penetrating a computer-controlled water treatment system and increased the amount of sodium hydroxide (lye). Luckily, the plant operator saw an attempt and reduced the level to normal and disabled the remote access program.

The ever-growing list of security breaches and threats worldwide has attracted the attention of organizations and prompted them to invest in comprehensive data security, including professional education and training for Data and Information Security [27], [28]. Organizations have implemented policies and procedures that may protect them against security issues and vulnerabilities associated with internet connectivity [17]. This includes the implementation of security architecture which provides risk management for the institution and coordinates the controls that reduce that risk.

In the era of the Internet of Things, developed countries have practically transformed the conventional household items, educational tools and office equipment into internet-enabled smart devices for added convenience and ease of use [29]. The fact that so many devices are interacting in real-time with users in cyberspace makes users more vulnerable to cyber attacks than in the past [30].

Security challenges such as IoT Top Security Concerns: Device Cloning, Sensitive Data Exposure, Denial of Service, Unauthorized Device Access and Control, Tampering Data are evident with the increasing use of IoT [31].

While Fiji has been subject to cyber attacks in the past [32], [33], the recent cyber-attack on Fiji's government website is a clear indication that the pacific, particularly Fiji, being the technically hub of the pacific islands faces imminent threats [33]. As such, financial organizations are presented with new cyber threats every day. There is a dire need for a thorough evaluation of all existing cyber security mechanisms to be tested, and new, needful solutions to be developed.

In this paper, the main contributions are as follows:

- Presenting a detailed and organized view of data and information security concept with recent computing threats globally and locally in Fiji. To the authors' knowledge this is one of the first baseline studies conducted in the area of data and information security for Fiji.
- Exploring the different attacks focusing on three main areas; confidentiality, integrity and availability of information in the banking sector.
- Determining the challenges faced during the acceptance of e-banking.
- Providing top six recommendations specifically imperative to the banking sector security issues and vulnerabilities.

The rest of the paper organization is as follows. Section 2, discusses Information security and evolving cybersecurity threats, presenting some international, regional and local cases of attacks in the financial institution. Section 3, 4, 5 categorizes and discusses the core CIA Triad (Confidentiality, Integrity, Availability) of information security. Section 6 and 7, provides main threats and vulnerabilities in banking and finance sector that affects important aspect such as internet banking, e-commerce, and credit card. Section 8, impact on bank and finance sector are introduced. Then in Section 9, control measures bank sectors should take are discussed. Then, Section 10, presents the authors' recommendations that are imperative for the banking sector and possible mitigation solutions. Finally, conclusions are presented in Section 11.

II. Information Security Issues

In the context of a changing global banking landscape, where branch networks are shrinking, volumes of digital payments are increasing, and payments are being processed in seconds, fraudsters and scammers are creatively finding new ways to steal from banks and their customers [34]. Security is a fundamental requirement for all banks as customers expect their investments, personal information, and credit details to be secure [35]. While most fraudulent activities are currently related to cards and payments, identity theft [26] and account breaches are also on the rise. As a result, information security in the financial sector is paramount [35], [37].

The Cyber Security Annual Report by [38] confirms that more than half a billion Facebook users' records were found exposed on unprotected Amazon cloud servers [39]. The exposed data sets were collected and insecurely stored online by third-party Facebook app developers. In relation to the Asia Pacific, the report also highlighted that the personal medical data of nearly one million people in New Zealand was exposed in an intrusion to the systems of Tu Ora Compass Health organization. A hacker under the name of "Vanda The God" [40] threatened to sell the information. Investigations revealed the systems were hacked on four different occasions [38]. Cyber exploits are more sophisticated, illusive, and targeted than ever before. With cybercrime rates estimated to have generated US$1.5 trillion in 2018 [41], navigating today's complex cyber threat landscape requires comprehensive cybersecurity. Computer Cyber Security Annual confirms that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting. This presents an example of the huge amount of loss organizations have to go through due to poor information security issues.

According to [42], a host of new and evolving cybersecurity threats has the information security industry on high alert. Ever-more sophisticated cyberattacks involving malware, phishing, machine learning and artificial intelligence, cryptocurrency and more have placed the data and assets of corporations, governments, and individuals at constant risk. A study by [43] recommends that all employees, from the senior management to the junior subordinate, have the responsibility to protect organizational information from such threats. Top management members are accountable to play imperative roles in steering information security programs to ensure the confidentiality, integrity and availability (CIA) of valuable organizational assets are protected. They should be more involved to allow information security to become an intrinsic part of corporate governance.

