2020

FUTURE CYBER THREATS

The latest extreme but plausible threat scenarios in financial services
CONTENTS

FOREWORD

KEY THREATS

01 / Supply chains introduce increasingly interconnected attack surfaces

02 / Credential and identity theft continue to accelerate

03 / Data theft and data manipulation stems from new vulnerabilities and cybercriminal behaviors

04 / Emerging technologies, especially deepfakes and 5G, advance cyberthreats

05 / Destructive and disruptive malware attacks spur multiparty and cross-sector targeting

06 / Misinformation shakes trust in retail and government-backed banks

PROACTIVE, COLLECTIVE DEFENSE
What a difference a year makes. Although many of the threat scenarios we reviewed in last year’s report still apply, security teams in the financial services sector are experiencing even more exacting demands as they defend their organizations in a world under a new and unexpected threat—a global pandemic.

Malicious threat actors are taking advantage as organizations reconfigure vulnerable supply chains and offer more digital experiences. Working from home has opened a pandora’s box of new attack vectors and workforce challenges—including those from insider threats. And there are challenges around rethinking culture and collaborative practices as organizations seek to outmaneuver uncertainty in the future.

The 2020 Accenture cyber threat intelligence research revisits the trouble spots for security leaders. We see that credential and identity theft continue to accelerate while new vulnerabilities and cybercriminal behavior increase data theft and data manipulation. We look at emerging technologies, especially deepfakes and 5G, and how these are advancing cyberthreats. We see how destructive and disruptive malware attacks are spurring multiparty and cross-sector targeting and report on how misinformation is affecting trust in retail and state-owned banks. One new area that has joined our list of key threats this year is the topic of vulnerable supply chains and new interdependent attack surfaces that adversaries can undermine.

We hope this latest view of the market will inform the necessary steps to adapt your security strategy and the collective activities of the financial sector.

Valerie Abend
Managing Director, Accenture Security

Howard Marshall
Managing Director, Accenture Security
KEY THREATS

Through this report, based on research by the Accenture iDefense threat intelligence team, we revisit the central themes outlined in the Future Cyber Threats: Extreme but Plausible Threat Scenarios in Financial Services report published in 2019.

In addition, as the threat landscape evolves, we identified a sixth trend that is gaining significance: vulnerable supply chains that introduce increasingly interconnected attack surfaces.

This report evaluates the current state of each of the six threat trends and offers insights into how the threats are likely to influence financial institutions going forward.

The six threats are:

01/ Supply chains introduce increasingly interconnected attack surfaces.

02/ Credential and identity theft continue to accelerate.

03/ Data theft and data manipulation stems from new vulnerabilities and cybercriminal behaviors.

04/ Emerging technologies, especially deepfakes and 5G, advance cyberthreats.

05/ Destructive and disruptive malware attacks spur multiparty and cross-sector targeting.

06/ Misinformation shakes trust in retail and government-backed banks.
Supply chains introduce increasingly interconnected attack surfaces

Financial institutions have complex, interdependent supply chains. These offer a broad, target-rich attack surface that adversaries can undermine. Attackers have been conducting supply chain attacks for years.¹ However, supply chain threats to financial institutions in the past year have primarily involved technology service providers (TSPs), including managed service providers (MSPs) and cloud service providers (CSPs). Core financial TSPs and IT service providers have been affected by ransomware incidents, disrupting services for some of their financial institution clients.²³

For years, actors exploiting SS7 successfully drained retail banking clients’ accounts. While some mobile carriers have employed compensating security measures to deter SS7 attacks, others have yet to do so. This lack of standardization in the approach to counter this threat exposes financial institutions and their clients to risk when SMS 2FA is used. The nexus between the telecommunications and financial sectors could continue to be a chokepoint for cybersecurity, as actors exploit vulnerabilities or even focus on disrupting communication systems at scale.

