Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **March 2022**
Sponsored by **BIO-key International**

Cybersecurity in Financial Services: Viewpoint 2022

Executive Summary

The financial services industry is under cyberattack with threat vectors including data breaches, advanced attacks that bypass security protections, and misconfigured cloud services. Regulators across the world demand a higher standard of performance from financial firms, as do customers who require safe access to their funds in an increasingly mobile and app-driven world. The industry will remain a key target for threat actors due to money and identities being on offer, along with opportunities for financial sabotage to cripple a country. Financial services organizations must revisit the efficacy of current cybersecurity protections, invest in new solutions to address emerging threats, and build a strong security posture by following best practices.

The term "financial services organization" covers a wide range of organizations including banks (central, retail, commercial, and internet), credit unions, investment banks, insurance companies, and brokerage firms.

The financial services industry will remain a key target for threat actors due to money and identities being on offer, along with opportunities for financial sabotage to cripple a country.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Financial services organizations are under attack from many sides**
  New entrant banks with new business models, the move away from in-person banking, a complex ecosystem rife with legacy technology, and the rise of cryptocurrencies creates a challenging context for financial services firms.
- **Traditional cyberattacks are complemented by emerging ones**
  Data breaches, impersonation attacks, and insider misdeeds remain rife in the sector. Emerging threats are being seen against cloud infrastructure, SaaS, cross-app access tokens, and application programming interfaces.
- **Highly demanding regulatory environment**
  Government and industry bodies have imposed significant cybersecurity preparedness and reporting regulations on the sector, in addition to broader data protection mandates. Regulators are also pushing operational resilience.
- **Threat actors find the sector alluring, and that is not expected to change**
  While there is money to be gained by illicit means, threat actors will keep trying. Smaller gangs are after the money, but nation-state threat actors are more interested in causing financial sabotage to destabilize a foreign enemy.
- **Solutions are needed to protect and defend the sector—and its customers**
  Cloud services must be better protected, identity and authentication strengthened, and overprivileged access systematically reduced. Bots must be stopped, email hardened, and employees better trained to detect threats.
- **Complement solutions with cybersecurity best practices**
  Start with an updated, context-rich cyber risk assessment for your organization, along with improved risk management frameworks internally and externally. Go beyond training and build human resilience to cope with cyberattacks.

ABOUT THIS WHITE PAPER

This white paper was sponsored by BIO-key International. Information about BIO-key International is provided at the end of this paper.

Financial Services: A Challenging Context

Traditional financial services firms are under tremendous pressure from many directions. It is an industry under attack, and not just cyberattack. Factors that make financial services a challenging sector include:

- **New entrant banks with new business models**
  Fintech startups or neobanks offer digital-first or digital-only banking services.[1] Customer interaction is through a website or mobile app, not a physical branch. Fees are low, the technology platforms are new, and the product line tightly focused. Their cost structure is very different from traditional firms with decades of legacy technology, a broad portfolio of banking and investment services, and an expensive bricks-and-mortar branch network to staff and maintain.
- **The move away from in-person banking**
  The value of the traditional face-to-face relationship between a banker and a client is eroding rapidly as customers shift toward mobile and online interaction. Having a branch network is looking more like a net negative when customers have physical access to their banking services through a mobile device wherever they are, and particularly so in the context of the health pandemic which has seen customers unable or unwilling to visit a branch office. There is increasing preference among customers for personalized mobile and online experiences, and when a traditional financial services institution is too slow to deliver, customers look at newer and more dynamic alternatives.
- **A complex ecosystem rife with legacy technology**
  The global financial system relies on a complex ecosystem of financial clearinghouses owned by a range of players, each with their own interdependencies and access requirements. Technology standards, systems, and exchange protocols were developed decades ago, and while modernization activities are underway, legacy infrastructure remains embedded.
- **The rise of cryptocurrency**
  Cryptocurrency platforms offer a decentralized means of storing and exchanging value, and when valuations are increasing for this volatile currency, crypto delivers financial returns that far outstrip what is available in a traditional savings account. For example, the theft of 120,000 bitcoins in 2016 at a value of $66 million was worth over $4.5 billion when the Department of Justice seized the stolen wallets in February 2022.[2] No savings account will deliver that kind of return, and both customers and cybercriminals are flocking to the higher-risk markets in pursuit of outsized (or illicit) gains.[3]

Having a branch network is looking more like a net negative when customers have physical access to their banking services through a mobile device in their hand.

In combination, these factors create a perfect storm for cybersecurity. CIOs, IT directors, and CISOs face competing and urgent demands from multiple sides. New technology is urgently demanded from the business to address elevated customer expectations and deliver new products and services to market. Growing demands from government and industry regulators leave little space for offerings that do not meet the highest security standards from day one. Cyber insurance providers are pulling back on cyber coverage, changing the risk calculus dramatically. Daily cyberattacks and the immediate business, economic, and cyberthreats of the Russian war on Ukraine complicate matters further. Prioritizing cybersecurity during such a maelstrom relies on decision-makers with informed perspectives, clear judgment, and the will to drive systemic change.

Financial Services Organizations are Under Cyberattack

Cyberattacks come in many shapes and sizes. In this section, we look at the variety of cyberattacks, cyber fraud, and security incidents of concern to financial services organizations.

