Banks Top 8 Cyber Security Challenges and how to overcome them

And

Top 10 FinTech Cyber Challenges

MANK

2022

By Alon Bar,

Banks were attacked on average 700 times every week during the past year, a 53% increase YoY. From Phishing scams and Denial-of-Service attacks to sophisticated attacks by nation-state actors, cyber threats

targeting banks are continually on the rise. In this blog series, we will present real-life stories from banks worldwide, the specific challenges they faced, and the solutions they leveraged to overcome the challenge and bolster their security posture.

The main **banking technology trends that increase cyber vulnerability**

- Growing adoption of new technologies spurred on by **digital transformations**
- **Hybrid data centers** are becoming the norm
- Widespread migrations to the **public cloud** for multiple applications
- Increased use of **online and mobile channels** for banking needs
- The ongoing state of **remote work** due to a pandemic that's not going away
- Accelerating the proliferation of **IoT devices**
- Extensive deployment of **SD-WAN connectivity** for remote branches

As the cyber threat landscape continues to evolve and become more dangerous every year, protecting a bank's IT infrastructure will only continue to become more and more challenging. This first blog will focus on the **Banks' top cyber security challenges**

Securing growing data centers and high-frequency trading platforms

Banks need network security that performs at the speed of business. This is the key to transferring hundreds of terabytes of data securely and in minutes, as well as to providing low latency for high-frequency financial transactions and for scaling security on-demand to support a hyper-growth business such as online commerce.

The main challenges to achieving these goals include assuring:

- **Zero trust**, granular network segmentation to prevent lateral movement
- The **secure transfer** of hundreds of terabytes
- **Low latency** for ongoing high-frequency financial transactions
- **Simplifying** cumbersome management and gaining **visibility** across on-premise and cloud datacenters

Check Point's Network Security solutions simplify the bank's security posture management and streamline and scale operations for continued business growth.

Specifically, the **Quantum Network Security** solution provides ultra-scalable protection against Gen V cyber-attacks on the network, cloud, data center, IoT, and remote users.

Assuring a secure & compliant cloud migration

As banks move data and workloads to the cloud, they need to ensure that cloud assets and data are secured and meet compliance with regulations such as those from the US's Federal Financial Institutions Examination Council (**FFIEC**) and the European Banking Association (**EBA**).

But modern cloud deployments are tremendously complex, typically spanning multiple clouds. So, while public cloud providers do invest extensive efforts into security, the bank still remains the one who is accountable for assuring the organization's cybersecurity.

Achieving this goal entails multiple challenges:

- **Unified security management** across clouds and an on-premise datacenter
- Detecting and remediating **misconfigurations** in real-time
- Streamlining and assuring **governance**
- Meeting stringent **compliance** and privacy regulations

Check Point offers comprehensive security and compliance solutions for financial service organizations' multi-cloud environments. With **CloudGuard Network Security,** they get advanced, multi-layered cloud network security across public and private clouds.

Simplifying compliance and the complexity of security operations

Managing a bank's security operations is a complex undertaking entailing many tasks for keeping up with ever-changing security needs:

- Translating demanding industry regulations into **security frameworks** easily and efficiently
- Defining, accelerating, and enforcing ongoing **policy update installations**

- Assuring operational efficiency amidst numerous time-consuming **manual processes**
- Delivering quick security system upgrades and security gateways updates with no impact on **business continuity**

Check Point enables banks to cut operation management by up to 80% with unified security management across all cloud and network environments, as well as to centrally manage thousands of security gateways.

With the **R81 Unified Cyber Security Platform**, the industry's most advanced threat prevention and security management software, they get uncompromising simplicity and consolidation across the enterprise.

Securing advanced e-Banking services

A bank's applications drive the business. And as they evolve and grow, they expose more APIs causing the attack surface to grow as well.

Cybercriminals are exploiting this phenomenon, attacking web applications and APIs with advanced methods that include SQL injection, cross-site scripting, and deploying automatic scripts known as "bots."

These attacks are damaging and costly, and the ability to secure applications has never been more critical.

But detecting and preventing these attacks is challenging, requiring the bank to implement app-specific security defenses, such as building security into their mobile apps from the get-go.

When they don't, the implications are dire, with great damage that can be incurred to customer security and the bank's reputation.

Banks can protect web apps and APIs from cyber security attacks and build secure mobile apps from the get-go with Check Point's **CloudGuard AppSec**, which automates financial service applications and API protection, and with **Harmony App Protect** for securing e-banking mobile apps.

Watch the Cybersecurity for Banks webinar on-demand.

Enabling the secure remote workforce

With remote users connecting to corporate applications more than ever, the organization's attack surface has never been wider.

To assure advanced protection of its remote workforce, a bank must secure:

- **All devices**, including tablets, mobile, BYOD, and managed devices
- **Users** while browsing the internet and using email and collaboration apps
- **Third parties**, including contractors, consultants, and partners accessing devices and applications

And, they must ensure **zero-trust access** to corporate applications from anywhere.