Another dependency for the financial sector is global navigation satellite systems (GNSS), which provide crucial data for financial transactions. Stock exchanges rely upon GNSS data to uniformly timestamp financial transactions, including automated transactions. Actors can spoof this data or jam the systems, so that transactions cannot be properly timestamped. What is more, if actors undermined GNSS systems and knocked them offline, it is possible that “exchanges could not reconcile trades and automated teller machines and its related key, which are used to identify and authenticate subscribers on mobile telephony devices such as mobile phones and computers.

² Cyberattack on IT services giant [REDACTED] impacts clients, April, 2020, https://www.techrepublic.com/article/cyberattack-on-it-services-giant-[REDACTED]-impacts-clients/
⁴ Subscriber Identity Module cards securely store the international mobile subscriber identity (IMSI) number
⁵ Signaling system number 7 is a set of telephony signaling protocols developed in 1975, which is used to set up and tear down telephone calls in most parts of the world-wide public switched telephone network (PSTN).
(ATMs) would no longer work because the banks would be unable to verify the money is there.\textsuperscript{7} GNSS’s are controlled by a handful of nations across the globe and have attracted nation state interference\textsuperscript{8,9} including by countries that have been suspected culprits of state-sponsored cyberattacks against the financial sector in the past.

Other supply chain threat scenarios which pose significant risk to the financial sector include power grid outages. Actors have made strides in targeting each of these areas through malicious cyber activity in the past few years—in some cases leading to warnings from governments around such attacks. “An electricity disruption, such as a blackout, can have a domino effect—a series of failures that can affect banking, communications, traffic, and security.”\textsuperscript{10} Such blackouts have famously occurred in Ukraine\textsuperscript{11} and have been linked to a malware which other actors later repurposed for destructive, financially-motivated attacks against banks in Latin America.\textsuperscript{12,13}

The COVID-19 pandemic has rapidly increased the role the nesting aspects of cloud will play in supply chain threats to critical infrastructure, including financial services. Cyber threat actors are taking advantage as businesses shift the information security focus from an enterprise infrastructure to a virtual and cloud environment to support remote workforces.\textsuperscript{14} Looking ahead, adversaries will exploit vulnerabilities across each of the core service categories of cloud—SaaS (Software as-a-Service), PaaS (Platform as-a-Service) and IaaS (Infrastructure as-a-Service) (Figure 1). These layers often sit on top of one another, chaining together potentially vulnerable environments supporting critical business functions. Protections need to exist both within each layer and holistically to thwart exploitation.

One of the biggest challenges to securing cloud has been misconfigurations. For example, a failure to deploy multifactor authentication (MFA) for all cloud services and disable legacy services threat actors can manipulate to bypass controls contributed to the majority of cloud intrusions that the Accenture Cyber Investigation and Forensics Response (CIFR) team responded to in 2019.\textsuperscript{15} It is likely this trend will continue; unprecedented usage of PaaS, SaaS and IaaS solutions due to the COVID-19 pandemic foreshadow large cloud breach disclosures in the future.

\textsuperscript{7} The entire global financial system depends on GPS, and it’s shockingly vulnerable to attack, October, 2017,https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/
\textsuperscript{8} [REDACTED] are screwing with the GPS system to send bogus navigation data to thousands of ships, April, 2019, https://www.businessinsider.com/gnss-hacking-spoofing-jamming-[REDACTED]-screwing-with-gps-2019-4
\textsuperscript{10} Smartgrid.gov, https://www.smartgrid.gov/the_smart_grid/smart_grid.html
\textsuperscript{11} Technical Analysis and Perspective of Recent Attack that Caused Ukraine Power Outage, January 6, 2020, iDefense Threat Intelligence
The wide spectrum of supply chain attack vectors makes it a significant blind spot for financial institutions of all sizes. Cross-sector intelligence sharing and collective response is central to effectively mitigating supply and third-party cyber risks. A cyberattack against a handful of critical financial institutions could prove catastrophic for the sector as a whole. The United States Federal Reserve Bank (FRB) of New York further unpacked this plausible scenario in its January 2020 pre-mortem assessment of attacks against United States wholesale payments. The FRB estimated that “the impairment of any of the five most active United States banks will result in significant spillovers to other banks” potentially reaching 2.5 times daily gross domestic product (GDP), more than US$130 billion, in forgone payment activity.\(^{16}\)