CYBER FRAUD

Digital fraud attacks such as identity theft and phishing against financial services organizations increased 109% during early 2021, more than four times the cross-industry average.[4] Not surprisingly, cyber fraud is the highest-rated concern among banks about the global economy, with banks rating post-pandemic supply chain issues and interest rate risk as lesser concerns.[5]

DATA BREACHES

Threat actors attempt to steal or compromise data held by financial services organizations. In 2021, the industry had one of the highest rates of data breach incidents (third highest in the United Kingdom, with healthcare in first place and education and childcare in second),[6] with successful incidents due to multiple types of attacks. For example:

- **Hacking of a cloud service, e.g., Capital One**
  Capital One stored credit card application data in an Amazon Web Services (AWS) account. An aggrieved ex-AWS employee wrote code to identify AWS accounts with configuration weaknesses and was able to breach data on 100 million individuals who had applied for a credit card from Capital One over a 15-year period. Capital One was fined $80 million by the Office of the Comptroller of the Currency for failing to establish and maintain effective risk management processes before moving to the cloud.[7] Capital One also agreed to a $190 million settlement in a class-action suit covering the breach.[8]
- **Exploitation of an unpatched vulnerability, e.g., Punjab National Bank**
  Data leakage is the most common consequence of unresolved vulnerabilities in applications.[9] An IT security consulting firm in India alleged that a major local bank exposed the personal and financial details of its 180 million customers by failing to resolve a known vulnerability in Exchange Server. The bank confirmed the unpatched vulnerability but largely denied any unauthorized access.[10] In the wider scheme of things, one study found that 43% of applications in the finance and insurance sector were perpetually exposed during 2021 due to at least one serious exploitable vulnerability.[11]
- **Weaknesses in third-party processes, e.g., Ascension Data & Analytics**
  Ascension Data & Analytics, a data analytics company serving the mortgage industry, contracted with a third-party firm to provide text recognition services. The third-party firm stored Ascension's documents in a cloud service with no access controls, providing open access to 24 million records for one year. Logs showed the data was accessed more than 50 times from computers apparently located in Russia and China. Ascension performed no due diligence on the third-party firm's security practices before sharing personal and financial data with them.[12] The Federal Trade Commission (FTC) demanded that Ascension bolster its security protections, including those extending to third-parties. One Commissioner protested strongly that a harsher penalty should be levied.[13]

Cyber fraud is the highest-rated concern among banks about the global economy —higher than supply chain issues and interest rate risk.

- **Weaknesses in internal security controls, e.g., First American Financial**
  A bug introduced in 2014 during a routine application update exposed personal and financial data in 885 million documents at First American Financial to unauthorized access by anyone with a web browser.[14] In mid-2019, a third-party analysis concluded that data on only 32 individuals had been breached, yet another analysis in 2020 said 350,000 documents had been accessed without authorization. The SEC fined First American $488,000 for failing to maintain cybersecurity disclosure controls and procedures (under the Securities Exchange Act of 1934 Rule 13a-15(a)),[15] and the New York Department of Financial Services alleged multiple charges under the New York Cybersecurity Regulation (23 NYCRR 500), which provides for a much higher level of compliance penalty.[16] Although the vulnerability had already been discovered through internal testing, it had been misclassified as low risk and left unaddressed.

- **Theft of authentication tokens granted to third-party firms, e.g., Dave**
  Dave, a provider of a banking app in the United States, had data on more than seven million customers stolen after hackers breached their systems after first breaching the systems at a technology provider with which Dave had previously worked.[17] The breach used an old but still valid OAuth authentication token that had been created for Dave.[18]

- **Abuse of overprivileged accounts, e.g., Desjardins**
  Just as abuse by bank employees of dormant financial accounts is a costly form of financial fraud,[19] so is abuse of inactive user accounts (e.g., when the account for a departed employee has not been deactivated) or unmonitored user accounts (e.g., when the actions taken by a current employee are not monitored for excess access rights, unexplained behavior, or malicious action). A high-performing but disgruntled employee at Desjardins, a bank in Canada, accessed personal data on 9.7 million customers over a two-year timeframe.[20] While the employee did not have the access rights to the data warehouses containing the data, he could access the shared drive where copies of the data were stored. The employee used scripts to create additional copies of the confidential data on his work computer and USB keys.[21] Although trust was an important value at Desjardins, the Office of the Privacy Commissioner of Canada stated the bank needed better tools and greater vigilance to protect against such internal threats. The lack of monitoring which allowed the abuse of the overprivileged account cost Desjardins over $200 million to resolve.[22]

Weak internal controls and lack of protections against malicious employees results in costly data breaches.

THREAT ACTORS MASQUERADING AS FINANCIAL SERVICES ORGANIZATIONS

Financial services organizations are intricately intertwined with daily economic rhythms, and threat actors seek to leverage the connection between consumers and their bank for malicious ends. Phishing attacks against consumers are a common approach by threat actors who masquerade as a financial services organization. Thousands of people fall for phishing scams supposedly sent from their bank every day.[23] Data on the threat of phishing in the financial services sector includes:

- **Phishing and data breaches**
  Phishing has been implicated as the leading threat vector in 90% of data breaches.[24] The financial services sector is one of the most frequently targeted industries—and often the top-targeted industry in any given year.

- **Financial services brands are commonly impersonated for phishing attacks**
  For the first half of 2021, financial services brands were impersonated in 36.4% of all phishing URLs. Commonly impersonated brands included Crédit Agricole, PayPal, Chase, and Wells Fargo.[25] For phishing schemes focused solely on financial payment system brands, PayPal, Mastercard, American Express, and Visa represented 70% of such phishing attacks during 2021.[26]
- **$1 billion stolen in six months in England**
  Online bank fraud in England cost consumers $1 billion in the first half of 2021,[27] earning the United Kingdom the title of "bank scam capital of the world."[28] Avenues for this theft include phishing emails to steal bank account credentials, phone calls impersonating the victim's bank and the UK Financial Conduct Authority, fake financial websites, and the theft of cryptowallets.
- **$10.1 million lost in phishing scams in Singapore in one month for one bank**
  Customers of the OCBC Bank in Singapore lost a combined $10.1 million in December 2021 when they responded to SMS alerts supposedly coming from OCBC to alert of account irregularities. Almost 800 customers clicked the link in the SMS alert and entered their internet banking account credentials, at which point the fraudsters transferred funds out of their accounts.[29] The bank refunded all affected victims as a "one-off gesture of goodwill," making the phishing attack on its customers a costly one for the bank.
- **Even people at cryptocurrency firms fall for phishing attacks**
  bZx, a crypto company, suffered a successful phishing attack against one of its developers in November 2021, resulting in the theft of $55 million in cryptocurrency.[30] The developer opened an attached Word document that contained a malicious macro, which compromised access to his crypto wallet and the wallets of other users.