The Check Point Harmony family of products provides uncompromised protection and simplicity for the financial services sector and includes:

Harmony Endpoint for comprehensive endpoint protection at the highest security level and for avoiding security breaches and data compromise.

Harmony Mobile for complete protection of the mobile workforce, with simple deployment, management, and scale.

Harmony Connect for easily connecting any user to any resource, anywhere, without compromising security.

Harmony Email and Collaboration for complete protection of Office 365, Teams, OneDrive, SharePoint, and Google Drive, using the Avanan technology.

Enabling secure SD-WAN connectivity for branches

Connecting branches directly to the cloud significantly increase the risk of attack via malicious files, malware, zero-day, bots, viruses, APTs, and more.

To mitigate the risk, many banks are seeking to enable their branches with SD-WAN connectivity to the internet and cloud, and to do so gradually for assuring enhanced security.

Check Point solutions assure secure SD-WAN connections to the internet and cloud to protect the bank's remote branch offices from every threat.
With **Quantum Edge** connected banks facilities on-premises are secured with top-rated threat prevention.

Securing bank IoT networks & devices against attacks

From IP cameras and smart elevators to access devices and printers, IoT networked devices are constantly under attack.

Though assuring protection is a great challenge for banks, requiring the ability to:

- **Identify** every IoT device on the network
- **Apply** and manage multiple and complex IoT policies
- **Protect** the network and as well as all IoT assets

Check Point's **IoT Protect** enables banks to secure the IoT network against cyberattacks, from IP cameras to smart elevators, and so much more, delivering capabilities that include:

- **An advanced discovery service** that leverages a built-in discovery engine
- **Seamless policy management** that provides autonomous zero-trust segmentation and automation, with AI and behavioral learning-based analysis
- **Real-time threat prevention** with virtual patching and protection activation against device exploit, with continuous updates from **ThreatCloud**

Augmenting security with support from premier experts

One of the biggest challenges faced by almost every security organization, including the bank's, is the global **shortage in cybersecurity experts**.

It is also very difficult to **stay up-to-date** and maintain **compliance readiness** with continually updated regulations.

And running a **24/7 security** operation can be very demanding – requiring the orchestration of **siloed tools**, keeping the right **headcount**, providing right-time **training** to existing and new staff, controlling **alert fatigue**, and reducing **false positives**.

The key to overcoming the challenge is to augment security design, deployment, operation, and optimization with the support of an industry-leading **cybersecurity team of experts**.

This is where Check Point comes in. Our experts provide support for every phase and need along the cybersecurity journey.

With dozens of cumulative years of Check Point **experience,** the team executes superlative security **design**, seamless **deployments**, and any other **operations** and **optimization**-related needs.

We offer **professional services** with long and short-term engineers who make sure that your organization is always up to date, performing efficiently, and is compliance-ready, whether through manual execution or full automation.

Additional services include:

- **Advanced Technical Account Management** (ATAM)
- **Cyber Resilience Testing** (CRT)
- **Lifecycle Management Services** (LCMS)

- **Incident Response** provided by our Incident Response Team (IRT)
- **Managed Services** with managed detection & response (MDR)
- **Security Consulting Services**
- **Security Training**

Moreover, Check Point provides complete **security operations as-a-service** that includes the Check Point **Managed Detection & Response (MDR) service** for detecting and responding faster to real attacks anywhere in the organization by leveraging our managed SecOps services.

With **Infinity MDR**, the Check Point MDR team monitors, detects, investigates, hunts, responds, and remediates attacks on the environment, covering the entire infrastructure, including the network, endpoint, email, and more.

In conclusion

Check Point enables banks to provide advanced digital services to their customers with the highest level of security to their network, cloud, users, and access, with the Quantum, CloudGuard, Harmony, and Infinity families of products.

By adopting a consolidated security approach with **Check Point Infinity architecture and services**, banks realize preemptive protection against advanced fifth-generation attacks while achieving a **50% increase in operational efficiency** and a **20% reduction in security costs**.

This broad cybersecurity offering of solutions and services from Check Point is enabling 6,500 financial institutions around the world to overcome their toughest challenges today by:

- Protecting the bank's **network** and hybrid **datacenter**
- Assuring a secure and compliant **cloud migration**
- Simplifying **compliance** and the complexity of **security operations**
- Securing advanced **e-Banking** services
- Enabling a secure **remote workforce**
- Enabling secure **SD-WAN connectivity** for branches
- Securing the bank's **IoT network and devices** against attacks
- Augmenting security with the support of cybersecurity **experts**

Top 10 FinTech Cyber Challenges

While startups in this industry can move fast and innovate quickly, as soon as they start to grow they become viable targets for cyber criminals. After all, what's more attractive than financial AND personal data all wrapped in a single package? This is exactly what FinTech companies hold and what makes them so likely to be the target of cyber-attacks.

