CYBER CRIMES AMONG THE FINANCIAL INSTITUTIONS: AN OVERVIEW

Dr.N.Ramesh Kumar Professor, Department of Management Studies

S.V.S Group of Institutions, Warangal.

Dr.K.Sravan Kumar Asst.professor, Department of Management Studies

S.V.S Group of Institutions, Warangal.

Abstract

The digital world has transformed almost every aspect of our lives including risk and crime. Financial institutions are an obvious target for cybercrime. Cybercriminals increasingly target online banking and mobile apps. In the current digital era, it is imperative that the financial institutions enhance investments in security, fraud prevention, customer education, and privacy of personal information to enhance trustworthiness. In view of its growing concern the present study is conducted to focus on aspects like major trends of cyber crimes among the financial institutions, cyber crime threats to financial institutions and challenges faced by them with such crimes.

Key words: *cyber crime***,** *financial institutions, Digtal world*

I. Importance of the study

According to recent research, financial fraud has grown substantially in recent years. Financial cybercrime and identity theft in India are increasing. There is a dramatic correlation in India between booming adoption of mobile apps, digital payments and increasing rate of financial fraud. 96 percent of Indian consumers who were victimized by financial fraud during the last year had switched to a mobile app and digital payments, from cash as mode of payment, significantly impacting the country's efforts towards financial integration. Though Indians have embraced digital transactions, they are yet to learn the dos and don'ts of sharing personal information, as social engineering and phishing emails are rampant. The importance of consistent security hygiene remains vital to addressing the total scope of these attacks. That's why financial institutions including banks, credit unions, brokerages, and payments companies need to take a layered approach to cyber security and fraud prevention.

II. Objectives of the study

1. To study the theoretical aspects of cyber law.
2. To find out the major trends of cyber crimes prevailing in financial institutions.
3. To assess the recent cyber security threats among the financial institutions.
4. To discuss the major challenges to cyber security among financial institutions.

III .Theoretical aspects

Cyber Crime: It is a crime where use of computers coupled with the use of internet is involved.

Cyber Law: It is a term which is related to all legal issues involving computer and internet. It is an intersection of various fields like privacy issues, intellectual property rights issues.

Cyber Attack: It is a deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber criminals use malicious code, logic, or data resulting in disruptive consequences that can compromise data and lead to cyber crimes.

IV. Recent trends in cybercrime related to financial Services

- The ultimate purpose of most cyber attacks is financial gain by the theft of information, whether credit card or banking data or the selling of PII on the dark web, ultimately involves taking advantage of someone or some organization associated with the financial services sector.
- According to the recent Threat Landscape Report, around one third of organizations experienced a mobile malware attack in 2018, in which majority of them targeting or originating from devices run by Android operating system.
- Exploits targeting banking apps on mobile devices. Compromising mobile devices not only allows attackers to steal data stored on that device, but can be used to collect personal banking information using phishing apps, intercept data moving between a user and his or her online bank, and monitor financial transactions when purchasing goods or services online. A malware can target several banking apps to steal login credentials, hijack SMSs, and upload contact lists and other data onto a malicious server.
- These apps are being downloaded from risky sites. Though most of such Trojans masquerading as legitimate apps were removed from the Google Play store, but only after they had been installed by over many users. But even that is only part of the exposure. Compromised devices are also becoming a gateway through which the larger financial services network can be exploited.

Some of the major types of cyber attacks are discussed below

1. Crypto jacking: This has become a gateway for other attacks. In many industries, including financial services, crypto jacking has leapfrogged ransom ware as the malware of choice. While ransom ware continues to be a serious concern for financial networks, the number of unique crypto jacking signatures nearly doubled in recent past, while the number of platforms compromised by crypto jacking is also increasing. Perpetrators include advanced attackers using customized malware, as well as “as-a-service” options available on the dark web for novice criminals. Although crypto jacking is often considered to be a nuisance threat that only hijacks unused CPU cycles, a growing number of new attack techniques include disabling essential security functions on devices, thereby enabling crypto jacking to actually become a gateway for additional attacks.

2. Botnets: It is a combination of words ‘robot’ and’ network’. This term is used with a negative or malicious connotation. It is a number of internet-connected devices, each of which is running one or more bots which can be used to performed distributed denial of –service attack(D. D.o.s attack),steel data, send spam and allows the attacker to access the device and its connection.They are getting smarter. The number of days that a bonnet infection was able to persist inside an organization increased these days, indicating that bonnets are becoming more sophisticated, difficult to detect, and harder to remove. This is also the result of many organizations still failing to practice good cyber hygiene, including patching and updating vulnerable devices .many botnets can go dormant when detected and may return after normal business operations have resumed if the root cause or has not been addressed.

V. Emerging cyber security threats to financial institutions

1. **Identity Theft**: It is the crime of using someone’s personal information, credit history or other identifying characteristics in order to make purchases or borrow money without that person’s permission.

When there’s a large-scale data breach, much of the personal information hijacked from the breach is soon be available on the dark web, where it can be bought and sold and appended to other data acquired from other breaches to perpetrate identity theft and account takeover on a grander scale.