Financial services brands are a common target for impersonation in phishing attacks.

ATTACKS THAT BYPASS SECURITY PROTECTIONS

Threat actors are actively designing attacks that bypass security protections used by organizations and individuals, such as multi-factor authentication (MFA). MFA has been a key method of stopping phishing attacks from being successful in gaining usable account credentials. Methods of bypassing protections include:

- **Theft of session tokens to cloud services**
  Session tokens are created in a web browser to give and extend access to cloud apps; they play a common enabling role in single sign-on solutions. If a threat actor can capture a user's session token, they gain access to the cloud service in parallel to whatever the user is doing and even when the user changes their password or gets a new authentication code. Session tokens offer persistent access to a service for a set duration of time, often for as many as 30 days. Detecting the theft and use of session tokens is challenging because the token itself is legitimate and has been approved by an authorized user.
- **Fake authentication pages added in front of a user's real SaaS applications**
  Man-in-the-middle attacks seek ways of capturing access to accounts or data without the user being aware that someone else is surreptitiously involved. Threat actors are increasing the sophistication of phishing attacks, for example by giving the phished user access to their real SaaS application at the end of the phishing line, albeit after also stealing their credentials by using fake authentication pages that look and feel just like the real ones. Falling for the phish is less likely to ring alarm bells for the individual when they are presented with their actual account rather than hitting a dead end or error page.

- **Growing use of phishing toolkits to bypass two-factor authentication (2FA)**
  Threat actors are making increasing use of toolkits that bypass 2FA protections by capturing or intercepting the 2FA code or stealing the user's authentication cookie. A recent study found more than 1,200 phishing sites using approaches that bypass 2FA protections, up from 200 sites only three years ago.[31] Phishing toolkits make advanced threat tools available to anyone.

CREDENTIAL STUFFING ATTACKS TO BREAK INTO ACCOUNTS

Data breaches cause immediate problems for the breached company and their customers, but there is a longer-running problem too: they often expose valid credentials for use in new attacks. With more than 15 billion credentials from over 100,000 data breaches available for sale on the dark web,[32] financial services firms face the threat of credential stuffing attacks. In these attacks, credentials compromised from one site are used against another site to see if the user has reused the same credential pair across multiple sites—a common approach by users struggling to remember a plethora of passwords. Even for perfect applications with no vulnerabilities, credential stuffing attacks work because the credentials are valid. Financial services firms faced 3.4 billion such attacks in 2020, up 45% from 2019.[33]

Credential stuffing attacks rely on bots and automated scripts. Several types of cybersecurity protections have proven ineffective at stopping credential stuffing attacks, including web application firewalls, CAPTCHAs, and some types of MFA.[34]

RANSOMWARE INCIDENTS

The past several years have witnessed the continued rise in the threat of ransomware, the pivot toward attacking critical infrastructure, and multi-level extortion designs intended to increase the likelihood of a payout to the threat actor. In the financial services sector, the following is happening:

- **Increasing volume of ransomware activity**
  In the first six months of 2021, the Financial Crimes Enforcement Network in the United States Treasury saw an increasing volume and value of ransomware-related activity in the United States, threatening the financial sector in the United States, along with businesses and the public.[35] The volume and value of activity in the first half of 2021 were both higher than the equivalent activity for all of 2020.
- **Growth of ransomware attacks against banks**
  One study found that the banking industry experienced a 1,318% year-on-year growth in ransomware attacks in the first half of 2021.[36] By contrast, across all sectors, ransomware grew by 148% in the first three quarters of 2021.[37]
- **Growth of ransomware attacks against the wider sector**
  In the third quarter of 2021, financial services was the industry sector facing the most ransomware attacks (22% of total) and the most advanced persistent threat attacks (37% of total). Threats against the sector increased by 21% over the second quarter.[38]
- **Ryuk a problem for financial services**
  The Ryuk ransomware variant was a particular problem for financial services firms during 2020.[39] Ryuk has been linked with nation-state threat groups and is often used in attacks against larger organizations that are judged to have the financial resources to pay a ransom.

Ransomware attacks in the financial services sector increased 10x more than in other sectors.

ATTACKS AGAINST CLOUD SERVICES

Financial institutions are making increasing use of cloud services, with a growing percentage of workloads expected to be hosted in the public cloud.[40] Deployment patterns include the use of multiple clouds, hybrid models combining on-premises infrastructure and multiple cloud services, and use of the cloud services for infrastructure, platform capabilities, and packaged services. Misconfiguration of cloud services has been a significant threat in recent years, driving incidents such as the Capital One data breach on AWS profiled earlier in this white paper.

The adoption of SaaS applications by financial institutions increases the footprint for threat actors. Confidential, sensitive, and personal data types are being entrusted to these applications, with avenues for compromise including exploiting vulnerabilities in cloud services, capturing account credentials through phishing attacks, hijacking session tokens, and moving laterally across connected SaaS applications after an initial breach. SaaS applications are often owned by line-of-business managers and not the IT department, which means the higher-security disciplines that are trained into IT professionals are less likely to be understood and managed by business owners. Unlike with on-premises infrastructure where financial institutions bear the complete weight of ensuring a high security posture, the shared-responsibility model divides security responsibilities between cloud providers and the organization. The model threatens oversights, mistakes, and finger-pointing, particularly when the organization holds onto a mistaken belief that security is the cloud provider's responsibility.[41] Various financial institutions have already failed to ensure their share of responsibilities is met, with examples of access privileges being misconfigured or ignored entirely.

The adoption of SaaS apps by financial institutions increases the attack footprint for threat actors.