If you run a FinTech company, cyber security should be your top concern. Yes, even before innovation.

To mitigate risks, you have to get to know them first. These are the top 10 cyber security challenges for FinTech companies in 2021:

- ## 1. Cloud Computing Security Issues

More and more financial services like digital wallets, payment gateways, internet banking services, and others rely on cloud-based platforms. The benefits of cloud computing are undeniable: speed, accessibility, scalability – to name a few.

However, it also has a lot of data flowing through it and this makes the cloud a perfect smoke screen for attackers. This is why it's essential to choose a reliable cloud provider, whose security approach is up-to-date and pro-active.

- ## 2. Malware Attacks

Perhaps the most prominent example here is the series of attacks on SWIFT (the Society for Worldwide Interbank Financial Telecommunication), the protocol that most banks and other financial institutions rely on.

While newer FinTechs are moving away from SWIFT and into blockchain-based payment protocols, the malware attacks are still an important risk. Unlike other types of attacks, malware can use multiple entry points from various sources: emails, pop-ups, malicious websites, third-party software, and so on. These attacks are especially dangerous as their rate of transfer is high and as they can cause whole networks to crash.

Features like automated real-time malware detection and regular VAPT can keep your FinTech safe from malware attacks.

- ## 3. Application Breaches

FinTech companies rely heavily on applications that allow end-users to fill in sensitive data and transfer money with a single screen touch. Applications are also one of the main attack vectors.

Since they are user-facing, gaining access to them is easier than gaining access to the company's network directly. But if an attacker has gotten access to your application, it's only a matter of (short) time until they gain access to your entire network.

Regular vulnerability scanning is essential for any mobile or web application, along with penetration testing.

- ## 4. Money Laundering and Cryptocurrency-Related Risks

Cryptocurrencies have gained a lot of popularity in recent years, but they have also established themselves as a major security challenge for FinTech. Since the origin of the money can be anonymous, cryptocurrency can be used to launder money.

More notably, cryptocurrency transfers can be scams that hackers use as entry points for data theft. Such a security risk can cause both significant financial losses and law enforcement problems.

This is why FinTech companies that deal with cryptocurrencies should only use secure trading platforms. Even more, it's important to stick to mainstream cryptocurrencies that are universally recognized.

- ## 5. Identity Theft

Most financial institutions use biometrics, passwords, or one-time payments to ensure the security of each transaction and to verify the identity of the person who initiates it. However, there is a major drawback of these methods: they can easily be replicated and become an entry point for hackers who can then siphon large amounts of money.

The best way to mitigate this risk is to use more than one verification gateway. Better yet, the verification gateways should be based on different principles and technologies to make penetration more difficult.

- ## 6. Meeting Compliance Requirements

Depending on the types of financial institution you run (Specialized Bank, Electronic Money Institution, Payment Institution), you may have to comply with different standards related to security and data privacy, like GDPR, PSD2, PCI DSS, and so on.

Failing to meet the compliance requirements can result in hefty fines but, more importantly, in major security flaws.

- ## 7. Scalability Issues

"Growth pains" are inherent to startups, especially in the FinTech industry. Why? Because growing means scaling your infrastructure constantly.

Ideally, you should have a highly-scalable infrastructure in place from the very beginning. But, even if that is the case, the fast developing cyber security challenges in this field will require additional changes in your infrastructure. Which brings us to the next point;

- ## 8. Financial Challenges

Securing FinTech infrastructure can get very expensive very fast. Irrespective of how scalable your architecture is, you will need to change or improve your infrastructure constantly.

However, it is important to note that the investment in cyber security measures and tests are a drop in the ocean compared to what you stand to lose if you forego them.

Looking for affordable cybersecurity solutions for FinTech? Talk to our experts and get a personalized offer.

- ## 9. Mobile Platforms and IoT Devices

We now have access to our financials anytime, anywhere through our phones and other mobile devices. The only problem? So do hackers!

The more devices are used to access a certain account, the greater the chances of that account being broken are. IoT and voice assistants add considerably to this risk.

While moving fast is imperative in FinTech, it's also recommendable to add new supported platforms only after heavy security testing.

- ## 10. Convenience or Security?

Customers want fast access to financial products. FinTech companies know that oftentimes they have to choose between convenience and security.

However, the increase in regulatory bodies and compliance requirements in FinTech will force the industry to strike a solid balance between convenience and security before launching a new product.

- ## Final Thoughts

The only industry that develops as fast as FinTech is cybersecurity, although the latter seems to be one step behind attackers. For financial institutions, cyber security is a major concern and a major expense.

Affordable cyber security solutions for companies of all sizes are the only way to be one step ahead of attackers for a change. This is why at Bluedog we have made it our mission to provide SMEs with the

security solutions they need to keep their digital assets safe but without breaking the bank.

MANK

Mohammad Alkhudari – Edited

Green Circle