The interdependencies across financial services exposes institutions to significant risk should adversaries concentrate their campaigns on disrupting a systemically important financial institution (SIFI), or worse multiple. The interdependency risks for financial institutions within the sector are as significant as the risks posed by supply chain dependencies with organizations outside of the sector. This was illustrated when a “foreign currency exchange that does business in 26 countries paid a ransomware gang US$2.3 million to regain access to its data following an attack on New Year's Eve.”\(^{17}\) The incident caused foreign exchange outages and disrupted the international payments facility of Samsung Pay.\(^{18}\)

---


Credential and identity theft continue to accelerate

Credential and identity theft, compromise and abuse continue to be cornerstones for targeted attacks and fraud. As novel coronavirus, COVID-19 spread across the globe, financial institutions moved rapidly to adjust their operations. Cybercriminals also moved swiftly to take advantage of the expanded attack surface presented through largely remote workforces and rich feeding ground for fraud from the extensive government funding programs extended through financial institutions to small businesses in greatest need. Credential-stealing malwares surged, including mobile malwares such as EventBot and Cerberus which are collectively capable of stealing customer credentials for more than 200 financial institutions. The premier seller of Cerberus noted their sales increased exponentially in early April 2020, netting them more profit in a single week than the prior four months combined.

As most financial institutions’ employees moved to remote workforces, there was a surge in reliance on mobile devices. There are claims that actors were able to install Cerberus nearly one million times. This activity foreshadows an increase in fraud and intrusions that will be a drain on security and fraud teams as financial institutions continue to orientate themselves to new working conditions and technologies.

The increase in credential theft campaigns and related cybercrime during the COVID-19 pandemic comes hard on the heels of sustained threat activity in recent years. In early July 2019, cyber threat actors launched a highly targeted credential theft attack against at least 100 organizations around the world. Security researchers believe the actors’ goal was to deploy the well-known malware Lokibot to exfiltrate sensitive data, including credentials. A financial sector-wide alert was issued in late 2019 noting a spear phishing attempt made on a Middle Eastern bank using a Lokibot variant.

Identity theft also continued to grow over the last year, especially as governments and financial institutions implemented financial relief programs to assist individuals and businesses affected by COVID-19. Cybercriminals created COVID-19 channels on major criminal forums and marketplaces, peddling information to support identity theft activities as part of cybercriminals fraud activities. This shift came as chatter around tax season-related identity theft reduced somewhat in the light of opportunities to use similar stolen and fabricated data for stimulus fraud. This pivot highlights the versatility and

---

10 EventBot Malware Family, April, 2020, iDefense Threat Intelligence.
19 EventBot Malware Family, April, 2020, iDefense Threat Intelligence.
20 Significant Increase in Sale of Cerberus Android Banking Malware, April, 2020, iDefense Threat Intelligence.
flexibility actors have to use resources related to identity theft through different mechanisms. Even as organizations work to thwart identity theft and account takeovers, actors’ commonization of superior tools keeps them a step ahead.