INSUFFICIENT SECURITY PRACTICES AT SUPPLY CHAIN PARTNERS

A data breach at a third-party firm can implicate an organization's data, even when due diligence on the security practices at the third-party firm has been undertaken. For example, Debt-IN Consultants, a debt recovery firm that subcontracts to financial services organizations in South Africa, suffered a data breach that compromised personal and financial data on more than 1.4 million people in South Africa sourced from its clients.[42]

BUSINESS EMAIL COMPROMISE (BEC)

Threat actors seek financial gain by compromising business email accounts and conversation threads, attempting to commit invoice fraud, and masquerading as customers ordering wire transfers to bank accounts controlled by the threat actors. When a bank in the United States is targeted for wire transfer fraud, threat actors request an average of $1.5 million.[43] In combination, successful business email compromise attacks in the United States represent the costliest form of cyberattacks against organizations in all sectors.[44]

GROWTH IN LENDING FRAUD DUE TO IDENTITY THEFT

The use of stolen or falsified personal and business identities when applying for a loan—along with the increased use of mobile lending apps—is driving higher rates of lending fraud. LexisNexis found that smaller banks and credit unions (with under $10 billion in assets) along with digital lenders suffered losses of 6.9% of revenue in 2021 due to lending fraud, and larger banks with more than $10 billion in assets faced losses of 5.9% of 2021 revenue.[45] Fraudsters are using stolen personal and financial data to apply for lending that results in funds being stolen from banks and credit unions.

THREATS FROM THE INSIDE

Most financial services organizations also face cyberthreats from internal actors and weak processes. Internal threats include:

- **Lack of cybersecurity talent**
  Locating, hiring, and retaining experienced cybersecurity professionals is an uphill challenge for organizations across all industry sectors—including financial services.[46] Essential tasks are more likely to be left undone or only partially addressed when there are not enough people to build and maintain strong cyber defenses, e.g., patching vulnerabilities, checking phishing alerts.

- **Abuse of organizational position**
  When employees in trusted positions act with malicious intent within a bank or credit union, they cause financial damage at minimum and business closure at worst. This happened recently at a small credit union in the United States, where the CEO opened multiple unauthorized credit cards in her name and kept raising the credit limit. She alone had access to the credit card database and manipulated the interest rates and monthly payments in her favor. The $2.1 million she charged to the cards resulted in the closure of the credit union. She was one of only three employees at the credit union, the board trusted her entirely, and there were no checks and balances to ensure her actions were appropriate.[47] The CEO was sentenced to more than four years in federal prison, followed by three years of supervised release including one year of home detention.[48]

- **Insufficient data protection practices**
  Failure to design or follow strong data security practices—or assure they have been followed—can result in breached or exposed data. Morgan Stanley, for example, faced a class-action suit after its decommissioned computer equipment was found to contain the personal data of over 15 million customers.[49] Morgan Stanley claimed the issue happened because of a software flaw. Insufficient data protection practices were also blamed for the massive data breach at Capital One. Security teams often lack visibility across cloud services to know what data must be protected, and insiders can bypass traditional security controls by exporting data or copying files or databases.

- **Employees not sufficiently trained in security threats**
  Employees willingly, albeit unwittingly, become active participants in a cyberattack when they fail to recognize the telltale signs of a security threat. For example, a hacker breached personal data on more than seven million users of the Robinhood brokerage app by calling the customer support line and tricking a customer support employee into giving up their account credentials to various customer support systems.[50]

- **Employees actively ignoring regulated communication duties**
  Financial institutions are required to archive and supervise the work-related communications of employees. However, employees can easily bypass these requirements by using unsanctioned communication and chat tools, such as WhatsApp, personal email accounts, and Telegram. Regulators do not take a positive view on such behavior; for instance, the Securities Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) fined JPMorgan Chase & Co. a combined $200 million in late 2021 for widespread and systematic avoidance of surveillance responsibilities by using WhatsApp and other unsanctioned platforms.[51] Other banks are under investigation by the CFTC too, including HSBC Holdings[52] and Deutsche Bank.[53]

Employees unwittingly become active participants in a cyberattack when they fail to recognize the telltale signs of a security threat.

LINGERING REPUTATION DAMAGE WITH SLOW ENFORCEMENTS

Financial services organizations experience lingering reputational damage when the fallout from significant data breaches takes years to resolve. Regulatory actions, civil cases, and class-action suits are never resolved quickly, and the elongated timeframes reinforce the awareness of previous failings. The settlement for a class-action suit against Desjardins for the 2019 data breach was only proposed in December 2021.[54] Similarly, the 2019 data breach at Capital One resulted in regulatory action after one year and the settlement for a class-action suit after more than two years.

COMPROMISE OF OAUTH ACCESS TOKENS

OAuth access tokens provide connectivity across SaaS cloud apps, streamlining data flows and simplifying cross-service integration for customers. The simplicity of asking a user to approve an enduring set of rights is also attractive to threat actors. Compromising an application, its data, and rights results from a user unknowingly authorizing malicious OAuth connections after falling for a phishing attack or downloading a compromised app. It also results when an authorized, legitimate third-party party application is compromised—by exploiting a vulnerability, gaining access through a phishing attack, or planting malware—and moving laterally into customer environments, e.g., SolarWinds, Log4j. Since OAuth tokens are given valid authorization by authorized users, the mere presence of an authorized connection is an insufficient threat evaluation. Organizations need to take a nuanced, risk-based approach to continually assess every connection.

ATTACKS AGAINST APPLICATION PROGRAMMING INTERFACES (APIS)

Modern applications publish APIs to enable system functions such as creating accounts, requesting information, and initiating transactions. Threat actors like APIs because they contain vulnerabilities that can be exploited to gain control of an account and steal funds. A recent study documented a litany of API security issues found in mobile apps provided by large and small financial institutions.[55] On a broader scale, at least 75% of the total login attacks against financial institutions seek to compromise APIs. Bots and botnets are prevalent in these attacks.

At least 75% of the total login attacks against financial institutions seek to compromise APIs.