The pervasive use of the internet indicates that the impacts of information security are far far-reaching and anyone can be vulnerable from global to pacific to our nation. In 2017, the Association of Banks of Fiji had indicated the discovery of a skimming device at an ATM (Automated Teller Machine), whereby fraudsters were gaining access to customer bank card details through ATM skimming devices, hand-held skimming devices and online shopping sites [44], [45] .

A card scanner is physically installed inside the ATM. When a customer inserts a card to access cash or makes a payment, the skimming device scans the card and captures the card number. A secondary camera or overlayer is also installed to capture the client's ATM PIN or an overlay number pad inserted, which can also capture the PIN of the card as the client punches the card number using the secondary number pad [45]. These are the two methods of illegally accessing the client card details.

Fiji Financial Intelligence Unit (FIU) director Mr. Razim Buksh detected the first skimming device case in 2003 [46]. Since then, an increasing rate of the same type of attack has been taking place. For example, from June to December 2015, more than 500 credit and debit cardholders were affected due to the attack [47].

[46] also reported a major email compromise and email spoofing cases in Fiji where in March 2018, an email account of a local bank customer was compromised, and a fraudulent payment instruction was sent to the local bank.

— Approximately FJ$575,000 was transferred to a foreign bank account belonging to a cybercriminal syndicate [46], [44].

— In September 2018, in a case involving cyber money laundering, FJ$556,000 was fraudulently transferred from a local business bank account to an offshore ""incorrect"" bank account number. In this case, the foreign 'supplier's business email was compromised [46], [44].

— In October 2018, proceeds of approximately FJ$27,000 from the sale of investment shares of a local investor residing abroad were remitted to a cybercriminal's bank account in another country as a result of email compromise of the investor [46], [44].

— In October 2018, an estate property settlement proceeds totaling approximately FJ$845,000 was remitted to the foreign bank account of a cybercriminal who pretended to be the beneficiary of the estate. It appears that the email accounts of the beneficiary and local party were compromised.

— Since 2014, 39 businesses and individuals have lost funds totaling $5 million in foreign remittance transactions to cybercriminals through email compromise scams. Only $169,000 was recovered [46], [44].

Every security control and every security vulnerability can be viewed considering the core CIA Triad of information security:

- Confidentiality,
- Integrity and
- Availability

III. Confidentiality:

Confidentiality measures protected information from unauthorized access and exploitation. The banking sector houses information that has a high degree of sensitivity. “Confidentiality" refers to limitations of information access and disclosure to authorized users and preventing access by or disclosure to unauthorized users. In other words, confidentiality is an assurance that information is shared only among authorized persons or organizations. [35], [48] and [21] state that maintaining confidentiality protection is most important to businesses such as banks which keep financial information of their clients. According to [48], a 'bank's duty of confidentiality is a cornerstone of banking law. The information available to a bank with regards to its customers is often used in the daily operations of the banks and Fiji, bank secrecy is governed by ss.27 of the Banking Act 1995 [49], which clearly defines the confidentiality of information. Privacy issues have received an increasing amount of attention in the past few years, placing the importance of confidentiality on protecting the personal information maintained in automated systems by government agencies and private-sector organizations.

[36] stated that a crucial aspect of confidentiality is user identification and authentication. Identification of each system user is essential to ensuring the effectiveness of policies that specify who is allowed access to which data items. Accessing important information by the wrong group of users can lead to data manipulation and millions of dollars to the concerned organization [4]. Therefore, confidentiality must be well defined, and procedures for maintaining confidentiality must be carefully implemented. For Westpac Banking Corporation Fiji, its clients' personal information is protected and bounded by the Australian Privacy Act 1988 of Australia '('Privacy 'Act').

Confidentiality is related to the broader concept of information privacy: limiting access to 'individuals' personal information. Authentication methods, like user IDs and passwords that identify users, can help reach confidentiality. Other control methods support confidentiality, limiting each identified 'user's access to the data 'system's resources. Additionally, critical to confidentiality (also to integrity and availability) are protection against malware, spyware, spam, and other attacks.

IV. Integrity:

The challenge of any security program is to ensure that data is maintained in the state that users expect. A critical requirement of commercial data processing is to ensure data integrity to prevent fraud and errors. The concept of “Integrity" relates to the trustworthiness of information resources. It is used to ensure that information is sufficiently accurate for its purposes. The information should be authentic and complete. Although the security program cannot improve the accuracy of data added by users, it can help ensure that any changes are intended and correctly applied [50], [48]. An additional element of integrity is the need to protect the process or program used to manipulate unauthorized modification data. It is imperative, therefore, that no user be able to modify data in a way that might corrupt or lose assets or financial records or render decision-making information unreliable.

Examples of commercial systems that require a high level of integrity include credit reporting systems, production control systems, and payroll systems. As with the confidentiality policy, users' identification and authentication are key elements of the information integrity policy. Integrity depends on access controls; therefore, it is necessary to positively and uniquely identify all persons who attempt access [50].

