Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, June 2018, vol. 23, no. 2

IMPACT OF CYBERATTACKS ON FINANCIAL INSTITUTIONS

NIDA TARIQ

Hailey College of Commerce, University of the Punjab, Pakistan

Tel: **00923224153528;**

Email: **nidawaqas1991@gmail.com**

Abstract

Use of modern technology has geared up the business activities. Cyber technology has taken the organizations above the heights of profits. Specially, it has given a great favor to the financial institutions by providing data storage, digital money, networking and many other online services. The fact, cannot be hindered in any way that where technology facilitates intensively, can also be severely disastrous for financial institutions. Cybercrimes as a technology disease are spreading very speedily in present era. Nothing is secure now and financial institutions are under a great threat. Therefore, this study has undertaken to explore impact of cyberattacks on financial institutions. The study has witnessed that there may be the lesser cases of cyberattacks on financial institutions but their impact is severe in terms of direct and indirect loss. It has also been witnessed that cyberattacks are growing rapidly as compare to few years back. In this alarming situation, organizations, especially financial institutes must pay attention to the security. Some of the preventive measures can be tightening internal security, cybersecurity assessment, cybersecurity training and cybersecurity audit.

Keywords: **Cybercrime; Cyber-Attack; Financial Institutions**

INTRODUCTION

With the emerging trends in business most of the companies are depending on digital money, electronic data and computer networks where all of the personal and financial information is stored. By these trends theft tactics have also been upgraded. Cybercrime is one of the major challenges today. Major cyberattack in the recent years not only caused financial loss but also leaked other sensitive information. According to Group-IB expert evaluations, almost 99% of all cybercrimes in the world now involve money theft. Massive malware attack that hit in 2017, ruined many of the companies like MDLZ, DLA Piper in US, Rosneft, EVRAZ and Banks in Russia, Maersk in India and Denmark and many other countries were the victim of this attack [1]. Identity theft as a subset of cybercrime is intentionally stealing someone's identity to gain benefit in any kind. In recent years identity theft crashed operations and profitability of many businesses. "2017 was a great year for identity thieves". Equifax is one of the victims who suffered the worst data breaches in 2017, all of the sensitive information hacked could be used for identity theft [2]. Although, cyberattacks have disastrously affected many of the business but still it requires more attention. "In the past few years, a growing number of organized and specialized groups have been robbing these financial institutions with the aid of malware." Banks are as exposed to 'mass market' attacks as any other organization [3].

Various studies have been done before in the context of cyberattack but either it is country specific or attack type specific or victims describing [4], but this study undertakes global demographics where financial institutions became a victim of cyber-attack. This study presents an overall view and impact of cyberattacks on financial institutions. This research is very significant for emerging financial institutions.

LITERATURE REVIEW

This review presents in depth the basic and relevant body of knowledge in the field of electronic money, cybercrime, types of attackers and financial institutions.

Digital Money

"Electronic money (also e-Money or digital money) are traditional currency in a digital format. They are issued by the government, are regulated and legal tender in the country of issue. The supply of money is fixed and controlled by the state (European Central Bank Report, 2012). Example: Euro or US dollar used to make online

payments" [5]. The use of digital money is uncontrollably increasing day by day because of its intense ease. There has also been a concurrent proliferation of new businesses and services related to all aspects of digital currency, from the computing hardware required to mine it, the processing of transactions, payment platforms for merchants, legal services devoted to navigating the still ambiguous and contradictory regulatory environments surrounding it, and both online and print publications devoted to covering significant events and promoting its use [6].

Cybercrime

"Cybercrime refers to the unlawful acts where in the computer is either a tool or target or both" [7]. "Cybercrime" means illegal acts, the commission of which involves the use of information and communication technologies [8]. "Evidence shows us that organizations such as banks, government agencies, healthcare institutions and large corporations that maintain highly valuable data are more likely to be attacked more frequently than most" [9].

Types of Attackers

Attackers generally fall into three broad categories:

- The financially motivated attacker who intends to compromise systems to conduct theft or fraud electronically.
- The espionage motivated attacker who intends to steal information to sell on to a third party.
- The politically motivated attacker who intends to compromise information or systems to achieve a goal shared within a group [4].

