us signal

Navigating Banking Cybersecurity Challenges

In the Age of Digital Transformation

Table of Contents

Chapter 1: Introduction

Digital banking has been growing and gaining momentum in recent years. More customers are using digital online services in every aspect of their lives, including banking. In 2021, mobile banking was the primary choice of account access for 43.5% of U.S. consumers, making it the most prevalent banking method. And in 2022, it's estimated that over 200 million U.S. customers used digital banking.

The rise in digital banking reflects a trend across all industries: consolidating locations. From 2017 to 2021, 9% of all bank branch locations in the U.S. closed down.

This accelerated migration toward banking online has dramatically increased demands on network resources, and adds several major concerns regarding security, privacy, compliance and maintenance. Computer systems age faster than a bank vault, after all, and poorly maintained legacy systems are hard to protect.

This eBook takes a closer look at the growing trends in digital banking systems, the potential pitfalls of the same, and how to manage the cybersecurity risks involved with proactive planning and mitigation in financial institutions.

Chapter 2: Trends in Banking That Drive Customer Experience

Some of the primary drivers behind banking's digital transformation are the growing customer demand for an improved customer experience, the desire to increase operational efficiency and the need to remain competitive in a connected world.

While technology helps banks meet these needs, it also opens financial institutions to risks that brick-and-mortar branches never had to face. Instead of security cameras and guards, today's banks need a cybersecurity plan to protect their critical data.

The fact of the matter is today's financial services customers expect convenience, speed and accessibility in their banking interactions — at the same time, their information and transactions must remain safe from bad actors. Several trends are emerging in this new landscape, and banks must keep up with the changes without compromising cybersecurity.

Customer demand for seamless experiences

Customers today want to be able to perform a wide range of transactions and access banking services anytime, anywhere. They also want their transactions to look and feel the same, whether they're on their phone, at their computer or using a kiosk at their bank.

At the same time, internet access and smartphone apps empower customers to seek out digital solutions that simplify their financial activities. Online and mobile banking applications have led to a seismic shift in consumer behavior and a rise in banking on the go. Customers now can do anything they can do from their brick-and-mortar bank from their preferred device — check account balances, transfer funds, pay bills, and even apply for loans or credit cards.

Banks are leveraging technology to enhance their services and provide seamless experiences across various touchpoints. Customers can now move consistently and easily across mobile, online and in-person banking.

Yet this increased convenience comes at a cost. With more technology, attackers are finding more ways to enter networks and access sensitive customer data. Financial institutions must invest in robust cybersecurity measures to ensure customer information doesn't end up in the wrong hands.

The drive toward end-to-end, hyper-personalized customer journeys

Banks are leveraging customer data and advanced analytics to create tailored solutions, products and services that address real-time customer requirements. By understanding each customer's individual needs, banks can offer recommendations such as customized portfolios, loan offerings or financial advice.

These services benefit not only customers but banks themselves, by allowing them to streamline processes and reduce costs. However, the storage, integrations and APIs required to deliver these services open additional potential attack vectors, increasing the need for a comprehensive security posture.

Chapter 2: Trends in Banking That Drive Customer Experience Cont.

Competition from and within fintech

The rise of fintech companies — innovative startups that digitize banking to provide financial services in a more agile, user-friendly and cost-effective manner — have disrupted the traditional banking sector. Fintech companies offer convenient and personalized solutions such as:

- **Mobile banking apps**
- **Digital wallets**
- **Peer-to-peer lending platforms**
- **Robo-advisors**
- **Blockchain-based services**

To compete, banks have reevaluated their strategies and invested in online and mobile platforms, as well as emerging technologies like AI, advanced analytics and edge computing. As banks move toward offering a seamless omnichannel experience through multiple touchpoints, they must design and develop these advanced systems with a DevSecOps mindset — working security into the development process from start to finish.

Open banking

Open banking is the practice of sharing financial information and data securely between different financial institutions using application programming interfaces (APIs). Open banking enables financial institutions to:

- **Gain access to customer financial data, with their consent**
- **Develop innovative and personalized financial services and products**
- **Empower their customers by giving them greater control over their financial data**
- **Increase competition and innovation through collaboration between traditional banks and fintech startups**

However, it also presents security and privacy challenges. Sharing financial data requires robust security measures to protect against phishing, ransomware and Denial of Service (DoS) attacks.

Chapter 3: Cybersecurity Challenges Of Banking Modernization

By digitizing their operations, banks rely on a much more complex IT infrastructure with numerous interconnected systems, applications and databases, creating:

- **A larger attack surface**
- **More vulnerabilities**
- **More opportunity for costly human errors**
- **Lower visibility across the environment**
- **Higher risk of shadow IT**

Keeping these organizations secure takes planning, monitoring, and constant patching and updating.