[50] and [48] further identified that banks utilize a fusion of authentication, encryption and auditing mechanisms to assure that there is the safeguarding of the privacy, confidentiality, and integrity of transactions and information that is exchanged, disclosed, shared, stored, or used in online banking systems. The combinations of these mechanisms function as a formidable barrier to guard against the penetration and abuse of systems in any form. Among the mechanisms used are:

- secure sockets layer (SSL) channel
- 128-bit Encryption
- username & password protection and authentication
- firewalls, and
- account-locking

Series of independent security audits are conducted to ensure that all mechanisms are systematically tested to protect and safeguard against known security issues and prevent any form of tampering or theft of information or threats to transactions.

V. Availability:

The third part of CIA Triad is Information availability. “Availability" means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe. [51], [50], [48], [36] discussed that threats to information availability are:

- Denial of service.
- Loss of data processing capabilities because of natural disasters (e.g., fires, floods, storms, or earthquakes) or human actions (e.g., bombs or strikes).

Physical, technical, and administrative issues are important aspects of security initiatives that address availability [51]. Considerable effort is being devoted to addressing various aspects of availability. The availability of network components that achieve security strategies such as WAF, IPS, IDS, external firewall, internal firewall, DDoS protection device, DMZ, application layer and security layers and perimeter defense are the paramount solution to mitigate risks. A sign that availability is a primary concern is that increasing investments are being made in disaster recovery planning combined with alternative-site processing facilities [51]. In addition, [51], [52] states that known threats to availability can be expected to continue and new threats may emerge as technology evolves, making it quicker and easier for users to share information resources with other users, often at remote locations [19].

VI. Main Threats and Vulnerabilities in Banking and Finance Sector That Affects Important Aspect such as Internet Banking, E-Commerce, and Credit Card

The way of conducting banking transactions by clients has been changed by using electronic banking services, and accordingly, there is less need to visit the bank personally to perform activities of banking [53]. However, there is a need to assess the threats and vulnerabilities impacting the online services of a bank. According to [54], security is a major problem in the adoption of internet banking and approximately 72% of respondents in their survey stated that they are concerned about the safety of access to financial data on a mobile device. As the various researches from around the world give credence to these challenges, the situation is the same for Fiji where threats and opportunities arise faster and more often after it has embraced internet banking [33], [32].

In the research by [54], the types of attacks that affect online and mobile banking are indicated as follows:

- Social Engineering: It is the most commonly used attack type that does not require any computer system. Social engineers can identify themselves as bank representatives or system administrators and may get sensitive information from the user. Social engineering is one of the most effective phishing methods. Voice phishing (vishing) specifically targets mobile applications and in 2014, UK bank customers lost $24 million from vishing attacks.
- Port Scanners: Attackers can use port scanners to identify entry points to a system. The main purpose of a port scanner, to collect information about hardware and software that the system is running, thus an attack plan can be developed by the attacker.
- Packet Sniffers: Connection between a user's computer and a web server can be sniffed to collect a large amount of data about the 'user's credit card information and passwords. It is advisable to use a Secure Socket Layer connection to prevent this attack.
- Password Cracking: Brute Force is one of the most important password cracking attacks in breaking non-strong passwords. Other password cracking methods use hash tables to decode password files.
- Trojans: In terms of E-Commerce security, Trojan software is considered the most harmful attack. Trojans can be installed to track e-mails, instant messages, database communications, and many other services.

VII. Other Internet Banking Vulnerabilities

Weak passwords are one of the easiest ways for hackers to break into a system. Users normally choose something easy to remember (and as such, easy to guess or crack) and use it for all website credentials [55]. Moreover, users dislike changing their passwords and will use simplistic recycled variations of the same password if forced to do so. If a hacker manages to steal a password from an insecure site, he can access any account that the password unlocks [56].

Another vulnerability can be in the form of a lack of relevant education, awareness and training of staff but also the need for continuous upskilling in light of the dynamic nature of the banking sector and its threats. The biggest threat comes from insiders'. Given the extensive use of information technology by banks, the risk of unauthorized access, disclosure, and information modification by insiders or employees of banks is high. Even unintentional errors could have undesirable implications [53]. [54] states that ""many, if not most, inside breaches, are neither caused by disgruntled employees nor by student interns on harming. The sources are people who either are not aware of the security threats or are wrongly relying on someone else to deal with them or are not adequately skilled to address them. Unfortunately, potential intruders are all too aware of this human vulnerability and they take advantage of it in a big way.