Financial Institution

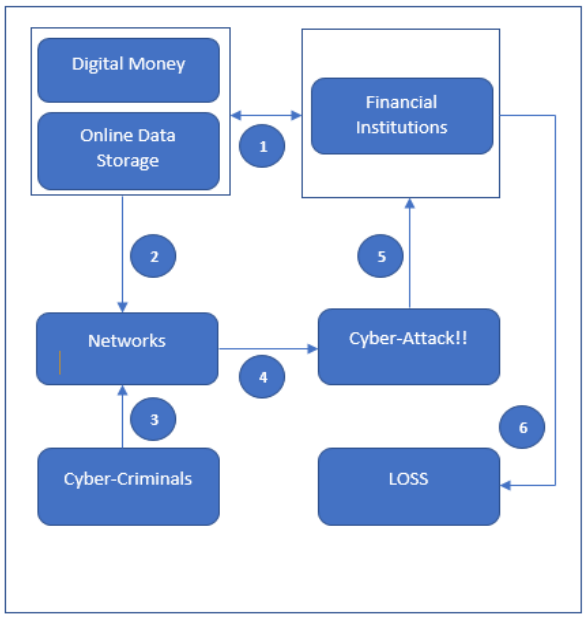
Financial institutions are corporations which provide services as intermediaries of financial markets [10]. A financial institution is responsible for the supply of money to the market through the transfer of funds from investors to the companies in the form of loans, deposits, and investments [11].

Conceptual Framework

It is an explanatory research and uses qualitative approach to elaborate the impact of cyberattacks. The model (Figure 1) shows the relationship between different variables of this research study.

In the given Figure 1, (1) shows the use of digital money and online data storage by financial institutions. (2) shows digital money and online data can be stored by using networks. (3) Depicts interference of cyber-criminals into the network that results in (4) and (5) cyber-theft of the organizations ultimately, they suffer from financial loss or data breach (6).

Figure 1: Demonstrating the impact of Cyber-Attacks on Financial Institutions.



Research Question

How cyber-attack impact on financial institution?

METHODOLOGY

Literature provides the base about the concept and but effect is still unclear. Therefore, hybrid research method is adopted. This is global study on financial institutions and banks are chosen as sample as they cover most of the services provided by other financial institutions like insurance etc. Therefore, result is expected to generalize on rest of the financial institutes. Collected data is analyzed by descriptive statistics method where central tendency mode is used to check most frequent effect in the time span of 2010-2018. Data is collected from secondary sources because of limited time and budget availability, therefore, convenience sampling technique is adopted.

Cyber-Attacks (2010-2018)

United States

2012: As a result of cyber-attack reported by New York Times, “Frustrated customers of Bank of America, JPMorgan Chase, Citigroup, U.S. Bank, Wells Fargo and PNC, who could not get access to their accounts or pay bills online, were upset because

the banks had not explained clearly what was going on" [12]. Furthermore, "CEO Brian Moynihan told analysts the bank of America is spending "hundreds of millions of dollars a year" on cyber security to guard against data breaches" [13]. The aim of attackers was not to gain a financial advantage/theft but to frustrate the customers that could ultimately cause a financial loss to the institutions. As reported by CNN, "Denial of service attacks is an effective but unsophisticated tool that doesn't involve any actual hacking. No data was stolen from the banks, and their transactional systems like their ATM networks remained unaffected. The aim of the attacks was simply to temporarily knock down the banks' public-facing websites [14].

2014: USA Today reports, "Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building" [15].

2016: Another news reports, "Forty-six major financial institutions were targeted with distributed denial of service (DDoS) attacks in which hackers gain remote control of hundreds of computers and servers and use them to flood a target's server with data, clogging it up so that it can't receive legitimate traffic" [16]. Furthermore, NBC news says "Targets included Bank of America, the New York Stock Exchange, Capital One and ING, and PNC Banks, according to court papers" [16]. In addition to the above, "FBI and US secret service agents have arrested a man charged with the largest cyber-attack of financial firms in America's history. The company hit hardest by the breach was JPMorgan. More than 83 million of the bank's customers had data stolen in the breach [17].

Europe

2015: "The RBS banking group has revealed it suffered a cyber-attack on its online services that left customers struggling to log on for nearly an hour – just as monthly pay cheques were arriving in accounts" [18].

In late 2015, several incidents of cyber-attacks took place in online trading as mentioned by NASDAQ, "The latest data breach was reported by FXCM Inc. FXCM , an online foreign exchange trading and related service provider, on Oct 1. According to the company, hackers gained unauthorized access to customer information and a few transfers were made from certain accounts" [19].