DENIAL OF SERVICE ATTACKS

Denial of service (DoS) attacks flood the servers at a targeted organization with more traffic than they are set up to handle, resulting in applications and services going offline. These may be launched to cause disruption or for financial gain. For example, banks in Australia have been threatened with sustained DoS attacks if they do not pay a ransom in advance,[56] and New Zealand's stock exchange (NZX) was offline for over six days in August 2020 because of a DoS attack.[57] The attack against the NZX was part of a wider attack campaign against financial institutions around the world.[58]

COMPROMISE OF FINANCIAL SYSTEMS

Compromising a victim's financial systems provides the opportunity for a threat actor to create fraudulent transactions directly in the financial system. This type of attack enables the threat actor to create a stack of fraudulent transactions over time. Elephant Beetle, a threat actor group active in Latin America, is stealing millions of dollars from victims in the financial services sector after breaking into and establishing persistence in their financial systems.[59]

The Regulatory Environment

Across the world, the financial services sector is one of the most heavily regulated industries, with controls imposed by governmental and industry bodies on many aspects of operating within the sector. In this section, we look briefly at a sampling of regulations touching on cybersecurity. This treatment is not exhaustive.

UNITED STATES

Cybersecurity regulations in the United States for financial services organizations include requirements to capture and retain data, protect sensitive and confidential data held on organizations and individuals, and develop a set of effective protections against cybersecurity threats. Examples include:

- **SEC (Securities and Exchange Commission)**
  The SEC requires business communications of certain groups to be captured, supervised, and archived. Electronic recordkeeping is permitted and there are strict requirements around immutability and accessibility. The SEC does not take kindly to firms deliberately circumventing data retention requirements.[60]
- **FINRA (Financial Industry Regulatory Authority)**
  FINRA requires that policies and controls are established over how data is captured, managed, and protected. Firms must conduct regular assessments of cybersecurity readiness, actively monitor for insider trading (use of unsanctioned communications apps can signal activities with nefarious intent), and strictly retain certain business records for up to seven years, among others.
- **PCI-DSS (Payment Card Industry Data Security Standard)**
  Organizations that accept credit card and debit card transactions must comply with the PCI standard, which focuses on how card and transaction data is protected during transmission and storage.
- **New York's Cybersecurity Regulation**
  The Department of Financial Services in New York requires most financial institutions to enact a comprehensive cybersecurity policy, identify all internal and external cybersecurity threats, and have the right solutions in place to defend against identified threats. Detection and recovery capabilities are also required, along with regular reporting.
- **NCUA (National Credit Union Administration)**
  Cooperative credit unions that are federally insured need to meet cybersecurity regulations from the NCUA. Regulations cover areas such as developing a comprehensive written security program (including confidentiality and integrity of member records), reporting major incidents and disasters (that are projected to disrupt member services for more than two consecutive business days), and notification of data breach incidents.[61] Federally insured credit unions undergo a periodic review by the NCUA of their information security program; the review must take place at least every 20 months.[62]
- **FFIEC (Federal Financial Institutions Examination Council)**
  The FFIEC offers guidance to financial institutions on a range of cybersecurity topics in the spirit of raising awareness of cybersecurity risks and threats. While its statements do not generally impose regulatory expectations, its materials and approaches have become influential standards for financial institutions and align with the regulations issued by its member agencies in the federal

Financial services is one of the most heavily regulated sectors, with controls imposed by government and industry bodies.

government, including the Board of Governors of the Federal Reserve, NCUA, the Federal Deposit Insurance Corporation, and others.

- **Reporting data breaches and cyber incidents within 36 hours**
  A new federal rule, effective from April 1, 2022, requires banks to disclose data breaches and cyber incidents within 36 hours if they will disrupt or degrade—or threaten to do so—the ability of the bank to perform banking operations or deliver its products and services.[63] Service providers to banks are required to notify their bank customers of similar incidents as soon as possible.
- **State-level data protection requirements, e.g., California, Virginia, Colorado**
  While not specific to the financial services sector, emerging state-level data protection regulations in California, Virginia, and Colorado impose heightened requirements on how the personal data of consumers is captured, stored, protected, and used. Organizations holding covered data must extend certain rights to data subjects.

Financial institutions are audited regularly, with cybersecurity readiness a key assessment criterion.

UNITED KINGDOM

Cybersecurity regulations in the United Kingdom are concerned with similar threats and risks as in the United States. Regulations focus on increasing the cyber resilience of firms in the financial sector. Examples include:

Financial institutions are audited regularly, with cybersecurity readiness a key assessment criterion.

- **PRA (Prudential Regulatory Authority)**
  The overriding concern of the PRA is maintaining financial stability of the UK financial sector. Cyberattacks are viewed as detrimental to reaching this stability objective.[64] A key focus is ensuring that banks and other financial institutions operating in the UK can continue to operate under the threat of operational disruption from cyberattacks. A second key focus is that firms are appropriately managing their third-party risk with cloud providers.[65]
- **FCA (Financial Conduct Authority)**
  The FCA is focused on protecting consumers and the integrity of the financial market.[66] By implication, the FCA wants market participants to develop a security culture, identify their information assets, and have protections and recovery plans in place to mitigate cybersecurity incidents.[67] Staff awareness of cyberthreats is viewed as an essential component of a strong cybersecurity posture, along with visibility into where data is stored and processed by the firm itself and via third-party partners. Firms must carry out regular cybersecurity reviews, be appropriately wary of cloud outsourcing agreements, and ensure vulnerabilities in affected applications are patched promptly.[68] Firms must report data breaches and cyber incidents when loss of data, availability, or control occurs.
- **Data Protection Act**
  The Data Protection Act 2018 implements Europe's General Data Protection Regulation into UK law.[69] Organizations are required to protect the personal data of customers, extend a set of data rights to customers, and advise of data breaches and cyber incidents that result in decreased system availability. Organizations must establish controls on how personal data is used for profiling and decision-making. Based on reports from organizations of data security incidents, the financial services sector in the United Kingdom ranks as the third-highest sector in terms of reported incidents. The sector also has the highest

count for ransomware and access misconfiguration incidents and the second-highest number of phishing incidents.[70]