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing attack refers to the most defiant security threats that are often perpetuated by conning user's information, whereby personal information is inadvertently disclosed, sensitive information is deleted, and other related resources are destroyed. [57]. Customers are directed to a fraudulent replica of the original institution's website when they click on the links to enter their information, and so they remain unaware that fraud has occurred [53]. The fraudster then has access to the customer's online bank account and the funds in that account. In some cases, pop-up windows appear in front of a copy of a genuine bank website. The real website address is displayed; however, any information that is typed into the pop-up directly goes to unauthorized users [57], [53].

The attacker can also install a Trojan, such as a key logger program, on a 'user's computer. This happens when users visit certain websites and download programs. As they are doing this, the keylogger program gets installed in parallel on their computer without their knowledge. When users log into their 'bank's website, the information keyed in during that session will be captured and sent to the attacker. Here, the attacker uses the Trojan as an agent to piggyback information from the 'user's computer to his backyard and make any fraudulent transactions whenever he wants. [40], [38].

Furthermore, in the Man-in-the-middle attack, the attacker creates a fake website and catches the attention of users to that website. Normally, the attacker can trick the users by disguising his/her identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website, users do not realize that they actually go to the 'fraudster's website [46]. The information keyed in during that session will be captured and the fraudsters can make their own transactions at the same time. [40]

In addition, email spoofing, which refers to an email that appears to have originated from one source when it was actually sent from another source, is another threat from hackers [47].

Attacks involving malware are a factor in online financial crime as well. Malware is the term for maliciously crafted software code. They replace a 'bank's legitimate website with a page that can look identical, except that the web address will vary somehow. Such a ""man-in-the-middle attack"" site enables an attacker to intercept user information [46]. The attacker adds additional fields to the copy of the web page opened in the browser. When an individual submits the information, it is sent to both the bank and the malicious attacker without his/ her knowledge.

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently [40]. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying the service of the system to legitimate users. [52] mentions that although a DoS attack does not usually result in the theft of information or other security loss, it can cost the target person or company a great deal of time and money. A denial-of-service attack can also destroy programming and files in affected computer systems. In some cases, DoS attacks have forced websites accessed by millions of people to temporarily cease operation [40], [51]. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks and credit card payment gateways.

VIII. Impact on bank and Finance sector

According to [61], when an attack occurs, the time and efforts of IT staff are devoted to dealing with the problem instead of managing other IT operational and security priorities. This leaves financial institutions open to more dangerous attacks that further compromise their infrastructure. [48]

Classified data and information are compromised when vulnerabilities are exploited. These data may be in the form of customer and employee details and critical bank information, which are crucial to the bank's continuous operation [44]. If information security policies and procedures are not implemented and enforced, the banks will likely divert more IT resources [38], [43] towards resolving these security attacks. Consequently, the systems are exposed to further and maybe more serious attacks that subsequently lead to further financial losses and curtailed reputation.

For example, when bank websites are disrupted, customers are frustrated as they cannot access their online accounts. Slow responses to website outages caused by bank cyber-attacks may lead to the loss of bank website customers.

The technology risks have a direct impact on a bank as operational risks and can also exacerbate other risks like credit risks and market risks. Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security-related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks [48].

IX. Control Measures Bank Sectors Should Take

Determining the exact requirements for security for a given organization is essential for implementing the proper security measures. Such measures are designed to protect information systems from security breaches. Banks in Fiji and beyond should put in place an information security policy and review it periodically. Without policies, standards, procedures, and guidelines, there is no general security framework or foundation, therefore, exposing gaps and opportunities for frauds and scams. The policy establishes technology selection and how it will be configured and implemented. Policies are the consensus among people, especially important between all layers of corporate management. The policy can ensure that the security manager and his or her peers apply security technology with the proper emphasis and return on investment for the good of the business [49].

For example, banks should conduct thorough background checks before hiring employees. Appropriate recruitment procedures can prevent the hiring of people who are likely to violate security policies. A thorough background investigation should be conducted, including checking the applicant's criminal history and references. Although this does not necessarily screen individuals for honesty and integrity, it can help identify areas that should be investigated further.

As stipulated in all banks' policies, standards, procedures and guidelines, the key to protecting an internet banking account is selecting a strong password and protecting it. Implementing a strong password policy includes developing and enforcing the policy and educating employees about how they should be protecting their passwords. Using a strong password will decrease hackers' likelihood of cracking the password and gaining access to the account. It should be ensured that the password to access the company's accounts is not the same as any other password used since not every site maintains the same level of security a bank does. Thorough control of passwords is an easy and effective first step in maintaining and protecting information Security [44] [40], [38].

The Internet banking system needs to be secured by using industry-standard methods that ensure the privacy of transactions during transmission. One such method is through the use of Encryption [50], [37]. All communication between the 'customer's browser and the Internet banking sites should be encrypted using encryption technology to ensure confidentiality, integrity, and authenticity of transactions performed on the site.