An Information Security Company Group-IB published in a blog," In February 2015, for the first time ever, a Trojan dubbed Corkow (Metel) gained control of a stock exchange trading terminal and placed orders worth a total of several hundred million dollars. In just 14 minutes attackers created abnormal volatility, which made it possible to buy dollars for 55 rubles and sell them for 62 rubles. As a result of the incident, a Russian bank suffered huge losses, although it was random traders rather than the hackers themselves that profited from it". (1) Further it by Group-IB stated, In February 2016, hackers tried to steal $951 million from the Central Bank of

Bangladesh via the SWIFT system. This company highlighted that cyberattack does not cause only financial loss or information breach but it can also be used in spying and cyberterrorism. Corkow is also known as Metel.

2016: In another report by Crime Russia, “Hackers from the Lurk team, which created the banking Trojan of the same name, were able to steal more than 1.7 billion rubles ($28.3m) from the accounts of Russian banks before being detained by the Interior Ministry and the FSB in June 2016” [20]. Crime Russia highlights the case of Energobank where Metel’s attack caused the bank damages of 244 million rubles ($3.7M). (20) The Kaspersky written in a blog,” One way or another, the criminals stripped each victim bank of $2.5 mln to $10 mln – the amount looks striking even when assessed individually”.

Buhtrap is another cyberattack. “Experts estimate that the lowest amount stolen from a Russian bank is $370,000 (25 million RUB), and the highest amount is close to $9 million (600 million RUB)” [21].

2017: HSBC one of the largest bank in world as well as in Europe suffered from a cyber-attack in early 2017. A report from The Week Newsletter stated, “HSBC customers were unable to access online banking services for the second time in a month today, in the wake of an apparent cyber-attack” [22].

Asia

2010: Umashankar Sivasubramaniam Vs ICICI Bank is one of the famous phishing fraud case. According to Economic Times,” In a verdict in the first case filed under the Information Technology Act, Tamil Nadu IT secretary on Monday directed ICICI Bank to pay Rs.12.85 lakh to an Abu Dhabi-based NRI within 60 days for the loss suffered by him due to a phishing fraud” [23].

2016: “ICICI Bank, HDFC Bank and Axis Bank - the top three private sector lenders - confirmed in separate statements some of their customers’ card accounts had been possibly breached after use at outside ATMs” [24].

According to Crime Russia, “Another group, purposefully attacking banks, is Lazarus, the most famous theft of $81 million from the Bangladesh Bank in 2016” [20]. Further it stated by Group-IB, In February 2016, hackers tried to steal $951 million from the Central Bank of Bangladesh via the SWIFT system. This company highlighted that cyberattack does not cause only financial loss or information breach but it can also be used in spying and cyberterrorism. Corkow is also known as Metel [1]. In another incident of cyber-attack in Turkey Insurance Journal stated, “Hackers targeted Turkish lender Akbank in a cyber-attack on the SWIFT global money transfer system, the bank said, adding it faced a liability of up to $4 million from the incident but no customer information was compromised” [25].

2017: Taipei Times reported in 2017, “Far Eastern on Friday said it reported to the Financial Supervisory Commission that malware had been implanted in its computer system, which affected some of its PCs and servers, as well as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network” [26]. The Focus Taiwan said,” Through the planted malware, hackers conducted virtual transactions to move funds totaling nearly US$60 million from Far Eastern Bank customers' accounts to some foreign destinations such as Sri Lanka, Cambodia and the United States, the bank found on Tuesday” [27].

2018: The Habib Bank Limited became a victim of ATM skimming. The Habib Bank Limited confirmed that over Rs10 million had been stolen from 559 of its accounts. [28] Dawn says, “Hundreds of thousands of rupees have been skimmed out of 32 accounts of a private bank located in the Saddar area of Rawalpindi, indicating the presence of ATM hackers in the twin cities including Islamabad” [29]. Another report by Dawn says,” Several foreigners have been arrested for allegedly stealing data from banks using skimming devices at ATM facilities” [30].

Africa

2016: According to Serianu report, “cyber criminals employed a very complex cyber-attack targeting 10 organizations in banking, insurance, utilities and government across 3 countries in Africa.” According to this report damages to banking and financial service sector (as a result of cyber-attack is highest among all sectors) that is $206m in 2016. At least 19 organizations in Kenya have been affected by the ransomware virus in an ongoing global hacking [31].

Australia

The banking, financial services and insurance sector are clearly one of the most prone industries to cyber-attacks, CBA which became a victim of cyber-attack in 2016.

Hundreds of thousands of Australians have been targeted by a fake Commonwealth Bank email designed to infect recipients with malware. Customers and non-customers are vulnerable to the scam, which asks people to click to view a ‘Secure Message’ [32]. Furthermore, those who take the bait will in fact download a trojan used by cybercriminals to hack computers [32].

