Check Point
SOFTWARE TECHNOLOGIES LTD

FINANCIAL SERVICES
REELING FROM ONGOING CYBERATTACKS

Introduction

Capital One becomes one of the largest banking thefts ever with the compromise of personal information belonging to 100 million people. Per the U.S. Department of Treasury, Capital One is one of 3,500 successful attacks on financial institutions in 2019.[1] The financial services sector continues to be targeted by cyberattackers, and in many cases, the results have been devastating to the organization, and its customers and employees. Looking ahead at 2020 and beyond, the finance sector can expect no different, as cybercrime is estimated to cost banks $350 billion over the next five years.[2]

A financial institution's PII and PCI data are the crown jewels for cybercriminals, who can monetize the stolen loot on the Dark Web. A Ponemon Institute study now puts the average cost of a data breach industry-wide in 2019 at $3.92 million. A further sobering statistic is U.S. firms are spending an average of $8.19 million in security incident recovery costs.[5]

In this paper, we'll explore financial services' major cyberthreats. The growing needs for cyber security of financial institutions can be seen in its claim to fame as the largest and fastest growing private sector cyber security market.[6] We'll also propose what security leadership can do to help prevent cyberattacks and safeguard sensitive financial data.

Paige Thompson, a former employee of Amazon Web Services and a self-proclaimed hacker, allegedly hacked Amazon's cloud servers to access Capital One databases. She stole 140,000 Social Security numbers and 80,000 bank account numbers, plus investigators say she had data from 30 other organizations.[3] Federal officials seized as much as 30 terabytes of data as evidence.[4]

[1] "Financial Sector Hit with Thousands of Cyberattacks," by Roy Maurer, SHRM, August 6, 2019
[2] "Capital One hacking suspect Paige Thompson appears in court, ordered to remain in custody," by James Thorne, August 23, 2019
[3] "Capital One hacking suspect Paige Thompson appears in court, ordered to remain in custody," by James Thorne, August 23, 2019
[4] "Accused Capital One hacker had as much as 30 terabytes of stolen data, feds say," by Jeff Stone, cyberscoop, October 16, 2019
[5] "Examining the Financial Consequences of a Data Breach," by Steve Turner, September 26, 2019
[6] "U.S. Financial Services: U.S. Financial Services: Cybersecurity Systems & Services Market - 2016-2020" Cyber Security Market Report, Kenneth Research

Financial Sector Threatscape

One 2019 report said 25 percent of all malware attacks are aimed at banks and other financial services organizations – surpassing all other industries.[7] Where the financial motive is known or applicable, financial gain is the most common driver of data breaches, representing 71% of the cases. Espionage is the motive in 25% of breaches.[8]

> "Consumer bank and credit card fraud remains the number one form of cybercrime affecting financial institutions, but the tactics are changing."[9]

One recent study conducted by the Carnegie Endowment for International Peace, a foreign-policy think tank, organized cyber threats involving financial sector organizations into two major categories: 1) High-impact operational risk scenarios and 2) Upstream infrastructure scenarios.[10] The following list identifies how financial institutions' operations can be disrupted by direct infrastructure cyberattacks, or indirectly, by attacks on affiliated partner organizations:

- **Locking malware or ransomware attack on a financial institution:** A large bank can suffer a ransomware attack that renders the majority of the bank's computers unusable, resulting in operational disruption and client service disruption.
- **Large wire transfer fraud:** A financial institution experiences a significant monetary loss from a fraudulent transfer induced by a cyberattack.
- **Data breach and targeted information leak:** A rating agency is compromised with attackers stealing sensitive data about rated companies and other financial institutions, and emails and other internal documents.
- **Placing malware in trading systems:** Malware induces abnormally large trading volumes that affect price discovery.
- **A large-scale cyberattack on a global messaging network for financial transactions:** Persistent, large-scale attack over a month forces the network to discontinue service and shut down.
- **Simultaneous cyberattacks on systemically important institutions:** A number of major attacks on critical core infrastructures occur at the same time with a bank losing millions.

---

7 "Cybercriminals Step Up Malware Attacks Against Financial Firms," by Calvin Hennick, September 12, 2019

8 "2019 Data Breach Investigations Report," Verizon

9 "Forces Shaping the Cyber Threat Landscape for Financial Institutions," by William A. Carter, SWIFT Institute, October 2, 2017

10 "Cyber Risk Scenarios, the Financial System, and System Risk Assessment," by Lincoln Kaffenberger, Emanuel Kopp, Carnegie Endowment for International Peace, September 30, 2019

Upstream infrastructure scenarios include:

- **Disruptions to central clearing:** Coordinated attack disrupts the ability to perform functions, resulting in the inability to clear trades.
- **Attack disrupts payment-processing gateways:** Cyberattack causes intermittent disruptions of a retail payment system over a week, affecting tens of thousands of companies worldwide.
- **Massive malware infection:** Millions of network routers worldwide begin malfunctioning simultaneously due to malware installed surreptitiously at the factory.
- **Cloud provider fails:** A large cloud provider fails suddenly for unforeseen reasons, with companies reliant on the provider no longer able to operate.

