International Journal of Management and Commerce Innovations ISSN 2348-7585 (Online)
Vol. 7, Issue 2, pp: (846-850), Month: October 2019 - March 2020, Available at: www.researchpublish.com

Business Continuity Management in Information Technology and Systems for Banking Institution in Malaysia

Nur Fadhilah Umar[1], Jamaludin Ibrahim[2]

[1,2] Centre for Information Technology Advancement, Kulliyyah of Information and Communication Technology (KICT), International Islamic University Malaysia

Abstract: **Banking, from the perspective of industry 4.0, calls for a greater level of digitalization. Just like autonomous cars promise to be the norm one day, "the bank of the future" will be mostly digital. However, this will bring with it many challenges. Cyber-threats have been targeting the financial sector worldwide. Downtime can cause widespread disruption and massive damage to an organization's bottom line and reputation. As organizations realize the size of potential exposure to uncontrol risk, insuring business continuity is becoming a vital task within all industrial especially financial sectors. This article will discuss on the threat and importance of business continuity plan in the banking institution, the response and recovery plan as well as the recommendation in maintaining the business continuity in financial institution in Malaysia.**

Keywords: **Business Continuity, System Disruption, Banking Sector, IR 4.0, Maximum Tolerable Downtime (MTD).**

I. INTRODUCTION

The world is moving at a fast pace with the digital economy. A fourth industrial revolution has emerged, known as Industry Revolution 4.0. It connects physical with digital, and allows for better collaboration and access across departments, partners, vendors, product, and people. It empowers business owners to better control and understand every aspect of their operation and allows them to leverage instant data to boost productivity, improve processes, and drive growth. Banking, from the perspective of industry 4.0, calls for an even greater level of digitalization.

Digital platforms, including mobile banking, e-wallets, and payment apps, are now a crucial mechanism for engaging with customers in the financial industry. New fintech solutions to consumer banking services (a combination of bank and financial advisor applications) with the convergence of technology will allow companies such as Amazon to be able to access bank accounts and buy products for you without your having to think about it. However, with these benefits from the latest technology, it will also bring with it many challenges.

The finance institution is a sector in which the development of information technology (IT) and information systems (IS) have had a significant effect upon competitiveness. In this sector, organizations have become dependent upon technologies that they do not fully comprehend. In fact, banking industry IT and IS are not considered as support technologies but are regarded as production. As such, IT and IS have supported tremendous changes in the ways business is conducted with consumers at the retail level.

Innovations in direct banking would have been impossible without appropriate IS. Therefore, business continuity planning (BCP) at banks is crucial as the industry develops to safeguard consumers and to comply with the regulatory requirement. In addition, BCP is important in the banking industry and at the same time different from other industries, for three other specific reasons as highlighted by the Bank of Japan in 2003 [2]:

• *Maintaining the economic activity of residents in disaster areas* by enabling the continuation of financial services during and after disasters, thereby sustaining business activities in the damaged area;

• *Preventing widespread payment and settlement disorder* or preventing systemic risks, by bounding the inability of financial institutions in a disaster area to execute payment transactions;

• *Reduce managerial risks* for example, by limiting the difficulties for banks to take profit.

The financial sector sees business continuity not only as a technical or risk management issue, but as a driver towards any consideration on mergers and investment. The capability to manage BC should also be considered as a strategic weapon to minimize the investment timeframe and shorten the data centre merge, often considered one of the vital issues in quick wins, as well as the information and communication technology (ICT) budget savings.

II. LITERATURE REVIEW

The Business Continuity Institute (BCI, 2007) describe BCM as a holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value creating activities. This is nowhere truer than in the banking sector. The need for readiness of banks to address the various needs of a varied customer base and evolution in its essence has driven banking institutions towards digitalization and IT enabled systems across all operations [2].

Regulatory standards are another main factor for all financial sectors in every country. Every organization is required to comply with national law in addition to national and international governing bodies. Regarding the Business Continuity Management, banking industries in Malaysia are required to comply with the Central Bank policy, Payment Network Malaysia (PayNet)'s Guidelines, as well as Laws of Malaysia Act; Financial Services Act 2013 (FSA), Islamic Financial Services Act 2013 (IFSA), Development Financial Institutions Act 2002 (DFIA) etc. However, despite complying to those regulations, there were still frequent incidents occurred in banking industry that was unable to be recovered within the maximum tolerable downtime (MTD).