RESULTS

In this study 26 bank cases studied under the head of cyber-attacks. Findings are demonstrated in Table 1.

Table 1: Demonstrating the major Cyberattcks on financial institutions from (2010-2018).

Cyberattacks on Financial Institutions 2010-2018 Demographics* Type of Loss					
		Type of Loss			
		Financial Loss	**Data Stealing**	**Customer Frustration**	**Total**
Demographics	US	4	1	6	11
	Europe	2	1	2	5
	Asia	6	3	0	9
	Africa	-			-
	Australia	0	1	0	1
Total		12	6	8	26

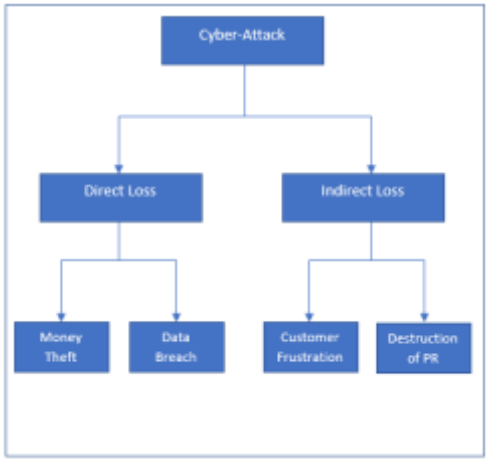
DISCUSSION

Evidences conclude that cyber-attacks impact on financial institutions in the following ways:

- Direct Loss
- Indirect Loss

Direct and indirect loss can be further classified in to two categories. Table 1 demonstrates categorized losses suffered by financial institutions as a consequence of cyber-attack (Figure 2).

Figure 2: Demonstrating the possible losses as a consequence of cyber-attack on financial institution.



- Cyber criminals gain remote access to the systems where they can administer

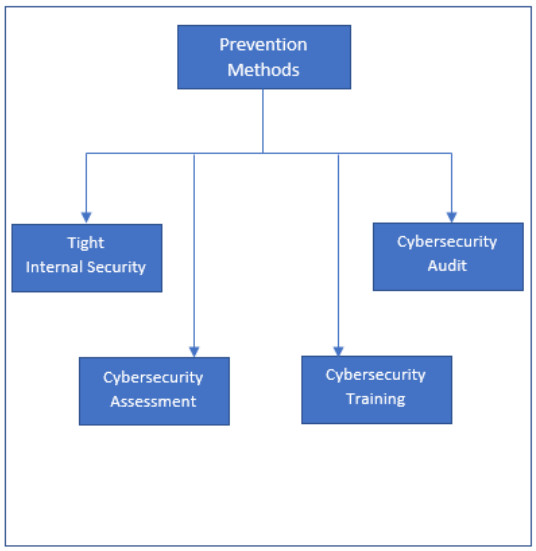
all data.
- They can cause a financial loss (by making false transaction).
- They can steal the confidential information and they can sale it, even they can use it for spying or terrorism.
- They can target customers by attacking on organization. It may result into customer frustration or customer identity theft.
- Organization's public image can be destructed for insufficient information security compliance.

From the above findings in Table 1, it can be noted that financial losses are highest in ranking followed by customer frustration and data breach. In addition to the above it can be noted cyber-attacks on US banks in the duration 2010-018 were more frequent among all demographics. African banks are also one of the victims of cyber-attack but no individual bank case found from secondary data that could be included in this study but overall sufferings are mentioned above.

Preventive Measures

It has been witnessed that every time cyber criminals use a tool or a tactic to break security. It could be in form of malware, DDos attack, Phishing, drive by download or password stealing. But organizations can prevent from cyber-attack as given in Figure 3.

Figure 3: Demonstrating the methods to prevent from cyber-attacks.



CONCLUSION

Cyber issues are global issues now. It can be noted that there is no discrimination of developed or underdeveloped countries. These attacks are not boundary restricted.

There is no way to escape from the fact that the most target organizations are financial institutions because money, information and public are most associated with them. It can be concluded that banks as a financial institution contain higher cyber risk as compare to other institutions. Most of the time motive of cyber criminals is to gain financial advantage or to frustrate the customers. But institutions can fight by working very actively. Organizations must be updated with latest tools and tactics used by hacker to gain any illegal advantage. In addition to the above, white hat hackers report the organizations from cyber threat. Organizations should pay attention to their reports and must encourage White-Hat hackers by splendid rewards and bounties so cyber-criminals may be discouraged.