REGULATIONS IN OTHER REGIONS

Financial services organizations in other regions and countries are also subject to a range of cybersecurity-related regulations. Three brief examples are:

- **GDPR (European Union's General Data Protection Regulation)**
  The GDPR offers cross-industry regulation on how personal data is captured, stored, managed, protected, and used. GDPR elevates the rights available to data subjects and significantly increases the administrative fines that can be levied against organizations that fall afoul of its requirements. Data breaches must be notified to the relevant data protection authority within 72 hours.
- **Australia's CPS 234 on managing information security risk**
  Released in mid-2019 by the Australian financial services regulator, CPS 234 sets standards for information security by covered entities.[71] Requirements include timelines for notifying the regulator of security incidents, the need for controls over third-party suppliers, and ongoing threat and vulnerability assessments, among others. The regulator intends to take an active approach in assessing the efficacy of cybersecurity protections, too, rather than solely relying on attestation.[72]
- **South Africa on data breach notification**
  Standard Bank of South Africa took nine days to notify customers affected by a data breach of its online property platform. The Information Regulator in South Africa ruled that nine days was too long, even though the Protection of Personal Information Act specifies the reporting standard to be "as soon as reasonably possible" rather than defining the number of hours or days within which disclosure must happen.[73]

THE DRIVE FOR OPERATIONAL RESILIENCE

Financial services industry regulators across the globe—such as the FCA and partners in the United Kingdom, the Federal Reserve and partners in the United States, and the Basel Committee on Banking Supervision—are driving an operational resilience agenda across the sector.[74] In the United States, operational resilience is viewed as "the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions."[75]

Industry regulators are driving an operational resilience agenda across the financial services sector.

The growth in cyberattacks—especially ransomware against critical infrastructure—has raised the risk of the financial system being rendered non-operational. If financial applications are rendered useless due to distributed denial-of-service attacks or unwanted encryption through ransomware, individual customers and the economy at large are hampered at best or prevented at worst from completing financial transactions. While financial resilience remains essential, which means banks and other financial organizations having sufficient reserves to function through lean times, the two types of resilience are increasingly intertwined. A country's financial system can be more easily destabilized by disrupting the operational capability of its financial institutions and technology partners, either due to attacks by malicious external actors or irregular and devastating events. Such destabilization can be manipulated on a quicker and easier timeframe by threat actors than waiting for the next cycle of systemic financial weakness to hit.

Attractiveness of the Financial Services Industry as a Target for Attacks

The financial services industry continues to be an attractive target for threat actors. Reasons include:

- **Money, money, money**
  Financial institutions hold and process vast sums of money, most of it belonging to other people. Compromising transaction logic, gaining account credentials for consumers with healthy bank balances, and diverting funds to an account controlled by a threat actor all provide a rich payday.
- **Potential for financial sabotage against a country**
  A successful cyberattack against a large financial institution has the potential to cripple the financial system of a nation, with potential flow-on effects to the wider global financial system. Non-operational financial systems quickly impede economic activity, bring normal life to a standstill, and undermine consumer and business confidence. Threat actors see the potential to inflict rapid havoc on a nation by attacking the players in its financial system—a strategy that was used recently to deter Russian aggression in its war against Ukraine.[76] Financial institutions shut down or otherwise compromised by a cyberattack face high urgency to enact a quick resolution.
- **Valuable data for identity theft and subsequent attacks**
  Compromising data on customers provides up-to-date personal data for use in identity theft and other attacks. Names, addresses, banking information, contact details, and mortgage documents offer details that can be used in impersonation attempts. The same underlying data can be used in phishing and vishing (voice phishing) attempts intended to capture account credentials, bypass multi-factor authentication controls, and steal funds from unwary customers. Industry regulations require banks to retain certain types of data for up to seven years, and banks themselves often choose to retain data for a lot longer. For example, Credit Suisse suffered a data breach covering more than 18,000 bank accounts, including some dating from the 1940s.[77]
- **Rapid modernization risks undermining security posture**
  Established financial services firms are under competitive attack from fintech startups, non-traditional financial services organizations, and new cryptocurrency offerings. Established players are rushing to modernize systems, create new products and services, and release updated account offerings to reduce customer churn. Such speed, however, risks creating new security shortcomings by releasing vulnerable applications, relying on cloud services with insufficient security provisions, and not hardening systems and processes sufficiently before releasing them to market.
- **Low-risk criminal activity, e.g., theft from the comfort of an armchair on the other side of the world**
  Cyberattacks hold the potential for criminals to steal significant funds from the relative safety of their home or office. They do not require trucks, dynamite, firearms, fake passports, or a band of thieves with whom to collaborate. With business email compromise attacks, the ideal scenario is that a falsified wire transfer is executed with the money appearing soon thereafter in the criminal's bank account. And hopefully just in time for a morning jaunt to the local coffee house.

Access to money, sabotaging financial systems, and stealing data for identity theft are key motivators for threat actors.

The Outlook for Threat Dynamics Against Financial Services

The financial sector will remain a key focus for cyberattacks and cyber fraud. Some threat actors unleash cyberattacks in pursuit of financial gain through malicious or nefarious means; others seek to destabilize a country's financial system.