A prime example is a thriving digital fingerprint marketplace on a well-known criminal forum. On the forum, actors are able to buy, sell and exchange compromised data including login credentials for sites visited, cookies, IP addresses, user agent, location, OS, operating times, keyboard layout and more. By using these digital fingerprints, threat actors can then bypass anti-fraud measures. For example, digital fingerprints for specific organizations’ infrastructures appeared in criminal forums and months later these organizations experienced Maze ransomware infections and data exfiltration attacks. The availability and multidimensionality of digital fingerprints and other compromised data could enable actors to continually defraud banks’ customers. Organizations should remain vigilant in their anti-phishing and security awareness education programs to reduce the likelihood of adversary success around capturing credentials, customer data and sensitive, nonpublic information.

\[\text{22 IT Services Firm Suffers Maze Ransomware Attack, April, 2020, iDefense Threat Intelligence}\]
Data theft and data manipulation stems from new vulnerabilities and cybercriminal behaviors

While threat actors continue to target data, their motivations often go beyond theft to include destruction and disruption. A new wave of cyberattacks sees data no longer simply being copied, but being destroyed—or changed—breeding distrust. In late 2019, security researchers disclosed a Microsoft Azure vulnerability referred to as BlackDirect. If not remediated, threat actors could exploit this vulnerability to steal sensitive data, compromise production servers, manipulate data, or even encrypt all of a victim organization’s data (ransomware). This vulnerability disclosure came as financial institutions and regulators were scrutinizing cloud security vulnerabilities and related cyber threats following the large scale data theft from a major United States financial institution.

In last year’s Future Cyber Threats: Extreme but Plausible Threat Scenarios in Financial Services, we discussed “the anatomy of the cover-up,” how actors use pseudo-ransomware to distract organizations during their attacks. While this activity remains a threat, actors have expanded their arsenal, combining data theft and data extortion during ransomware attacks. Threat actors realize that multi-pronged approaches against businesses help to sustain ransomware as a lucrative long-term approach. The concept of “naming and shaming” ransomware victims, coupled with threatening to release stolen data makes the process of responding to ransomware infections more challenging.

Recently, a ransomware group claimed they successfully exfiltrated millions of credit card records from a state-owned bank in Central America. This comes at a time when cybercriminal groups are cooperating with one another, quickly shifting from commodity malware infections to targeted attacks. In some instances, it has only taken hours for crimeware to cause devastating ransomware to enter the network. Looking ahead, this “collective offense” of cybercriminals will prove a formidable threat to businesses across all industry sectors.

---

25 Ibid.
26 A hacker gained access to 100 million credit card applications and accounts, July, 2019.
27 Extortion Entrepreneurs: How Cybercriminals are Bullying Businesses, April, 2020, iDefense Threat Intelligence
Emerging technologies, especially deepfakes and 5G, advance cyberthreats

Deepfakes

As technology rapidly advances, cyber-defenders and adversaries alike are exploring means of using cutting-edge tools. In particular, malicious actors recently used deepfake to increase the effectiveness of their campaigns. In March 2019, criminals used artificial intelligence (AI)-based deepfake recording software to impersonate a chief executive’s voice, leading to the fraudulent transfer of approximately US$245,000. This incident set a dangerous precedent for voice-spoofing attacks aimed at exploiting human vulnerabilities. As financial institutions continue to combat business e-mail compromise (BEC) and account takeover (ATO) attacks, they will need to track the emerging tactics, techniques and procedures (TTPs) adversaries may use to stay a step ahead. Organizations should also explore technological countermeasures in development to prevent adversarial abuse of this emerging technology.

5G

As the world adopts fifth generation mobile networks, threat actors will seek to gain new advantages with 5G technology. The opportunities for 5G in financial services abound, “5G will become a general-purpose technology for financial services organizations, providing new opportunities to create, store, and protect value, to move money, and to access credit.” However, it also presents risks, including those raised by governments including supply chain threats, software vulnerabilities, organized cybercrime, espionage as well as cross-sector threats.

Dependence upon a select handful of suppliers for 5G technology mirrors similar cyber threat scenarios raised at the advent of other technologies, such as cloud. Concentration of targets across a relatively undiversified pool of technology providers amplifies the impact a single malicious campaign can have globally. This also increases the return on investment (ROI) for adversaries—as witnessed during previous campaigns such as CloudHopper. Governments and think tanks have also voiced concern around the potential for nation-states to willfully exploit technological vulnerabilities present in software and hardware manufactured by companies within the reach of their influence.