Lastly, the 'scramble pad' feature can be included in the Internet banking login page to help protect information entered at the customer's access control systems. Scramble pad is where the letters are scrambled to different numbers each time user logs on so that each logon appears unique. Using the scramble pad becomes more difficult for key-logging viruses, which may have been inadvertently downloaded onto the customer's workstation, from compromising their access codes. The use of the scramble pad enhances customer information protection and reduces the possibility of unauthorized transactions occurring on their accounts.

X. Recommendation

Measures to be taken for security risks are important after understanding the security vulnerabilities in the banking sector. Listed below are our top six recommendations that banks in Fiji should apply. These recommendations are equally relevant to banks in other developed and developing countries.

1) ***Management Support for IT Security Policy:*** *[*43] states that ""management support for proper security software implementation, configuration, continued maintenance, and research and development of new security technologies is critical"". The CEO must sign a formal security policy to confirm that the company is not only concerned about security, but the relevant security policies are duly implemented and followed with constant monitoring and periodic reviews. The management must ensure that all staff members understand and comply with the policy and such responsibilities need to be laid out in the policy itself to remove any misunderstanding [43].

2) ***Implementation for IT Security framework Standards:*** Security policy and requirements must be followed by all stakeholders. [51] highlights that ""Not only is the job not done once the policy is written, but ensuring that every employee, customer, vendor, constituent, or stockholder knows and understands policy is essential. Training and upskilling employees on company policies and keeping records are critical. In addition, the consequences of security breaches should be specified and published. All those involved should be made aware that (intentional or unintentional) disregard for security requirements will incur disciplinary safeguards. To underline this, in each case it should be clearly noted (for example, in the organization's security policy) what consequences may be expected "IT security is an ongoing process." This statement sums up the core problem: most of the tasks associated with IT security must be repeated regularly. Every safeguard identified should be examined to establish whether it needs to be implemented only once or must be repeated at regular intervals. [39].

3) ***Banks should have formal procedures in place for data backup and recovery:*** This is to ensure they have access to essential information in the event that data has been lost or compromised. Organizations that implement information backup correctly and periodically, will experience minimal downtime and smooth recovery in the event of a failure [50].

4) ***Build and Implement a Security Awareness Program:*** Organization needs to develop a plan to ensure all its employees have the knowledge they need to make the right decisions and set up the infrastructure necessary to share new threats as they emerge and get everyone invested in organizational security. The bank needs to train Employees to recognize Phishing and Social Engineering Attacks. Apart from these, the National Training Productivity Centre of Fiji National University offers a range of industry-based IT-related courses focusing on security. Some of these courses include:

a. IT Security Awareness Training,

b. CompTIA Security+,

c. Essentials of Network and Systems Administration,

d. Windows Server Administration,

e. Disaster Recovery and Business Continuity Planning.

5) ***Increase Prescriptive Approaches to online threats and vulnerabilities:*** Preventative measures already in use include firewalls, antiviral and anti-malware applications and vulnerability scanning. However, defences can be boosted by implementing other intelligence-driven measures, such as the use of artificial intelligence (AI), already applied in strengthening authentication methods via biometric logins for multi-factor authentication (MFA). One example is the use of fingerprints to verify payments from digital wallets such as Apple Pay or Google Pay [51]. Another instance is the combination of AI and Machine Learning (ML) to detect and prevent potential phishing threats (which are one of the most common cyber-attacks on banks) in real-time.

6) ***More Complex, Sophisticated security measures and technology investment:*** As the world becomes more digital, security measures need to be more complex and sophisticated than ever, while also being constantly updated. The technologies that protect against external threats can be used alongside other measures to address internal threats such as employee errors and outdated legacy systems. Deep learning models have found to be effective in creating strategies for better cybersecurity [52]. But most importantly, firms need to instil a culture that keeps data secure is everyone's job, including employees and customers.

XI. Conclusion

To conclude Internet connectivity can be extremely valuable to a banking organization in Fiji, but using it involves many security risks. Information security is not just about technological controls but also managerial and administrative controls.

Security cannot be achieved solely through the application of software or hardware. Any attempt to implement technology controls without considering the cultural and social attitudes of the Fiji corporation is a formula for disaster.

Although the paper has been reviewed thoroughly, there are some limitations in terms of collecting precise information due to the nature of the selected topic security. The businesses in Fiji have been interviewed however confidentiality is strictly maintained to avoid any vulnerabilities. Regardless to say, this paper sets a benchmark framework for future researches to strengthen the security issues in the South Pacific.

