MANAGEMENT TODAY
-for a better tomorrow
An International Journal of Management Studies
home page: www.mgmt2day.griet.ac.in
Vol.8, No.1, January-March 2018

Impact of Cyber Crimes on Technology Enabled Banking Services

Pallavi, E. V. P. A. S.

Assistant Professor, Department of Management Studies, M V G R College of Engineering (Autonomous), Vijayaram Nagar Campus, Chintalavalasa, Vizianagaram, Mob: 9440072245, E-Mail: pallavielisetty@gmail.com

ARTICLE INFO

Article history:

Received 12.03.2018
Accepted 20.03.2018

Keywords:

information technology, cybercrime and technology enabled banking services

ABSTRACT

Information technology is one of the principal launch pad for the Indian banking industry in terms of its transactions processing as well as for a variety of other internal systems and processes. Now-a – days a variety of technical platforms are available to the banks to carry out of their day to day processes, their approach of reporting the transactions and the way in which interbank transactions and clearing has evolved significantly over the years. The explosion in online transactions growing on technologies like NEFT (National Electronic Fund Transfer), RTGS (Real-time Gross Settlement Systems), ECS (Electronic Clearing Service) and mobile transactions is a indication of technology in banking and financial matters. With the quick growth of computer and internet technologies, new forms of worldwide crimes known as "Cyber Crimes" have evolved in the picture. As the evidence from William duer retail banking is exposed 40% of cyber-attacks. The financial services sector faces specific challenges of its own. Banks are engaged with the decentralization of their services through digitization. Banks and financial institutions are the major targets to the criminals and hackers. Recently we have witnessed Ransomware attack on all the sectors where it has treated as a large cyber-attack on the functionality of all the sectors. This paper focuses on the impact of cybercrimes on banking sector and hoe to prevent such cyber-attacks in future for security.

Introduction

The technological advancement in the Indian banking industry has been mostly intended by different committees set up by the Reserve Bank of India and the government of India to evaluate the performance of technological transformation. No major advance in technology accomplishment was achieved by the industry till the early 80s, though some working groups and committees made references to the need for automation of some banking processes. This was mainly due to the inflexible conflict by the very tough bank employees unions. The early 1980s were involved in the beginning of automation and computerization in Indian banks. This was the period when banks as well as the RBI went very slow on automation, carefully eliminating the use of 'computers' to avoid struggle from employee unions. However, this was the most important period acting as the icebreaker, which leads to the slow and stable move towards large scale technology adoption in Indian banks.

The world is rapidly moving online with 46.1% of total world population now connected to the network according to internetlivestats.com (as on May 1, 2016). A notable example of this phenomenon has been accomplished in India with a prominent increase in the past three years i.e. 18% of the Indian population online in 2014, 27% in 2015 and 34.8% in 2016 (as on May 1, 2016).

ISSN: 2348-3989 (Online)
ISSN: 2230-9764 (Print)
Doi: http://dx.doi.org/10.11127/gmt.2018.03.07
pp. 30-33

Global Scenario

The international online banking industry has been playing an increasingly significant role in recent years within the online financial services industry, motivated by extensive internet penetration and changing consumer behavior.

Development in the e-commerce segment has seen more customers make the change from paper payments to online payments. Customers are now demanding a better degree of transparency and flexibility in their banking transactions. According to yStats, there will be almost 3.5 billion internet users across the globe in 2017, marking a 1 billion increase in four years. Financial service providers are under difficulty to find ways to set themselves apart to capture the maximum proportion of the active online customer base as competition stiffen in the sector.

Problem Statement

Today, technology enabled banking services has emerged as an fundamental and essential part of the Indian Banking sector. The improvement of non-cash based transactions around the globe has resulted in the stable expansion of robust online payment systems. Coming to paper-based transactions cleared through cheques amounted 793.1 million in 2014-15 and in 2015-16 729.3 millions. India has seen a rise in the volume of debit/credit cards due to increased technology enabled services. In the days to come, this size will gain grip as the younger generation will enter the economic twist. The last few years have seen a significant increase in cybercrime across all sectors and geographies. Given the explosion of these technological attacks, organisations face a important challenge to be resistant against cyber-attacks. This research attempts to analyze various forms of cybercrimes, threats to banking sector how to overcome these situations.

Impact of Cyber Crime Technology Enabled Banking Services

Cybercrimes are increasing globally and India too has been witnessing a sharp increase in cybercrimes related cases in the recent years. The sectors prone to cyber-attacks are:

Table-1: Sectoral Analysis of Cyber Attacks

Sector	% of cyber attack
Consumer/ Industrial market	3%
Government	8%
Infrastructure	11%
Financial Services	58%

Source: Cyber-crime report 2016

Types of Cyber Crimes

There are few techniques in which a cybercrime can be committed. Here we have to aware how these crimes will be affected our computer privacy. In this section, we talk about a few common tools and techniques used by the cyber criminals. This isn't a comprehensive list by any ways, but will give you a complete picture of the gaps in networks and security systems, which can be misused by attackers, and also their possible causes for doing such crimes.