The outlook we see for the financial sector is:

- **Protect your data; someone else wants it**
  Financial services organizations hold valuable data on individuals, businesses, and government agencies. This is not going to change. Compromising such data enables threat actors to collect intelligence for direct attacks against victims or to use up-to-date data to attempt various types of financial and lending fraud against banks and insurance companies through identity manipulation.
- **Protect your financial resources; other people want to steal them**
  Financial services organizations are the mechanism by which financial resources are stored, transferred, and protected. This is not going to change, although newer forms of currency will be added to the mix. Threat actors will remain perpetually interested in gaining access to funds that do not belong to them. Phishing and business email compromise attacks will continue, along with threat actors impersonating and masquerading as trusted financial services firms to bypass security protections and consumer awareness to steal funds.
- **Protect the availability and integrity of your systems; other people want to undermine them**
  Financial systems, networks, and interconnections facilitate the economic activities of individuals, organizations, and nations. Crippling or degrading the performance of these systems holds interest for nation-state actors to inflict economic pain and retaliatory pressure on other nations. For example, the Reserve Bank of Australia takes the view that a successful cyberattack against a significant financial institution in Australia is just a matter of time. There is so much threat activity happening that it is all but inevitable.[78]

With cyber insurance increasingly difficult to secure, firms face a changing risk calculus.

The potential of threats against financial institutions to undermine or destabilize a country was writ large from the early stages of the Russian war on Ukraine. Several financial sanctions were put in place against Russia, such as removing its access to the SWIFT financial network.[79] Fear of retaliatory attacks by Russia against financial sector organizations across the world greatly increased, with federal and national agencies warning banks, credit unions, and organizations across other sectors to be in a state of heightened readiness to counter cyberattacks (e.g., CISA in the United States[80] and the European Central Bank for European banks.[81])

Finally, cyber insurance is getting more difficult and costly to secure, with insurers ramping up premiums for much less coverage.[82] The growth in successful cyberattacks—particularly ransomware—has had a dramatic negative effect on the profitability of underwriters, and hence they are rebalancing their risk calculations.[83] Firms in all sectors, including financial services, will need to ensure they have the right technology solutions in place to counteract threats that insurance coverage was previously used for.

Cybersecurity Solutions to Consider

Financial services organizations have been increasingly under attack from cyber threat actors, and this trajectory is unlikely to abate. Firms need to ensure they have the right solutions in place to protect and defend themselves, their customers, and the financial systems in which they participate. It is important to note that solutions require people with an advanced understanding of how the parts of an effective cybersecurity implementation work together. For this, management must allocate funds, resources, and employee time to learn, understand, and think about these intersections. Ongoing education is key, which involves more than just getting a security certification.

In this section, we talk solutions.

CLOUD SECURITY, INCLUDING VISIBILITY AND VULNERABILITY

Ensuring the security of cloud services is critical as adoption increases. Organizations across all sectors—including financial services—are increasingly entrusting sensitive data to business-critical IaaS platforms and SaaS applications. These are complex systems with intricate functionalities, and designing, implementing, and extending a strong security posture across these platforms and apps is challenging. Financial services organizations benefit from specialized solutions that identify and mitigate threats, harden security posture, and provide early warning of vulnerabilities.

Protect cloud services from threats, misconfigurations, and risky connections.

Cloud security solutions should highlight initial misconfigurations, risky connections, questionable authentications, drift in configuration over time, and more. Specific offerings to look for are:

- **CASB (Cloud Access Security Broker)**
  CASB solutions monitor which cloud services users are connecting to, what types of data are being stored in the respective services, and where connections are coming from, among others. They give visibility that is unavailable with traditional monitoring solutions and can enforce data security policies for risky content and connections. CASB solutions provide an ongoing assessment of the risk of each identified cloud service, thereby helping IT and security teams to prioritize mitigation actions for cloud services.
- **CSPM (Cloud Security Posture Management) and SSPM (SaaS Security Posture Management)**
  Security posture management solutions cover both cloud infrastructure providers (CSPM) and SaaS solutions (SSPM). They provide ongoing visibility into and analysis of the configuration of various IaaS and SaaS services, recommendations on how to harden the security configuration (e.g., by removing access rights or reducing the access scope for an individual or group of people), and alerts on changes in security configurations that undermine the targeted posture. With the increased reliance of cloud offerings—IaaS and SaaS—having perpetual insight into security standing is critical. These solutions seek to prevent the type of attack that proved so costly for Capital One.

Cloud security solutions leverage artificial intelligence (AI) and machine learning (ML) models to analyze the behavior of users and data to detect threats such as account compromise, malicious insiders, and the exploitation of vulnerabilities.

IDENTITY AND AUTHENTICATION FOR EMPLOYEES AND CUSTOMERS

Move in the direction of fewer passwords and more biometrics for stronger authentication processes for employees and customers. Uniquely identifying an employee and ensuring the person supplying the authentication credentials is the correct employee is doomed to fail with usernames, passwords, and even basic forms of multi-factor authentication. Managed identity solutions where biometric identification using fingerprints or facial recognition is tied to an identity provides high-assurance authentication for employees doing their work, along with cryptographic hardware keys used in combination with managed biometrics.

Financial services organizations need to strengthen identity and authentication workflows for customers too, not just employees.[84] Customers form an integral part of the financial system; they access and interact with accounts and loan products, and initiate standard and high-value transactions. Providing system access to customers using only a username and password is an open invitation for compromise, and stronger methods of authentication within mobile apps, biometrics for multi-factor authentication, and zero-trust principles for detecting abnormal device and network characteristics are essential. High assurance that the person requesting access to an account or initiating a transaction is who they claim to be is critical for avoiding fraud and loss. Dependence on basic 2FA approaches, such as codes sent by SMS or email, should be eliminated in workflows granting system access to customers because the protections originally offered by these approaches are increasingly easy to break. There is an increasing digitalization of the banking experience for consumers, driven forcibly by shelter-in-place and lockdown orders during the pandemic and the closure of branch offices with the further erosion of any remaining face-to-face relationship between bankers and consumers. Developing stronger means of identity assurance is key to ongoing customer interaction and banking experiences.

Develop stronger means of identity assurance to safeguard customer interactions and banking experiences.

Identity and authorization must be monitored for hacking attempts, password-spray attacks, credential dumping, and attempts to use stolen credentials. Cloud security solutions offer capabilities for monitoring where authorization requests are coming from, as do identity management solutions.