The best approach to effective security is a multi-layered approach that encompasses both technological and non-technological safeguards. Ideally, these safeguards should be used to achieve an acceptable level of protection while enhancing business productivity. Security technology alone cannot eliminate all exposures. Therefore, security managers must integrate themselves with existing corporate support systems so together with their peers, they should develop security policies, standards, procedures, and guidelines that form the foundation for security activities. This approach will ensure that security becomes a function of the corporation and not an obstacle to business. There is no silver bullet, and any array of measures taken can be through dialogue and in reference to policies and standards, which of course is missing at the moment in Fiji.

As discussed, the information security attacks of a banking organization's assets have a high dollar impact, business disruptions, loss of customer confidence, and negative business reputation.

Implementing the most appropriate security measures in organizations assists organizations to protect their information assets and reduce security vulnerabilities. Therefore, information places the most important role if there is a bridge by an intruder into the banking system immediately the firewall must be strengthened and message alerting the clients of such attacks took place. Practically, the strategic decision-makers of the banking industry especially of Fiji need to develop more stringent information security strategies that will increase the adoption of internet banking in Fiji. As authors [51], [39] mentioned that with more services being offered online and increasing the risk of data breaches, there is now a greater emphasis to examine the importance of information security in the banking sector.

REFERENCES

[1] K. Kumar, B. Sharma, G. J. Khan, S. Nusair and K. Raghuwaiya, "An exploration on effectiveness of anonymous peer assessment strategy in online formative assessments," in 2020 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2020.

[2] A. Prasad, B. Sharma and J. Vanualailai, "A new stabilizing solution for motion planning and control of multiple robots," Robotica, vol. 34, no. 5, pp. 1071-1089, 2016.

[3] P. Reddy, K. Chaudhary, B. Sharma and D. Chand, "Contextualized game-based intervention for digital literacy for the Pacific Islands," Education and Information Technologies, 2021.

[4] P. Reddy, B. Sharma and S. Chandra, "Student Readiness and Perception of Tablet Learning in Higher Education in the Pacific- A Case Study of Fiji and Tuvalu: Tablet Learning at USP," Journal of Cases on Information Technology (JCIT), vol. 22, no. 2, pp. 52-69, 2020.

[5] B. Sharma, P. Reddy, E. Reddy, S. Narayan, V. Singh, R. Kumar, R. Naicker and R. Prasad, "Use of Mobile Devices for Learning and Student Support in the Pacific Region," in Handbook of Mobile Teaching and Learning., Springer, Berlin, Heidelberg, 2019.

[6] S. A. Kumar and J. Vanualailai, "A Lagrangian UAV swarm formation suitable for monitoring exclusive economic zone and for search and rescue," IEEE Conference on Control Technology and Applications (CCTA), 2017.

[7] A. Fehnker and K. Chaudhary, "Twenty Percent and a Few Days – Optimising a Bitcoin Majority Attack," in NASA Formal Methods, vol. 10811, Springer International Publishing AG, part of Springer Nature 2018, 2018, pp. 157-163.

[8] K. Chaudhary, V. Chand and A. Fehnker, "Double-Spending Analysis of Bitcoin," in Pacific Asia Conference on Information System, Dubai, 2020.

[9] S. A. Kumar, J. Vanualailai, B. Sharma, A. Chaudhary and V. Kapadia, "Emergent formations of a Lagrangian swarm of unmanned ground vehicles," 14th International Conference on Control, Automation, Robotics and Vision (ICARCV), 2016.

[10] S. A. Kumar, B. S. J Vanualailai and A. Prasad, "Velocity controllers for a swarm of unmanned aerial vehicles," Journal of Industrial Information Integration, vol. 22, 2021.

[11] J. Raj, K. Raghuwaiya, S. Singh, B. Sharma and J. Vanualailai, "Swarming Intelligence of 1-Trailer Systems.," in (eds) Advanced Computer and Communication Engineering Technology. Lecture Notes in Electrical Engineering, Springer, Cham, 2016.

[12] B. Sharma, J. Raj and J. Vanualailai, "Navigation of carlike robots in an extended dynamic environment with swarm avoidance," International Journal of Robust and Nonlinear Control, vol. 28, no. 12, 2017.

[13] B. Sharma, J. Vanualailai and S. Singh, "Motion planning and posture control of multiple n-link doubly nonholonomic manipulators," Robotica, Cambridge University Press, vol. 35, no. 1, pp. 1-25, 2015.

[14] D. Vlachopoulos and A. Makri, "The effect of games and simulations on higher education: a systematic literature review," International Journal of Educational Technology in Higher Education 14, 2017.

[15] P. Reddy, B. Sharma and K. Chaudhary, "Measuring the digital competency of freshmen at a higher education institute," PACIS 2020 Proceedings. 6, 2020.