FinTechs

Financial technology (FinTech) disruptors have rapidly expanded to new markets, increasing the level of dependence the broader financial sector has on these companies to deliver their core products.
and services. In the future, it is these areas on the periphery of financial institutions and markets, like FinTech, where large-scale, disruptive attacks may originate.

Consumer and financial institutions’ adoption of emerging and, in some cases, immature FinTech capabilities, has led to more opportunity for cyber threat actors. Adversaries have set their sights on FinTech during financially-motivated attacks. For example, in March 2020 a ransomware infection caused one of the world’s leading banking FinTechs to shut down key systems as part of its recovery measures. This incident came after another large ransomware infection led to outages of online foreign currency services in more than 30 countries. It is likely that FinTechs, especially those that are also critical points of failure, will be attractive targets for financially and politically motivated threat campaigns as long as vulnerabilities in software, platforms and infrastructure configurations afford them access to networks and valuable data.

Part of the challenge around FinTechs is that they are not regulated in the same way as traditional financial institutions. An Accenture survey found that 38% of FinTechs in New York reported that they were not addressing regulatory issues at all. This can pose challenges to overall security and resilience as FinTechs may not always be required to have sufficient security in their own processes and products to maintain as robust resiliency as everyone else down the line. Similar to other technology service providers, which adversaries view as a launchpad to other targets’ data or systems, FinTech companies could be an indirect entry point for threat actors’ intrusions of financial institutions.


Disruptive and destructive malware attacks spur multiparty and cross-sector targeting

Threat groups leveraging ransomware are targeting multiple related parties at once globally. On August 16, 2019, more than 20 entities in Texas, United States, reported ransomware attacks, prompting a coordinated state and federal response to a multi-jurisdictional cybersecurity event that was the first of its kind.\(^37\) Testing the resilience of the affected entities, this multiparty attack is a bellwether indicating the likelihood of additional concurrent, disruptive attacks. A proactive cyber-defense plan that incorporates multiparty attack simulations with industry and cross-industry peers could help financial institutions be better prepared to face this threat.

The disruptive and destructive impact upon financial institutions is a noteworthy recent change in ransomware attacks. Two UK-based organizations, integral to global financial organizations, were affected by ransomware in December 2019 and March 2020 respectively. The companies, one a foreign exchange (forex) market leader and the other a financial services TSP, had to take systems offline following the cyberattacks which left services disrupted for their global banking clients. As third parties fall victim to targeted malware campaigns, actors are likely to have a growing negative impact on the availability of some banking and insurance services on a global scale.

Financial services organizations are not always first in line to suffer from disruptive and destructive malware campaigns—but as referenced in Section 01 (page 5), they can be affected indirectly through the supply chain. For example, an investment fund that owned two chemical companies was impacted when these companies incurred LockerGoga ransomware infections in 2019.\(^38\) Since LockerGoga had already crippled a Norwegian aluminum company and led to at least US$40 million in immediate losses,\(^39\) the attack on the chemical companies had the potential to not only undermine their performance, but also have a knock-on effect on the performance of the investment fund. Financial services organizations can address this risk by following high exposure sectors in their portfolio and by participating in forums that facilitate cross-sector information sharing.

---


Misinformation shakes trust in retail and government-backed banks

Disinformation and misinformation is not only a threat to efforts to manage COVID-19, it also impacts the financial sector. Multiple United States entities, including the NASDAQ, Securities Exchange Commission and FINRA have warned of spikes in market manipulation in the wake of the COVID-19 pandemic. Often, market manipulation involves elements of disinformation or misinformation directed at influencing unsuspecting investors to aid criminal actors’ objectives. Some groups undertaking these activities, as well as pumping and dumping (a form of securities fraud that involves artificially inflating the price of a stock through false positive statements), have been connected to cyber intrusions in the past. Bad actors can take advantage of high market volatility which could further reduce confidence in the economy.