1. **Hacking**: In simple, hacking is an action committed by an intruder by accessing our computer system without our permission. Hackers are primarily computer programmers, who have a superior understanding of systems and commonly misuse this knowledge for tricky reasons. They're usually technology experts who have expert-level skill set in one particular software program or language.
2. **Virus:** Viruses are computer programs which will spread like a biological virus or infect a computer or files, and have a tendency to combine other systems on a network. They interrupt the computer operation and affect the database either by altering it or by removing it altogether. They just reproduce until they consume up all available memory in the computer.
3. **Logic bombs:** Logic bomb, also called as "slag code", is a horrible piece of code which is intentionally inserted into software to execute a malicious task when generated by a specific event.
4. **Denial-of-Service attack:** Attack is obvious attempt by attackers to deny service to prospective users of that service.
5. **Phishing:** This technique is used for removing confidential information such as credit card numbers and username passwords. Phishing is typically carried out by email tricking. The malware would have installed itself on the computer and stolen private data.
6. **Data diddling**: Data Diddling is an unlawful altering of data before or during entry into a computer system, and then altering it back after processing is completed. Using this technique, the attacker may change the expected outcome and is difficult to track.
7. **Keystroke Logging or Key logging**: Key logging is a process by which attackers' record actual keystrokes and mouse clicks. Key loggers are "Trojan" software programs that aim at computer's operating system and are "installed" via a virus. These are very dangerous because the fraudster captures user ID and password, account number, and anything else that has been typed by the user.
8. **Spyware:** Spyware is a technique to stolen online banking credentials of the users for fraudulent activities. Spyware works by capturing information either on the computer while it is transforming between the computers and websites.
9. **Watering hole:** "Watering hole" cyber fraud is considered to be a branch arising from phishing attacks. In watering hole a malicious code is injected onto public web pages of a website which is visited only by a small group of people. In a watering hole attack situation,

when the victim visit the site injected with malicious code by attackers the information of such victim is then traced by the attacker

10. **Credit Card Redirection and Pharming:** Pharming is connected with the words, 'farming' & 'phishing'. In Pharming a bank's URL is hijacked by the attacker in such a manner that when a customer log in to the bank website they are redirected to another website which is false but looks like an original website of the bank. Pharming is done over Internet and Skimming is another method which occurs usually in ATMs.
11. **DNS Cache Poisoning**: DNS servers are deployed in an organization's network to improve decision response by caching before obtained query results. Poisoning attacks against a DNS server are made by exploiting exposure in DNS software. That causes the server to wrongly validate DNS responses that ensure that they're from an authoritative source. The server will end up caching incorrect entries locally, and serve them to other users that make the same request.

Current Scenario of Cyber-crimes in Banking Sector

Table-2: Cases Registered Under Cyber Crimes Categorized By Motives and Suspects from 2010 – 2015

Motives and Suspects	2010	2011	2012	2013	2014	2015
Revenge/settling	38	70	87	112	285	304
Greed/Money	161	306	624	821	1736	3855
Extortion	24	27	48	73	199	295
Cause Disrepute	36	82	117	148	272	387
Prank/ satisfying of gaining control	13	77	45	39	110	214
Fraud/Illegal gain	266	487	668	1116	495	1119
Total	**538**	**1049**	**1589**	**2309**	**3097**	**6174**

Source: National Crime Report 2016

Table 3: Incidence of Cyber Crimes cases Registered during 2010-2015

Crime Type	2010	2011	2012	2013	2014	2015
Tampering Computer Source Document	64	94	161	137	89	88
Loss/ Damage to computer resource/utility	346	826	1440	1966	4192	4154
Hacking	164	157	435	550	784	1081
Obscene publication/ Transmission in electronic form	328	496	589	1203	758	792

Source: National Crime Report 2016

Table-4: Cases Registered Under Cyber Crimes Cauterized by Motives and Suspects from 2010-2015

Motives and Suspects	2010	2011	2012	2013	2014	2015
Revenge/settling	38	70	87	112	285	304
Greed/Money	161	306	624	821	1736	3855
Extortion	24	27	48	73	199	295
Cause / Disrepute	36	82	117	148	272	387
Prank / satisfying of gaining control	13	77	45	39	110	214
Fraud / Illegal gain	266	487	668	1116	495	1119
Total	**538**	**1049**	**1589**	**2309**	**3097**	**6174**

Source: National Crime Report 2016

From the above tables we can understand that the financial services sector faces specific challenges of its own. Banks are struggling with the decentralization of their services through digitization. The growth of Fintech throws pressure on the banking sector where the technology and e-commerce companies are now competitors to and partners with banks. Banks have to believe that having an effective digital strategy is one of the important priorities. Accompanying this will be the change management of the shift. Technology on its own improves nothing. But people using technology competently and effectively can make a big difference.