[16] R. Johnson, "Cybersecurity Ventures," 2 January 2019. [Online]. Available: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/. [Accessed 8 February 2021].

[17] S. K. Das and D. ManasNaskar, "Safety and Security of Digital Transactions of Banking Sector: An Analytical Study," 2019.

[18] R. G. Smith, "Estimating the cost to Australian businesses of identity crime and misuse," Australian Institute of Criminology, 2018.

[19] P. Reddy, B. Sharma and K. Chaudhary, "Digital Literacy: A Review of Literature," International Journal of Technoethics (IJT), vol. 11, no. 2, p. 30, 2020.

[20] J. v. Ogden, "Cimcor Blog," 2018. [Online]. Available: https://www.cimcor.com/blog/monitoring-for-suspicious-network-activity. [Accessed 11 February 2021].

[21] M. Singh, B. Ghutla, R. L. Jnr, A. F. Mohammed and M. A. Rashid, "Walmart's Sales Data Analysis - A Big Data Analytics Perspective," 4th Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), 2017.

[22] A. Singh, CyberStrong: A Primer on Cyber Risk Management for Business Managers, SAGE Publications India Pvt. Ltd, 2021.

[23] G. Wilkes, "Fundamentals for Reducing Your Attack Surface," 2019. [Online]. [Accessed 2 January 2021].

[24] US- Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," 17 February 2021. [Online]. Available: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and. [Accessed 21 February 2021].

[25] R. Lakshmanan, "U.S. Charges 3 North Korean Hackers Over $1.3 Billion Cryptocurrency Heist," 21 February 2021. [Online]. Available: https://thehackernews.com/2021/02/us-charges-3-north-korean-hackers-over.html. [Accessed 21 February 2021].

[26] BBC News, "Hacker tries to poison water supply of Florida city," 8 February 2021. [Online]. Available: https://www.bbc.com/news/world-us-canada-55989843.

[27] S. Moala, "ANALYSIS OF ISO27001 COMPLIANCE IN TONGA ORGANISATIONS INFORMATION SECURITY," AUT University, 2020.

[28] A. A. Pratt-Sensie, "Security Strategies to Prevent Data Breaches in Infrastructure as a Service Cloud Computing Service Cloud Computing," Walden University, 2020.

[29] Y. Lu and L. D. Xu, "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics," IEEE Internet of Things Journal, 2019.

[30] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. Kumar, R. Maddikunta and S. Singh, "A Review on Cyber Crimes on the Internet of Things," 12 September 2020.

[31] S. Naik and V. Maral, "Cyber security — IoT," 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), pp. 764-767, 2017.

[32] Communications Fiji Limited, "Fiji Police, RFMF and Immigration Fiji websites hacked," 4 March 2016. [Online]. Available: https://fijivillage.com/news/Fiji-Police-RFMF-and-Immigration-Fiji-websites-hacked-s9r52k. [Accessed 2 May 2021].

[33] Communications Fiji Limited, "ITC Department managing a cyber incident targeting the government network - Sayed-Khaiyum," 12 April 2021. [Online]. Available: https://www.fijivillage.com/feature/ITC-Department-managing-a-cyber-incident-targeting-the-government-network---Sayed-Khaiyum-f4rx85/. [Accessed 3 May 2021].

[34] KPMG International Limited, "The multi-faceted threat of fraud- Are banks up to the challenge?," 2021. [Online]. Available: https://home.kpmg/xx/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html.

[35] Dada, E. Gbenga, J. S. Bassi, H. Chiroma, A. O. Adetunmbi and O. E. Ajibuwa, "Machine learning for email spam filtering: review, approaches and open research problems," Heliyon, 2019.

[36] Golladay, Katelyn and K. Holtfreter, "The consequences of identity theft victimization: An examination of emotional and physical health outcomes.," Victims & Offenders, 2017.

[37] Dubois, P. Hélène, J. D. Fielder, R. Delonis, F. Fariello and K. Peters, "The World Bank's Sanctions System: Using Debarment to Combat Fraud and Corruption in International Development.," Good Governance and Modern International Financial Institutions, 2019.

[38] Check Point Software Technology Ltd, "Cyber Security Annual Report,," 2020.

[39] S. Khendelwal, "Facebook Caught Asking Some Users Passwords for Their Email Accounts," The Hacker News, 2019.

[40] P. Muncaster, "Check Point Unmasks Hacktivist Who Defaced Nearly 5000 Sites," 28 May 2020. [Online]. Available: https://www.infosecurity-magazine.com/news/hacktivist-defaced-5000/. [Accessed 8 March 2021].

[41] C. Cane, "33 Alarming Cybercrime Statistics You Should Know in 2019," Security Boulevard, 2019.