Based on the Risk Management in Technology (RMiT) by Central Bank of Malaysia [3], where there is a reasonable expectation for immediate delivery of service to customers or dealings with counterparties, a financial institution must ensure that the relevant critical systems are designed for high availability with a cumulative unplanned downtime affecting the interface with customers or counterparties of not more than 4 hours on a rolling 12 months basis and a maximum tolerable downtime of 120 minutes per incident.

British academic Richard Benham, chairman of the National Cyber Management Centre, warned the BBC that "a major bank will fail as a result of a cyberattack in 2017 leading to a loss of confidence and a run on that bank." Many banks already see millions of attempted attacks each year with modest losses resulting, but the precedent set by the SWIFT hack on central banks indicates that these attacks are rapidly becoming more sophisticated.

In April 2018, Central Bank of Malaysia announced that they suffered a cyberattack in an attempt to steal money through fraudulent wire transfers over the SWIFT bank messaging network[4]. Fortunately, no funds were stolen from the incident and all unauthorized transactions were stopped through prompt action in strong collaboration with SWIFT, financial institutions and other central banks. The last time this happened was in 2016, when the Bangladesh Bank lost $81 million from a great cyberattack. The same tactic was used by the hackers to steal funds and they successfully took over the bank's SWIFT servers to force fund transfers.

In September 2019, CIMB has been facing criticism online when customers were facing technical difficulties when trying to access to their banking services [5]. Companies like Malaysia Airlines was also issued statements to confirm that CIMB was experiencing a technical issue with its card payment system. Users were advised to use CIMB Clicks or other alternative payment methods.

Bank Simpanan Nasional (BSN) Malaysia's core banking system faced a serious outage over the long weekend in January 2019. The ATM, CDM, MEPS, myBSN, and Ejen Bank BSN services were affected at all automated banking channels and BSN branches [6]. Only its credit card facilities remained in operation as usual. BSN announced that its ATM services have been restored and all of BSN's affected services have resumed normal operations only after three days of downtime. Despite stating that the sources of the disruption had been identified during the rectification process, BSN has not disclosed these causes to the public.

Maybank's major banking disruption causes chaos on social media in March 2019 [7]. The funds' transfer services experienced an outage for at least six hours, with users on social media reporting they were unable to get security codes or TAC numbers to complete transfers across banks. The bank's customers have complained of being unable to transfer money through its ATMs and also through Maybank2U service. It was bad timing as many customers had just received their salaries and were paying their bills. Based on complaints by users on Twitter, the issue also extends to other banks in which those transferring funds from other banks into Maybank being failed to do so.

III. CYBER THREATS

Based on the nature of data held by financial institutions, there is no surprise they have the highest risk of cyberattacks. In recent years, Distributed Denial of Service (DDoS) attacks have grown in size and frequency and impacting banking sector worldwide. DDoS attacks can be explained as those in which multiple compromised computer systems attack a target such as a server, website or other network resource which leads to a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even may result to crash and shut down, thereby denying service to authorized users or systems.

A study in 2015 discovered that 56 percent of financial institutions saw a rise in the number of DDoS attacks against them in the previous year, and 60 percent said that attacks are larger than they were a year ago [8]. DDoS attacks are increasingly being used for cyber-extortion attacks, which aim to blackmail financial institutions into paying out high ransoms to refrain from having their sites taken down and intellectual property published in the underground.

Besides that, social engineering is being increasingly used in cyberattacks leading to data breaches. It relies on the trusting behaviour of the initial victim, in many cases employees, and makes attacks better designed to trick the victim into allowing access to data. Social engineering is used in spear phishing, in which an employee responds to a request that appears to originate from someone superior in the company. In 2016, Australian banks were among those targeted by a spear phishing attack named "Carbanak". Trough the compromised Australian banks, cyber criminals targeted 100 banks in 30 countries and stole about 1.3 billion dollars over an 18-month period. This attack used spearfishing techniques to encourage high-level employees to download the malware which then moved into the bank systems to issue transfers. In some cases, the malware ordered some ATMs to start dispensing cash [9].