Causes for Cyber Crimes

Cybercrime -- including everything from identify theft and hacking to virus distribution and computer fraud -- is difficult areas of criminology. Computers are important in our lives and handle more number of our personal data. Like other areas of crime, its causes are sometimes complex to establish, but certain trends in cybercrime are rising. As far as banking sector is concern it have to maintain huge database of their customers the trends in cybercrimes are creating threat to banking sector.

Financially Motivated Cyber Crime

As is the case with many crimes committed outside the Internet, money is a major motive for many cyber criminals. Especially because the threats of criminality are less evident when you're hiding behind a network, the perception of low risk and very high financial reward prompts many cyber criminals to employ in malware, phishing, identity theft and fraudulent money request attacks.

Personally Motivated Cyber Crime

Cyber criminals are still human beings and what they do – with their crimes -- is frequently the cause of personal emotions and disputes. There are many forms of cybercrimes like from the motivated employee installing a virus on office computers to a jealous boyfriend hacking into a girlfriend's social media accounts or a teenager taking down a school website just to prove that he could do it, many cybercrimes are basically crimes of passion dedicated over the Internet.

Ideologically Motivated Cyber Crime

These kinds of attacks are conducted for apparent ethical behavior, ideological or moral reasons, damaging or disabling computer equipment and networks to convey grievances against individuals, corporations, organizations or even national governments.

Operational Causes

The reason that stimulate criminals, the environment in which cybercrime is committed also serves to clarify the incidence of the phenomenon. While more and more personal and sensitive data is stored online -- increasing the possible rewards for cyber criminals -- neither computer security nor applications like email filters have enhanced extremely in terms of coverage. According to the anti-virus manufacturer Norton, for example, as many as 41 percent of computers did not have up-to-date security protection in 2014.

Preventative Steps

One of the best ways to keep attackers away from your computer is to affect patches and other software fixes when they happen to offered. By regularly updating our computer, we can block attackers from being able to take advantage of software flaws (vulnerabilities) that they could otherwise use to pause our system.

More recent versions of Microsoft Windows and other accepted software can be configured to download and apply updates mechanically so that we do not have to recall checking for the latest software. Taking advantage of "auto-update" feature in our software is a great start toward keeping our self safe online. Keep in mind that a recently purchased computer may not have the right level of security. When we are installing in our computer, we have to pay attention not just to making our new system function, but also focus on making it work securely.

Passwords are a reality of life on the Internet today—we use them for everything from ordering flowers and online banking to logging into our favorite airline, Web site to see how many miles we have accumulated, to book movie tickets, to order food etc.

Security software's are essential for basic online security. Security software essentials include firewall and antivirus programs. Here we have to be very cautious when we are sharing personal information such as name, home address, phone number, and email address via networks.

To gain advantage of many online services, you will surely have to provide personal data in order to handle billing and shipping of purchased goods. The impact of identity theft and online crimes can be greatly minimize if you can catch it shortly after your data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by evaluating the monthly statements provided by your bank and credit card companies.

Additionally, many banks and services use fraud prevention systems that call out rare purchasing behavior. In order to verify these out of the ordinary purchases, they might call you and ask you to confirm them. Don't take these calls lightly-this is your hint that something bad may have happened and you must think tracking some of the activities cited in the area covering how to respond if you have become a sufferer.

Conclusion

In India the cybercrimes are increasing considerably. The crimes such as social media, credit card fraud, phishing, and virus, Malware, Denial of services, Gambling, Personal data break, corporate data break and virtual currency are frequently done by cyber criminals. Most of the cybercrimes are devoted at nationalized banks. Maximum sufferers are suffered from money loss and data loss. The internet is the medium for transforming of huge information, it is essential to take certain precautions while sharing information through systems. It is very vital to educate users of internet regarding these cybercrimes and explain them what precautions they have to take to safeguard their computers as well as personal data. In this regard banks may have to take utmost care regarding their firewall and anti – virus systems.

References

- National Crime Record Bureau: Cybercrimes statistics in India 2014: http://ncrb.gov.in/pdf.
- Manisha M. More and Nalawade, K. M. (2014): Cyber Crimes and Attacks: The Current Scenario. 1st National Conference organized by NESGOI, Pune.
- Susheel Chandra Bhatt and Durgesh Pant. (2011). Cyber Crime complaints 2015:http://rbi.org.in/Press-release.
- Assocham India: Cybercrimes in India, study by 2015, The Associated Chambers of Commerce & Industry of India
- Computer Emergency Response Team (CERT): http://cert.India.com
- Cyber Crime complaints 2015:http://rbi.org.in/Press-release