Of course, the crux of this challenge is this: convenient, user-friendly experiences increase security risk. At the same time, implementing high security standards can hinder the user experience. Unless financial institutions find a way to balance convenience and security with an optimal customer experience, they can get caught in an endless priority loop.

Of the cybersecurity challenges that financial institutions face, five primary areas make up the heart of the problem.

1) Legacy Systems

Financial institutions often rely on legacy systems that were designed and implemented before the rise of modern cyber threats. These systems may be more vulnerable to attacks due to outdated software and a lack of necessary security features. Legacy systems may also have hidden weaknesses that cybercriminals can exploit, making it crucial to invest in upgrading and securing these systems.

Another challenge of legacy systems is in integrating new technologies due to compatibility issues that may create security gaps. Updating legacy systems can also represent a significant expense, in terms of investing in software, hardware, and employee time. For these reasons, some financial institutions may be reluctant to make the upgrade — and the risks of this move are plentiful.

2) Internal Resistance to Change

Another major cybersecurity challenge for financial institutions may come from within. Resistance to change from within an organization can hinder the adoption of new technologies and security measures.

Employees may have concerns about increased complexity, training requirements, or potential disruptions to their established workflows. This can lead to delays in implementing new security protocols or modernizing systems.

3) Customer Data Privacy and Security

Financial institutions handle vast amounts of sensitive customer data, from financial information to personal information. This data is vulnerable as organizations modernize systems and enhance online experiences. Cybercriminals are constantly looking to exploit vulnerabilities and gain unauthorized access to customer data for identity theft, fraud, or other malicious purposes. In 2022, more than 60% of global financial institutions with at least $5 billion in assets were hit by some sort of cyberattack. While larger, Fortune 500 institutions are often targets, hackers also target medium-sized to smaller banks

Chapter 3: Cybersecurity Challenges Of Banking Modernization Cont.

4) Advancing, Intelligent Cyberthreats

As technology advances, so does the threat landscape. Cybercriminals employ sophisticated technologies like artificial intelligence, automation and advanced malware to break through the network perimeter.

Some of the attacks financial institutions face include:

- Advanced persistent threats (APTs), designed to gain long-term access to a bank's systems.
- Ransomware attacks, which hold data hostage until the bank pays a ransom to the attackers.
- Social engineering attacks, such as phishing scams, where users are tricked into giving away sensitive information.
- Insider threats, where employees or contractors with access to critical systems can cause harm — intentionally or unintentionally — by leaking information or introducing malicious code.
- Artificial intelligence (AI) and machine learning (ML) to automate attacks and evade traditional security measures.

Financial institutions must face these new challenges by deploying advanced threat detection and response mechanisms, such as AI-powered security analytics and anomaly detection, to effectively counter these evolving threats

5) Complex, Evolving Regulatory Compliance

Financial institutions operate under strict regulations and compliance requirements to protect customers and maintain the integrity of the financial system. Compliance frameworks such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS), and industry-specific regulations make cybersecurity practices even more complex.

Institutions that digitize must ensure compliance with these evolving regulations while implementing robust security measures. This requires:

- Continuous monitoring
- Updated policies and procedures
- Risk assessments
- Strict security measures
- Employee awareness
- Proactive cyber defense

These actions are crucial to protect financial institutions and their customers

Chapter 4: Recent Cybersecurity Breaches In Financial Institutions

Today, cyberattacks in the financial industry are not if situations — they are when situations. In 2022, 47% of all businesses in the U.S. suffered an attack in some way. In the banking sector, the stakes are high, and it's not unusual for costs to run into millions or billions of dollars.

Here are five recent real-life examples of financial institutions that were hit by data breaches, including the cost of the attack and how the systems were breached.

Latitude Financial Services

On March 16, 2023, Latitude Financial Services disclosed that an attacker stole an employee's login and breached two service providers that hold Latitude customer data. The largest known data breach of an Australian financial institution, this attack exposed customer data from 14 million loan applicants in Australia and New Zealand. The stolen customer data included addresses, dates of birth, driver's license numbers, and passport numbers. Latitude refused to pay a ransom demand, and the cost of this breach isn't yet known.

Blockchain Project Ronin

Blockchain project Ronin lost $615 million in ether and USD Coin tokens on March 23, 2022. The second largest cryptocurrency heist ever happened when hackers exploited a feature allowing users to transfer their assets from one crypto network to another.

Cream Finance

The decentralized finance ("DeFi") platform Cream Finance lost $130 million on October 27, 2021, after attackers exploited a vulnerability in the platform's lending system and stole all of their assets and tokens running on the Ethereum blockchain. This attack came after the company lost $29 million in August and $37 million in February of the same year.

Liquid Cryptocurrency Exchange

The Japanese cryptocurrency exchange Liquid lost $97 million worth of digital coins on August 18, 2021, when hackers transferred assets out of a multiparty computation wallet. This attack happened only one week after the Poly Network attack, below.