In addition, ransomware attack can lock business critical data and prevents banks from servicing its customers, the attack leads to a denial of service attack. Once being attacked, it isn't as simple as paying the ransom or restoring from backup to recover. If the data is locked and encrypted by an attacker and this data is business critical, the bank will lose business. No bank can function if customers are locked out of conducting banking transactions either at a branch or via a cloud access point. For business banking customers that send and receive continuous streams of financial information to partner banks, losing access to financial data can be extremely damaging not only business operations but also the bank's reputation.

The majority of malware is categorized as Trojan Horse and comprises typical malicious activities like downloading and dropping files, spyware, keyloggers and password stealers, integration into botnets and conducting distributed denial of service attacks (DDoS). According to Kaspersky Lab, the number of cyberattacks targeting financial institutions and their customers increased significantly in 2016, which observed nearly 1.09 million banking trojan attacks on users, approximately 30.6 percent rise over the previous year [10].

IV. CURRENT PRACTICE

Fortunately, awareness and recognition of potential cybersecurity risks among banking institutions has proven generally successful. Banking institutions protect themselves better after seeing incidents happen around them. Financial institutions have reported that just hearing about cybersecurity incidents affecting other organizations has encouraged them to invest more in their own cybersecurity practices [11].

All of the financial Institutions in Malaysia must comply to the standard and requirement by Central Bank of Malaysia. Failure to do so may result in one or more enforcement actions. In the RMiT, it has stated that; "A financial institution must establish comprehensive cyber crisis management policies and procedures that incorporate cyber-attack scenarios and responses in the organisation's overall crisis management plan, escalation processes, business continuity and disaster recovery planning. This includes developing a clear communication plan for engaging shareholders, regulatory authorities, customers and employees in the event of a cyber-incident. "

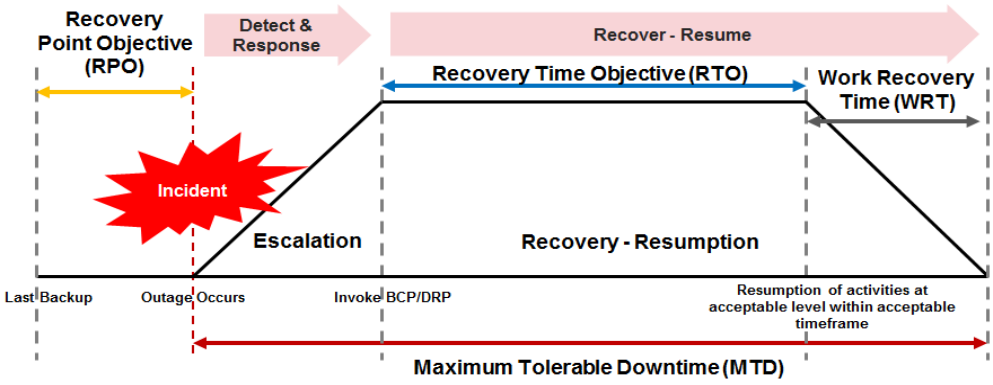

Fig. 1: Cyber Incident Response Plan

A financial institution must establish and implement a comprehensive Cyber Incident Response Plan (CIRP). CIRP is illustrated in Fig. 1.

The CIRP must address the following:

a) Preparedness

Establish a clear governance process, reporting structure and roles and responsibilities of the Cyber Emergency Response Team (CERT) as well as invocation and escalation procedures in the event of an incident.

(b) Detection and analysis

Ensure effective and expedient processes for identifying points of compromise, assessing the extent of damage and preserving sufficient evidence for forensics purposes.

(c) Containment, eradication and recovery

Identify and implement remedial actions to prevent or minimise damage to the financial institution, remove the known threats and resume business activities.

(d) Post-incident activity

Conduct post-incident review incorporating lessons learned and develop long-term risk mitigations.

In addition, a financial institution must conduct an annual cyber drill exercise to test the effectiveness of its CIRP, based on various current and emerging threat scenarios (e.g. social engineering), with the involvement of key stakeholders including members of the board, senior management and relevant third-party service providers. Besides that, they must establish a technology audit plan that provides appropriate coverage of critical technology services, third party service providers, material external system interfaces, delayed or prematurely terminated critical technology projects and post-implementation review of new or material enhancements of technology services.