2. Account Takeover: It is using another person's account information to get products and services using that person's existing accounts.

To execute this attack, a cybercriminal first gains access to a trusted email account, then uses this account to launch subsequent email attacks for financial gain or to execute a data breach. Such attacks are dangerous and effective because they originate from email accounts of trusted senders via phishing attacks. This has two important ramifications. First, the attack is very likely to succeed because there is a pre-existing trust relationship with the customer. Second, these attacks often go undetected by traditional security controls since they originate from legitimate accounts.

3. Synthetic Fraud: which occurs when criminals create a fictitious identity using various pieces of real and fabricated information such as a Social Security number, date of birth, address, phone number and email? The immediate victim is the bank or lender, but long-term, whoever's Social Security number is used, will have to deal with the impact of any accounts or debts attached to them fraudulently.

By all appearances, these fictitious people can seem like ideal customers, with multiple "proof of life" indicators, including their own social media profiles. And when they take out credit, they tend to pay bills promptly and nurture accounts for months or even years. It's important to note that monetary losses are just part of this attack; financial institutions also need to dedicate time, energy and resources to chase down these non-existent identities.

What's particularly worrisome about this new method of compromising the systems used to validate identities at account opening is that it's working.

4. Ransom ware: It is a type of malicious software designed to block access to a computer system until a sum of money is paid. Ransom ware is always triggered by an employee clicking on a link in a phishing email that they shouldn't and clicking the link ignites the malware.

It is non-negotiable for financial services companies to maintain the privacy of their customers and the security of their confidential data. If a bank or credit union is hit with a ransom ware attack, significant backlash is undoubtedly going to ensue particularly if customer data is held ransom for a significant amount of time.

5. Social Engineering: It is a method of deceiving people into giving their information, or exploiting their weakness, or laziness, to find the information.

Social engineering attacks are designed to trick the employees into granting access to systems or divulging information that helps attackers gain that access. Such attacks can come in many forms namely phone, email, snail mail, in person or through social media.

VI. Major Challenges

- Financial companies must improve the way they deliver their services, manage security risks, and train their employees.
- The challenge being faced by many financial organizations is that new digital transformation efforts have spread security resources thin, restricting visibility and fragmenting the controls of many I.T teams.
- Though financial institutions are putting cyber security systems in place to curb the scourge the preventive measures are being outpaced by technological advancement.
- Digital transformation requires an equivalent security transformation effort. This includes shifting from point security products, manual security management, and reactive security to a strategy where different security elements are integrated into a single system.

➢ As the speed of threats rapidly increases, the time windows for prevention, detection, and remediation continue to shrink. Rapid response times are crucial, which makes the implementation of truly expansive and integrated security automation essential, from data collection to coordinated responses to threats.

Making matters worse, cybercriminals are adopting new technologies, increasing their coordination and becoming more sophisticated. They're compromising employees' and customers' personally identifiable information (PII) for use in illicit schemes elsewhere. Thanks to large-scale data breaches, they're leveraging the dark web to take over legitimate accounts.

VII. Conclusion

Building the requisite safeguards to protect their assets, customer data and reputation. The security teams of financial services organizations need to rethink their strategy. Cyber security issues have been a bane for many industries. But firms operating in the financial sector have been the worst affected . security teams of financial services organizations need to rethink their strategy, from automating their security hygiene measures to replacing isolated security devices with an integrated security fabric architecture that can seamlessly span the growing attack surface.

VIII. Suggestions

Organizations should regularly scan the internet for fraudulent applications, warn consumers when they are found, and apply pressure on application stores to remove them. It's clear that there is no one-size-fits-all approach to cyber security readiness. It invariably requires an enterprise-wide approach tailored to the culture of your financial services organization, accounting for regulatory requirements. financial services organizations need to rethink how they capture and establish digital identities of new customers and verify high-risk transactions and leverage innovative solutions to ensure that your customers are who they claim to be. To do this, organizations need to implement an integrated security platform where each element is designed to communicate with all the others in real time.Identifying and tracking all mobile and I.oT devices. One essential approach to combating things like crypto jacking involves maintaining a comprehensive inventory of devices through third-generation network access controls and then base lining their behavior.To protect these customers, start by educating them about your legitimate banking applications. Such as online "password validation" or "account validation" techniques used by phishes and scammers. So, it's important to train the employees to avoid cyber crimes.

References

1. Nappinai N.S(2010), Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study,"**Journal of International Commercial Law and Technology" 5(1), January 2010**

2. Cyber security Threats Facing Financial Services, Dean Nicolls,Nov,2018

3. Cybercrime Trends and Financial Services, By Anthony Giandomenico , Jan,2019

4. Identity Fraud Study by Javelin Strategy & Research. 2018

5. KSN Report: Ransom ware malicious crypto miners 2016-2018"),

6. www.Google.com

List of abbreviations

1. P.I.I-Personal Identifiable Information.
2. App.-Applications.
3. I.T-Information Technology.
4. I.o.T-Internet of Things.