REFERENCES

1. Sachkov I (2017) Targeted attacks on banks. https://www.group-ib.com/blog/polygon
2. 2017 was a great year for identity thieves. https://www.myidcare.com/articles/single/2017-was-a-great-year-for-identity-thieves
3. Cherepanov A, Jean-Ian B (2016) Modern attacks against Russian financial institutions.
4. Pettersson M (2012) Banks likely to remain top cybercrime targets. Symantec Corporation, Excutive Report.
5. (2014) The Digital Currency Phenomenon.
6. Shaw L (2016) The meanings of new money: Social constructions of value in the rise of digital currencies. University of Washington.
7. Aggarwal P, Arora P, Neha, Poonam (2014) Review on cybercrime and security. International Journal of Research in Engineering and Applied Sciences, p. 51.
8. National Cyber security policy framework for South Africa. Government Publication.
9. (2017) Global Cybersecurity Report 2017. Nexia International Limited.
10. Siklos P (2001) Money, banking and financial institutions: Canada in the global environment.
11. https://www.myaccountingcourse.com/accounting-dictionary/financial-institution
12. Business Day. The New York Time.
13. McCoy DC, Kevin (2014) Business Day. https://www.usatoday.com/story/money/business/2014/10/15/bank-of-america-earnings/17275409/
14. Goldman D (2018) CNN Money. http://money.cnn.com/2012/09/27/technology/bank-cyberattacks/index.html
15. www.usatoday.com/story/news/politics/2014/10/20/secret-service-fbi-hack-cybersecuurity/17615029/
16. Winter TC, Tom (2016) U.S News.

https://www.nbcnews.com/news/us-news/iranians-charged-hacking-attacks-u-s-banks-dam-n544801
17. http://www.bbc.com/news/world-us-canada-38324245
18. Collinson P (2015) Business. The Guardian. https://www.theguardian.com/business/2015/jul/31/rbs-and-natwest-customers-complain-of-online-problems
19. Research Zacks Equity (2015) 5 Cyber security stocks to change how we protect our data. http://www.nasdaq.com/article/5-cyber-security-stocks-to-change-how-we-protect-our-data-cm531047
20. High Profile Cases (2017) Hackers of Russian group cobalt attacked 250 companies around the world.
21. Kovacs E (2016) Buhtrap gang steals millions from russian banks cybercrime. http://www.securityweek.com/buhtrap-gang-steals-millions-russian-banks
22. The Week. HSBC shares rise after £1.5bn buyback pledge. The Weekday Newsletter. http://www.theweek.co.uk/hsbc/63926/hsbc-profits-slides-by-almost-a-fifth/page/0/6
23. Agencies ET Bureau (2010) ICICI Bank told to pay Rs 13 lakh to NRI customer. https://economictimes.indiatimes.com/industry/banking/finance/banking/icici-bank-told-to-pay-rs-13-lakh-to-nri-customer/articleshow/5798944.cms
24. Tripath D (2016) Security breach feared in up to 3.25 million Indian debit cards. https://in.reuters.com/article/india-banks-atm-fraud/security-breach-feared-in-up-to-3-25-million-indian-debit-cards-idINKCN12K0CE
25. Altayli CS, Birsen (2016) Turkey's akbank faces possible $4m liability after cyber-attack but it's insured. Insurance Journal.
26. http://www.taipeitimes.com/News/front/archives/2017/10/08/2003679926
27. Cheng-wu S, Chien-pan L, Yi-chu T, Huang F (2017) Lai orders information security review.
28. Aybub I, Iqbal S (2017) Rs10m stolen from 559 bank accounts in ATM fraud. https://www.dawn.com/news/1374623
29. Tahir N (2018) 32 bank accounts compromised in Rawalpindi ATM skimming incident. https://www.dawn.com/news/1383524
30. Ali I (2018) 4 Chinese nationals arrested in another ATM skimming incident in Karachi. https://www.dawn.com/news/1382925
31. Nairobi (2017) WannaCry ransomware virus hits 19 Kenyan firms. The Indian Express. http://indianexpress.com/article/technology/tech-news-technology/wannacry-ransomware-virus-hits-19-kenyan-firms-4665265/
32. McRae J (2016) Malicious Commonwealth Bank fraud email targets hundreds of thousands of Australians. https://www.mailguard.com.au/blog/malicious-commonwealth-bank-fraud-email-targets-hundreds-of-thousands-of-australians