V. RECOMMENDATIONS

Despite being regulated by the Central Bank of Malaysia, there were still frequent incidents occurred in banking industry which failed to be recovered within the MTD. Below are some recommendations that may possibly help in improving business continuity management in banking industry:

1. All banking institution must provide at least a hot site for the alternate site to support the bank operation, which commensurate with the MTD and RTO, 2 hours and 1 hour respectively.

2. In an actual disaster, the MTD timing should start from the occurrence of incident. Typically, after a disaster has struck, there will be an immediate notification to the Crisis Management Team (CMT) members, a damage assessment activity by technical teams and various communications process before CMT decides to activate BCP/DRP. The duration taken by CMT to make decision may vary considerably but must be less than 30 minutes, in order to meet RTO timing.

3. It is important for Network Operation Centre (NOC) and Security Operation Centre (SOC) in every banking institution to collaborate more effectively. In doing so, business process can be better enhanced in terms of preventive measures such as network device configuration and incident management in terms of analysis, workflow, and minimizing risk of downtime.

4. Regular testing reveals any number of changes to a company'network that could inhibit the recovery of data, applications and systems should there be an unexpected IT failure. These changes can include added storage, new security patches and modified or removed applications. Backup corruption and human error add to the snags that are revealed with weekly testing and can include tape corruption and incorrect setup of backups. While testing with tape or disk backup solutions is complex and cumbersome, automatic, on-demand testing afforded by a hybrid cloud solution offers a simpler alternative.

5. Full interruption test or full-scale exercise must be done at least bi-annually which activate the alternate work site facilities and implement the business continuity plan in whole.

6. The internal and external audit function and dedicated internal technology audit function must be enlisted to provide advice on compliance with and adequacy of control processes during the planning and development phases of new major products, systems or technology operations. In such cases, the technology auditors participating in this capacity should carefully consider whether such an advisory or consulting role would materially impair their independence or objectivity in performing post-implementation reviews of the products, systems and operations concerned.

7. Penalty charges for MTD and RTO breaches must be imposed based on the duration and severity of the recovery.

VI. CONCLUSION

When it comes to the cybersecurity threats financial institutions face every day, there is only one guarantee: hackers will continue to find new ways to infiltrate the organization's network. The goal might be ruining a company's good name, causing a political stir or simply extorting money, but the methods cybercriminals employ are constantly evolving into newer, unforeseen dangers. In order to fight back, financial institutions must be prepared to adapt and redirect at every turn, facing both new threats and the old proven methods. No one can precisely predict the future but preparing for eventual disruption is something everyone should do.

REFERENCES

[1] Business continuity and the banking industry, Arduini F, Morabito V *Communications of the ACM (2010) 53(3) 121-125*

[2] Mohan and Rai, 2006; IBM Global Services, 2000; BSI, 1999

[3] Risk Management in Technology, Bank Negara Malaysia; 18 July 2019

[4] Publico, R., "The Bank Negara Malaysia Incident is Another Wake-Up Call for Banks". Retrieved from https://www.globalsign.com, April 2018.

[5] Pillai, V., "Core Banking System Intact Despite Technical Glitch, Says CIMB". Retrieved from https://www. freemalaysiatoday.com/category/nation, September 2019

[6] Tan, J., "BSN Banking Services Finally Restored After Weekend Outage". Retrieved from https://ringgitplus.com, January 2019

[7] Nambiar, P., "Maybank's Major Banking Outage causes Uproar on Social Media". Retrieved from https://www. freemalaysiatoday.com/category/nation, March 2019

[8] Kitten, T. (2015, August 24). DDoS Attacks Against Banks Increasing. Retrieved from http://www. bankinfosecurity .com/ddos-a-8497

[9] Dunn, J. (2017, June 20). Anyone can be a target of hacking. Retrieved from http://www.afr.com/news/ special-reports/technology-outlook-series/anyone-can-be-a-target-of-hacking-20170618-gwthfe

[10] Barth, B. (2017, February 23). Kaspersky: Banking malware attacks up 30.6% in 2016; finance sector phishing also more prevalent. Retrieved from https://www.scmagazine.com/kaspersky-banking-malware-attacksup-306-in-2016-finance-sector-phishing-also-more-prevalent/article/639969/

[11] Kaspersky Lab. (2017, March 27). Cybersecurity in financial institutions 2016 — and what 2017 holds.