Poly Network

On August 10, 2021, in one of the largest cryptocurrency heists ever, hackers exploited a vulnerability in the Chinese blockchain site Poly Network and stole $600 million worth of digital tokens. The hacker returned half of the funds within hours, and the remainder 13 days after the attack. The identity of the hacker hasn't been revealed.

Chapter 5: How an IT Service Provider Can Help Banks Secure Their Environment

Before your banking institution can improve its cybersecurity, it needs to know the current state of its operation. That's why at OneNeck, we recommend you start with a cybersecurity risk assessment.

After our security experts assess the current state of security and compliance at your organization, they prioritize steps to mitigate your risk, offer solutions to thwart future attacks and provide support in the event of a breach. The entire process is as follows.

1) In-Depth Assessment

Using proven frameworks, like the Center for Internet Security (CIS) Controls framework, we conduct an in-depth assessment, provide you with an understanding of your current risks and give you clear steps to address them. The framework-based assessment helps you establish a systematic approach to cybersecurity that prioritizes the most critical areas first and then builds a strong defense against cyber threats.

2) Security Strategy

Once we have your baseline risks, we give you clear steps to address them. We create an effective IT security strategy that protects your environment from DNS to network to endpoint. We'll help with actionable steps to assess cyber risks and maximize security investments. We'll also give you best practices for preventing and responding to threats and navigating cloud security

3) Security Defense Implementation

There's no single cyberthreat anymore. Today's complex cyber attacks require complex security solutions. In addition to ala carte security services based on your unique environment and requirements, OneNeck has created three IT security packages to help organizations at all levels establish a line of defense.

Essentials Cloud Protection is the base-level solution that helps establish a secure cloud environment. This package is ideal for organizations that are transitioning to the cloud or have staffing limitations. It offers network protection that allows secure communication for external internet entities and backup for data storage, duplication, and recovery.

Endpoint Defense extends security coverage to all systems connected to your cloud environment. It includes endpoint devices and agentsupported systems, which are fully monitored and managed by the OneNeck team. It also pairs with OneNeck's Managed Threat Detection and Response (MDR) solution, offering continuous threat research and analytics to detect and prevent intrusions, malware, and other malicious activity, with 24/7 monitoring.

Guardian combines the Essentials solution with Endpoint Defense to create a comprehensive environment. It monitors log, packet, and application data for suspicious activity and leverages internal and external network scans. If an attack occurs, it provides endpoint isolation and system quarantine, with assistance from security professionals to mitigate the attack.

With these bundled solutions, your financial institution gains the benefit of convenience and simplicity, along with cost-effective, comprehensive protection, integration and customization.

4) Monitoring for Threats

More employees than ever are using their own devices for work, in addition to your company devices. All of these devices, or endpoints, are potential vulnerabilities on your network that must be protected.

With more complex methods of attack, and more endpoints on the network to access, hackers have more opportunities to attack banks of all sizes. It's more important than ever to prevent attacks on your network before they happen and to detect attacks that do get through your defenses so you can respond quickly to contain and eliminate the threat.

OneNeck offers proven endpoint protection solutions to help keep your endpoints safe. We leverage global threat intelligence to help block known malware, run complex queries and investigations across all endpoints to detect stealthy malware, and contain attacks no matter what the endpoint operating system.

5) Mitigation if Something Should Happen

It's not a matter of if, but when you'll be breached. And when it happens, every second counts. What you do at that point is critical. Which is why OneNeck offers incident response and actionable mitigation for those critical, post-breach hours.

In the event of an attack, we identify the attack vector and deliver a comprehensive report with the incident timeline, threat intelligence, malware analysis and critical findings. The OneNeck security team works with you to review the report findings, recommendations, and best practices, and prioritize resolving vulnerabilities that contributed to the breach. Our goal is to help promptly resolve breaches and rapidly restore your business operations to normalcy

Chapter 6: OneNeck Cybersecurity Solutions for Banking

As the evolution of the banking industry continues, customers expect the convenience and personalized experiences they get from online and mobile banking. Financial institutions must stay on the leading edge of technology to compete in the marketplace.

At the same time, cyber threats against financial services companies continue to grow. More than ever, banks need help making sure that their technology and data remain secure and protected against cyberthreats and attacks.

With so much to worry about, you need a partner to ensure that your bank is protected. OneNeck is ready to help you secure your data from attacks, inside and outside the perimeter, so you can offer the latest digital banking solutions and the optimal customer experience.

us signal

Digital Infrastructure Solutions Built for Your Business

US Signal, established in 2001, is a premier national digital infrastructure company that operates a fully owned fiber network to deliver a wide range of advanced digital solutions. Our offerings include robust cloud services, secure colocation facilities, high-performance connectivity, comprehensive hardware resale, and managed IT services, empowering businesses to enhance their operational efficiency through tailored network, data center, data protection, and cybersecurity solutions.