"With the Covid-19 coronavirus pandemic striking in early 2020 and organizations moving online, the financial sector has been met with enhanced threats. Experts predict that 2020 will see a rise in the targeting of investment apps, a new target for cybercriminals.[11] Banks will continue to be targets of ransomware attacks. The cyber threats taken together, in combination with an unprecedented global pandemic, make the financial sector even more vulnerable to cyberattacks.

- **Utilities disruption causes knock-on effects:** Persistent, large-scale attack over a month forces the network to discontinue service and shut down.
- **Simultaneous cyberattacks on systemically important institutions:** A number of major attacks on critical core infrastructures occur at the same time with a bank losing millions.

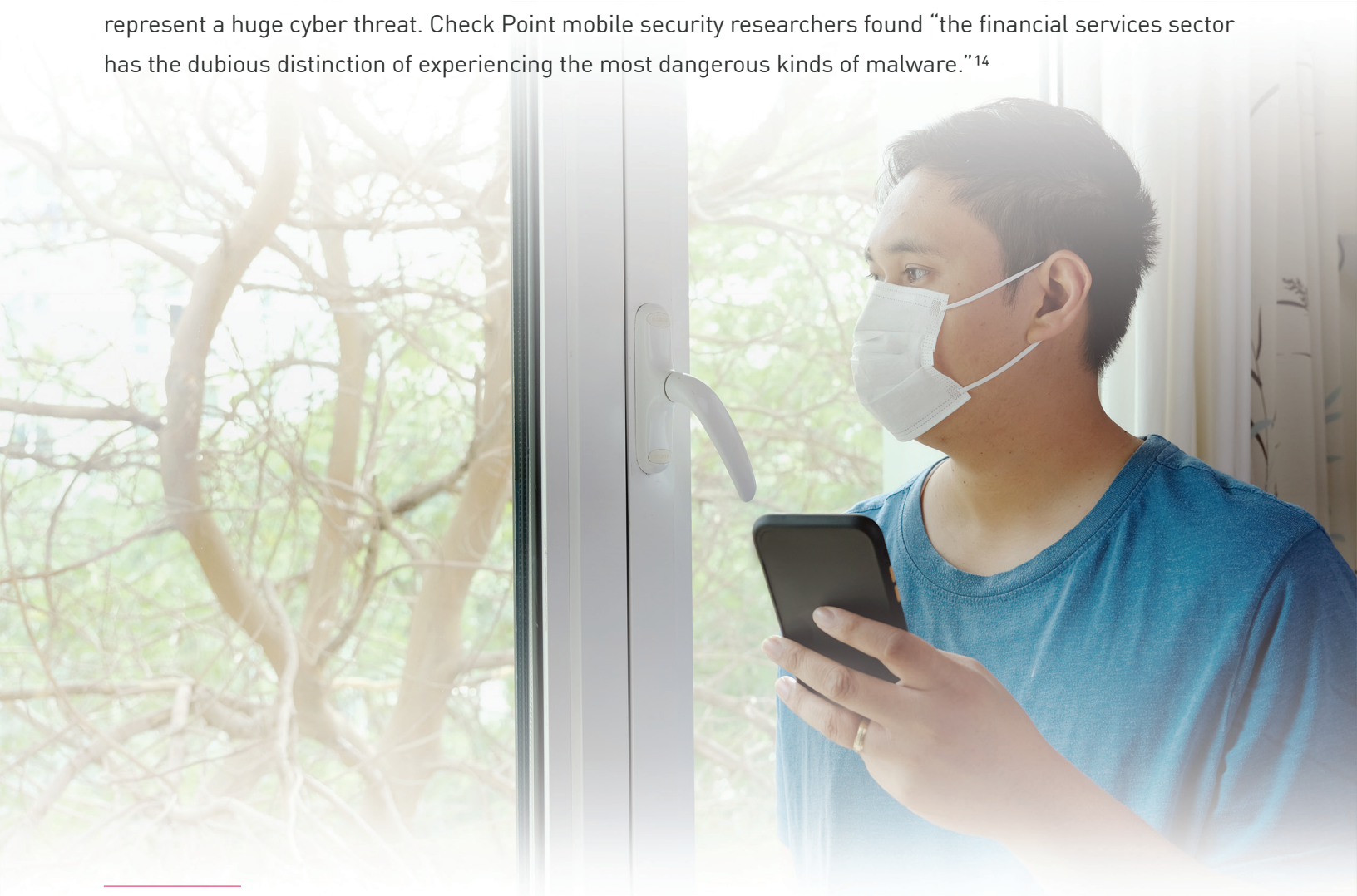
[11] "Cyberthreats to financial institutions 2020: Overview and predictions" by Yury Namestinov, Dmitry Bestuzhev, Kaspersky Security Bulletin December 3rd 2019.