[42] M. Moore, "Top Cybersecurity Threats in 2020," 2020. [Online]. Available: https://onlinedegrees.sandiego.edu/top-cyber-security-threats/.

[43] R. A. Munir, N. N. A. Molok and S. Talib, "Exploring the Factors influencing Top Management Involvement and Participation in Information Security," Pacific Asia Conference on Information Systems, 2017.

[44] Fiji Times Limited, "ATM fraud probe," November 2017. [Online]. Available: https://www.fijitimes.com.fj/atm-fraud-probe/. [Accessed 5 March 2021].

[45] Supadii, "What Is Credit Card Skimming?," 28 02 2018. [Online]. Available: http://www.criminalelement.com/what-is-credit-card-skimming/.

[46] Fiji Financial Intelligence Unit, "ATM Skimming in Fiji," 2018. [Online]. [Accessed 18 January 2021].

[47] R. Narayan, 28 08 2018. [Online]. Available: http://www.fbc.com.fj/fiji/33247/skimming-device-found-at-atm.

[48] T. V. Karlova, A. Y. Bekmeshov and N. M. Kuznetsova, "Protection the Data Banks in State Critical Information Infrastructure Organizations," International Conference "Quality Management, Transport and Information Security, Information Technologies", 2019.

[49] Office of the Athorney- General- Fiji, "Banking Act of Fiji," 2016. [Online]. Available: https://www.laws.gov.fj/Acts/DisplayAct/1024#.

[50] M. K. Normalini, T. Ramayah and M. S. Shabbir, "Investigating the Impact of Security Factors In E-business and Internet Banking Usage Intention among Malaysians," Industrial Engineering & Management Systems, 2019.

[51] S. Benqdara, A. Sultan and A. Elfergani, "Assessment of Security Issues in Banking Sector of Libya," International Journal of Computer Application, 2020.

[52] FinTech Futures, "Reducing threats to availability in the banking sector," 2021. [Online]. Available: https://www.fintechfutures.com/2013/07/reducing-threats-to-availability-in-the-banking-sector/. [Accessed 10 March 2021].

[53] H. Rawwash, F. Masa'd, O. Enaizan, B. Eneizan, M. J. Adaileh, A. M. Saleh and R. Almestarihi, "Factors affecting Jordanian electronic banking services," Management Science Letters 10, 2020.

[54] N. Yildirim and A. Varol, "A Research on Security Vulnerabilities in Online and Mobile Banking Systems," 7th International Symposium on Digital Forensics and Security (ISDFS), 2019.

[55] T. Hussain, K. Atta, N. Bawany and T. Qamar, "Passwords and User Behavior," JCP., 2018.

[56] M. Yıldırım and I. Mackie, "Encouraging users to improve password security and memorability," International Journal of Information Security , 2019.

[57] F. Aribake and Z. Aji, "Fight Against Phishing Attacks Among Internet Banking User: A Knowledge Management Technique," 2021.

[58] Cloudflare Inc, "What is a Phishing attack?," 28 08 2018. [Online]. Available: https://www.cloudflare.com/img/learning/security/threats/phishing-attack/diagram-phishing-attack.png.

[59] A. Mallik, "Man-in-the-middle-attack: Understanding in simple words," Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2019.

[60] P. Padmaavathy, "CYBER CRIMES: A THREAT TO THE BANKING INDUSTRY," International Journal of Management Research and Reviews, 2019.

[61] P. J. Steinbart, R. L. Raschke, G. Gal and W. N. Dilla., "The influence of a good relationship between the internal audit and information security functions on information security outcomes," Accounting, Organizations and Society, 2018.

[62] P. Pomerleau and D. Lowery, "Countering Cyber Threats to Financial Institutions.," Springer Books., 2020.

[63] Aboobu and I. B. Y. cker, "What obstruct customer acceptance of internet banking? Security and privacy, risk, trust and website usability and the role of moderators.," The Journal of High Technology Management Research, 2018.

[64] J. Kumire, "How are banks dealing with a rise in cyber attacks?," 2020. [Online]. Available: https://11fs.com/article/how-are-banks-dealing-with-a-rise-in-cyber-attacks. [Accessed 10 March 2021].

[65] M. Roopak, G. Y. Tian and J. Chambers, "Deep Learning Models for Cyber Security in IoT Networks," IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019.

[66] A. Shankar and C. Jebarajakirthy, "The influence of e-banking service quality on customer loyalty.," International Journal of Bank Marketing , 2019.

M. U. Hassan, A. Iqbal and Z. Iqbal, "Factors affecting the adoption of internet banking in Pakistan: an integration of technology acceptance model and theory of planned behaviour," International Journal of Business Information Systems (IJBIS), Vol. 28, No. 3, 24 June 2018.