Disinformation has affected the financial sector multiple times in the last year. A United Kingdom bank had to reassure customers of its financial health after its share price dropped 11% due to false rumors the bank was collapsing and encouraging customers to empty their accounts. Public sector banks (PSBs) in East Asia fell victim to a similar event via social media in September 2019. Following an announcement from the central bank that many of the India’s PSBs would be consolidated, unknown individuals amplified a false narrative that nine PSBs would be closed permanently. Word also spread that the central bank was urging the public to withdraw money from the supposedly folding banks. In both instances, the banks were able to quickly correct the record but these incidents highlight how susceptible financial markets are to manipulation as a result of disinformation.

There is no evidence that sophisticated actors are spreading misinformation to support a financial or political agenda—but it is plausible. As a result, the financial sector should consider how to combat both accidental misinformation and highly sophisticated disinformation campaigns that may arise in the future.
PROACTIVE, COLLECTIVE DEFENSE

In the face of evolving threats and adversaries in difficult times, security leaders have an opportunity to reimagine their strategy and technologies from the ground up. Security leaders are in pole position to act as decision makers and key influencers to help their institutions to be safe and secure and guide people to adapt to new ways of working that improve security in the long term. By adopting the attributes of adaptive security, security leaders can put the right controls in place to create a working environment that builds resilience.

Actions security leaders can take include:

**Adopt a secure mindset**

- Instill a “security first” ethos, using up-to-date company information protection procedures, while making sure that computers and devices include the most current system and application versions.

- Evaluate and promote solutions that mean distributed teams can connect and collaborate safely, securely and effectively—helping your organization to create better employee experiences while making them more productive.

**Secure the new perimeter**

- Rapidly address your security protocols and solutions to enable the expansion of remote connectivity.

- Deploy a zero trust network access approach with built-in technologies to enable secure application access without relying on traditional VPN solutions.

- Automate with endpoint management detection and response to reduce the amount of human intervention needed.

**Become agile and adaptive**

- Bring your existing focus on business risk and resilience into the broader executive planning discussions.

- Consider managed services and automate to increase the scalability and flexibility of your cyber defenses.

- Use cloud-based solutions to meet the increased demand for a fast, frictionless and secure remote access to enterprise data and applications.

- Conduct simulations to stress-test existing processes as well as penetration testing and red teaming to proactively identify gaps or areas for improvement.

- Track the emerging tactics, techniques and procedures (TTPs) adversaries use to stay a step ahead.
Focus on Nth party risks

- Advise cyber threat intelligence teams to monitor and report upstream on cyberthreats to critical suppliers and partners.
- Expand risk frameworks and automate response protocols to include cyberattacks against nth parties.
- Mobilize a rapid-response center to identify and prioritize third party and supply chain risks or blind spots.

Collectively respond and act

- Collaborate with others with the common goal of securing the enterprise and the broader ecosystem to help smaller partners beat cyberthreats with better protection for the front and back doors.
- Deepen and widen your relationships with other financial institutions, information-sharing communities and law enforcement.
- Participate in sector-wide or joint cyber exercises with peer financial institutions to more frequently gauge the effectiveness of current cyber defense resources, processes and technologies.
CONTACT US

Valerie Abend  
Managing Director, Accenture Security  
valerie.abend@accenture.com

Howard Marshall  
Managing Director, Accenture Security  
howard.marshall@accenture.com

LEGAL NOTICE & DISCLAIMER

© 2020 Accenture. All rights reserved. Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is prohibited without express written permission from iDefense.

Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. As such, Accenture provides the information and content on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report. The reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world’s largest network of Advanced Technology and Intelligent Operations centers. With 506,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at www.accenture.com

ABOUT ACCENTURE SECURITY

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security