Mobile Banking Applications: Friend and Foe

By 2006, 80% of US banks offered internet-based banking services.[12] Today, it's a mainstream convenience that allows customers, from a computer or mobile apps on cellphones, to transfer funds, deposit checks, and pay bills 24 hours a day. It's anywhere, anytime banking offers numerous advantages, however, there are major downsides, including cyber threats to mobile phones.

Check Point researchers found cyberattacks in the first half of 2019 targeting smartphones and other mobile devices rose by 50% compared with last year.[13] One reason for the increase is the popularity of mobile banking applications. Cybercriminals follow the money trail and design malware to steal payment data, login credentials, and ultimately, funds from victims' bank accounts.

Employees using bring-your-own mobile phones to access financial institution corporate networks also represent a huge cyber threat. Check Point mobile security researchers found "the financial services sector has the dubious distinction of experiencing the most dangerous kinds of malware."[14]



[12] "Rory Brown, Explains How Virtual Banks Went Mainstream," by Marela Bush, Chart Attack, October 4, 2019

[13] "Mobile malware attacks are booming in 2019: These are the most common threats," by Danny Palmer, ZDNet, July 25, 2019

[14] "Mobile Cyberattacks Impact Every Business," Check Point Software, 2017

What Financial Institutions Can Do to Prevent Threats

While financial sector operations are complex and diverse, there are cyber security strategies that you can employ to reduce exposures and increase security effectiveness.

Consolidated Security Architecture

As financial institutions further invest in cloud deployments, SaaS, mobility, and IoT devices, it's a habitual practice to add cyber security point solutions to protect each new component. However, the resulting patchwork of products can leave gaps for opportunistic attackers and present a management nightmare. Adding non-integrated solutions means the security team must monitor numerous user interfaces to find and respond to an overwhelming number of diverse security alerts.

One way of addressing security infrastructure complexity is by deploying a consolidated security architecture that can secure each threat vector and offer data-loss-prevention and forensic-analysis tools. This strategy lets financial firms cover all customer-facing technologies and infrastructure components whether on-site, SaaS, and in cloud environments, along with mobile devices. All vectors can then be monitored and managed through a single interface.

Consolidation has other advantages. When cyber security components talk to each other, they offer more effective protection against 5th generation multi-vector attacks. IT staff can keep tabs on the whole environment simultaneously. Streamlined monitoring raises security effectiveness while it lowers the burden on and the cost of security staffing.

"Within minutes, today's polymorphic malware can change to avoid detection systems and spread throughout your network.

Prevention

Many cyber security products and services mention a window in which to detect in-progress malware attacks. However, within minutes, today's polymorphic malware can change to avoid detection and can then quickly spread throughout your network. Cyber security that relies solely on detection can fail to prevent malware from entering your systems. This is one possible factor to explain the financial sectors high number of data breaches.

Cyber security solutions can now offer proactive attack prevention to stop malware threats before penetrating a network. Prevention is expanding through the use of advanced technologies such as artificial intelligence (AI) and/or machine learning (ML) and behavioral analysis monitored and managed through a single interface.

Conclusion

To meet digital-first initiatives, the IT infrastructure of financial service organizations will grow even more complex than it is today. As they undergo transformations to improve their services, a key challenge is building a secure infrastructure in parallel.

Implementing a consolidated security architecture that offers robust threat prevention across all threat vectors is worth strong consideration. It can help reduce the complexity with cyber security operations and increase security effectiveness. Proactive prevention, rather than just detection, is another best practice for financial institutions to defend against sophisticated cyber threats.

Cases in Point

"As a financial trading services SaaS solution, CloudGuard Dome9 is an essential part of our AWS infrastructure security. The CloudGuard Dome9 platform helps us minimize attack surface, manage dynamic access and comply with ongoing compliance requirements." – Avi Zloof, Director of Innovation and Product, Tradair

To learn more how this financial services firm minimized security risks and eliminated exposure of its cloud-based trading platform, click this link.

"SandBlast Mobile proved itself. It's an effective, affordable solution that protects us in ways that our container solution alone could not accomplish." – Stacy Dunn, Information Security Analyst, RCB Bank

Learn how this community bank identified, blocked, and receive notifications of cyber threats and noncompliant devices by visiting this site.

To learn how a single, consolidated architecture with granular visibility, automated tools, and prevention capabilities protections can help your organization, visit the Infinity web page, or contact your Check Point representative.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com