Financial Services: Security Challenges

"It's not a matter of if you will be breached, but just a matter of when." – Gary Meshell

Introduction

Financial Services have been and are still a significant target to cybercriminals and the black market. Because of the number of money cybercriminals can produce through hacking an individual's bank account, financial services are at the forefront of most cyber attacks, and therefore require a high level of cybersecurity.

Additionally, financial services must fulfill high-level compliances in order not to get penalized and construct a more reliable brand because many financial service users attend institutions that are compliant so that their information is secure.

In turn, financial services are not only vulnerable on the outside due to the number of compliance requirements and cybercriminal activity, but also on the inside because employees potentially steal money from within the company.

Security Issues

Financial Services Statistics

In the past three years, hackers stole six billion records. This means that every day, more and more regulations must be placed to minimize that number. For example, banks and other financial institutions in the United States must comply with multiple data protection regulations. These regulations are highly strict, and they will get more stringent throughout time. Collection, retention, and the process and sharing of personal information must be secure, and these actions are supervised continuously.

According to IP Switch, in a recent email spoofing attack, employees of a secret organization were asked to respond with their username and password. Out of the employees, 60% of them complied and sent their information.

Financial services require a high level of security, but there are many reasons why the security failed, and the hackers breach the day.

Backdoors and Supply Chain Attacks

Some cyber attacks are performed through "backdoors" or applications used to obtain remote access. With backdoors, hackers gain access to the network by bypassing any

detection systems. Backdoors are pieces of code that hackers implement within the system to allow easier access into the net.

Port binding, connection availability issues, and custom DNS lookups are examples of backdoor attacks.

Third Party Vendors

Being involved with third-party vendors may result in a data breach. 59% of companies reported that data breaches are from third-party vendors. Through third-party vendors, not only do they have access to the company's information, but also, they might allow cybercriminals to get into the company.

Third party vendors must agree to protect the company's information and not betray the company. As well, third-party vendors cannot get hacked because if a third-party vendor gets hacked, the company that they sponsor may also get hacked.

Employees

However, most of the attacks that significantly affect a financial institution are cyber attacks from inside the company. 60% of all cyber attacks are from employees. According to IBM, financial firms and services were in the top three sectors that were targeted by the inside. There are two types of employee-related cyberattacks: unintentional and intentional.

Out of the employee-related cyberattacks, 75% of them are intentional. Employees who have gone 'rogue' or against the company due to recently being fired or past employees whose data still works within the network are the types of employees that intentionally create cyberattacks. Employees can offer their username and password to a hacker to allow the hacker to gain access into the server, system, and overall secrets behind the company. After all, it saves the hacker much time and effort because they already have the necessary information from someone within the company.

The other 25% of insider attacks are from human error and are unintentional. Phishing scams, employees accidentally giving away their credentials, downloading malware through email, and staying logged into the company's network through a public computer are ways that employees can unintentionally create a cyber attack.

The Cybersecurity Threat Landscape

Financial services must start to recognize that being breached is more of a "when" rather than an "if."

These firms face a long list of complex risk factors:

- Geopolitical
- Phishing attacks
- Cyber fraud as known as executive digital impersonation
- Insider risk
- Supply chain risk

The number of attacks on financial services is increasing, and hackers are using phishing attacks to gain employee credentials and social engineering to narrow which employees have access to the finances of the financial institution.

According to IBM, TD Bank is taking down 12 fake LinkedIn profiles of the TD Bank CEO per month to stop employees from linking to that account.

One of the biggest challenges is the talent gap to respond and sustain the response to attacks. Primarily, financial services are always playing defense; no financial assistance gets on the offense during a cyber attack. As well, many financial services coordinate with a third-party vendor for live responses and protection but relying on third-party vendor results in a very late reaction or hackers performing cyber attacks through the third-party.

Regulatory Compliance

PCI-DSS

PCI-DSS was otherwise known as the Payment Card Industry-Data Security Standard is a widely accepted set of policies and procedures intended to optimize the security of credit, debit, and cash transactions and protect cardholders against the misuse of their personal information. This compliance standard was released in 2004 by the joint-partnership of the four major credit card companies: Visa, MasterCard, Discover, and American Express.

For a financial institution to be PCI-DSS compliant, the service must obey six objectives labeled as followed:

1. Supervisors conduct transactions in a maintained, secure network where there are firewalls that are not inconvenient to the cardholders nor vendors, but robust to be effective against potential cyber attacks.
2. Wherever this data is stored, financial services must protect cardholder information, i.e., vital data of birth, mother's maiden name as a standard answer to a business account, social security numbers, phone numbers, and mailing addresses. The second objective also involves digital encryption and its importance in credit-card transactions within e-commerce.

3. The payment system must be protection against malicious activities through frequently updated anti-virus software, anti-spyware programs, and other anti-malware solutions.
4. The access to the system information and operations must be restricted and managed by trusted employees, and every person who has computer access in the system obtains a unique and confidential ID name or number.
5. Networks will be constantly monitored and tested to ensure that it is compliant with security measures.
6. A formal information security policy must be defined, maintained, and always followed.

GLBA

GLBA which is known as the Gramm-Leach-Bliley Act requires financial institutions to explain how they share and protect their customer's private information. The focus on the GLBA is to tighten consumer data privacy safeguards and restrictions. This act revolves around three rules that financial services have to follow to be GLBA compliant.

The Financial Privacy Rule mandates that the financial institution provides notices of privacy policies and practices to consumers. The institution has to offer consumers the options to opt in or out of having their national provider identifier disclosed to non-for affiliated third-parties.

The Safeguard Rule requires that relevant financial institutions implement policies for protecting customer information which is defined as individuals that maintain a relationship with your organization.

The Pretexting Provisions is another GLBA standard that involves cybersecurity which encourages financial institutions to develop safeguards for pretexting or social engineering, and organizations develop a written plan for monitoring account activity, i.e., training staff not to provide NPI to fraud entities.

These standards and rules of GLBA apply to all business, regardless of size, as long as they are engaged in providing financial products or services to consumers, so not only financial institutions, but also check-cashing companies, payday lenders, mortgage brokers, and other functions involving the transaction of money.

Financial Institutions should employ encryption to mitigate the risk of disclosure, and encryption methods include effective key management and encryption strength.

Failure to be GLBA compliant results in a fine of $100,000.

J-SOX

J-SOX or the Japanese Sarbanes-Oxley Act defines Japan's financial instruments and exchange laws and is a basis for many financial institutions. The institution has internal controls over financial reporting which include financial statements.

Biometric Solutions

Many financial services organizations are addressing the challenge of roving employees – shared workstations by integrating a layer of biometric authentication. Superior to passwords or swipe cards, biometrics cannot be lost or shared. One touch instant authentication provides security while complimenting the streamlined workflow, benefiting the organization and enhancing the customer experience. As bank employees migrate from the drive-thru windows to the lobby and as supervisors bounce from computer to computer authorizing high-end transactions, biometrics becomes a "must have".

Scott Mahnken
VP Marketing
BIO-key International

https://www.thalesesecurity.com/solutions/industry/financial-services

https://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

https://www.eisneramper.com/j-sox-sarbanes-oxley-act/

https://www.ibm.com/blogs/insights-on-business/banking/the-cyber-security-threat-landscape-in-financial-services/?cm_mmc=OSocial_Voicestorm-_-Financial+Services+Sector_Banking+and+Financial+Markets-_-WW_WW-_-Elevate&cm_mmca1=000000QJ&cm_mmca2=10001385

https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act

https://www.blackstratus.com/compliance/glba-compliance