TACKLING OVERPRIVILEGED ACCESS

Any employee or contractor with access rights to data and systems that exceed what is necessary for their work tasks poses a risk to a financial services organization. This can result in data theft by a malicious employee, accidental oversharing by an employee, or data theft by an external threat actor after compromising an employee's credentials. One survey found that 37% of companies had detected overprivileged accounts in their environment, and 59% of the companies said privileged account credentials had been successfully phished.[85]

Systems that monitor and analyze the access levels of employees (including managers, executives, IT administrators, and contractors) to identify overprivileged access rights enable early intervention to reset rights to a more appropriate level. Such right-sizing reduces the likelihood that accounts with inappropriately high levels of access exist, reduces access drift when rights are mistakenly extended, and decreases the blast radius in the event of an insider attack or external breach. Systems that tackle overprivileged access use AI and ML models to create a normalized baseline of access rights for employees based on a reference group—for example, a marketing analyst should have the same level of rights as other marketing analysts in the marketing department. Deviations from the norm can be

automatically adjusted or permitted to continue based on authorization from the employee's manager.

For individuals that require high levels of access to systems, Privileged Access Management (PAM) solutions introduce additional safeguards. For example, rather than turning on super-user rights continually on the account, the user requests a time-limited or transaction-limited grant of elevated access which must be approved, is audited, and is automatically revoked when the time has elapsed or the transaction is completed.

Finally, overprivileged access also occurs when connections between apps, such as OAuth tokens used widely in SaaS environments, are granted unwisely or unwittingly to malicious actors. Use solutions to continually assess the intent of OAuth connections, detect hidden threats, and harden security configurations.

BOT MANAGEMENT

Bots and botnets are harnessed by threat actors to enable cyberattacks including distributed denial-of-service, credential stuffing, and API attacks. Bot management solutions that identify, block, and mitigate bot traffic enable firms to prevent downtime, protect customer accounts from opportunistic credential compromise, ensure APIs do not disclose protected or sensitive data, and prevent the introduction of malware to facilitate persistent access by threat actors. Bot management solutions that stop bot traffic enable greater responsiveness for valid customers, stop the creation of fake user accounts that can be used for subsequent attacks, and prevent false transactions when credit card details are brute-forced.

Identify and block malicious bot traffic to protect customer accounts and safeguard APIs.

ADVANCED EMAIL SECURITY TO PROTECT AGAINST PHISHING, MALWARE, AND BEC

Protect your email system and the email communication channel from impersonation, email-borne threats, and business email compromise attacks. The following solutions strengthen protections in these areas:

- **Scan messages, attachments, and links for malicious content**
  Email is a very common channel for delivery of malicious threats, with attachments and embedded links particularly pernicious. All inbound content should be scanned for the presence of threats, as should messages sent outbound to capture threats sent from compromised accounts or devices. Vendors of email security solutions seek to differentiate themselves based on features such as catch rates, levels of analysis (i.e., recursively unpacking and examining each individual component in a message or embedded attachment), and link scanning on use to capture post-delivery weaponization that is missed if link scanning is performed only on initial delivery.
- **Ensure SPF, DKIM, and DMARC are set up and aligned**
  Three basic Internet standards are available to protect email systems from impersonation, spoofing, and use for phishing attacks against other organizations. SPF (Sender Policy Framework) specifies the email hosts that are trusted to send email for a domain. DKIM (DomainKeys Identified Mail) signs messages using cryptography to assert validity. DMARC (Domain-based Message Authentication, Reporting and Conformance) states what organizations should do when receiving messages with suspicious attributes and includes reporting options for identifying fraudulent message flows. In combination, these controls increase the authenticity of the email channel.

Making changes to these controls normally requires updating DNS records, but there are newer and more dynamic approaches that simplify the configuration.

- **Track potential brand abuse**
  Misuse of brand names enables threat actors to masquerade as a trusted financial entity, for example, by registering the same domain name with a different extension or slightly different spelling to create a lookalike domain name or registering a new domain name that sounds like a trusted domain name. Use domain monitoring services to track and alert on the creation of domain names that could be used in attacks against customers.
- **Monitor cloud email services for vulnerabilities**
  Firms using cloud email services, such as Microsoft 365, should monitor for vulnerabilities in configuration and usage. This includes the use of legacy authentication protocols, legacy email standards for accessing messages (e.g., POP and IMAP), the creation of mail forwarding and deletion rules (which often happens when a threat actor takes over an employee's inbox), and forwarding email to personal accounts. SaaS Security Posture Management (SSPM) solutions provide visibility to identify and rectify such vulnerabilities.

VULNERABILITY AND PATCHING

Unpatched applications send an "open for compromise" signal to threat actors. Reducing the breadth and frequency of unpatched applications is a key strategy for reducing data leakage and data breaches. Systems that monitor for new vulnerability advisories from application vendors, match advisories against a real-time catalog of deployed applications and versions, and offer a prioritized list of patches to deploy give financial services organizations the data needed for keeping their application landscape up to date. Automated patching helps to reduce the elapsed time between identification and mitigation of a vulnerability, and virtual patching solutions protect applications from potential security threats while the vendor develops and tests an actual patch.

EXTERNAL ATTACK SURFACE MANAGEMENT

Threat actors conduct reconnaissance to find unpatched vulnerabilities, unprotected data, and exposed ports for remote access into a targeted victim's network and cloud data repositories. External attack surface management solutions provide financial services organizations with the ability to consistently audit and assess weaknesses in systems and cybersecurity controls. These solutions detect, identify, categorize, prioritize, mitigate, and address weaknesses directly or through notification to the security team. Security posture is continually assessed as vendors advise of new system vulnerability, new SaaS and IT systems are added by business units, and merger and acquisition activity brings new networks and risks into the wider security remit.

Protect email from impersonation, email-borne threats, and business email compromise attacks.

SECURITY AWARENESS TRAINING

Employees in financial services organizations hold the keys to important financial systems. If a threat actor can compromise an employee through a phishing, vishing, smishing or business email compromise attack, then credentials and funds can be stolen. Employees need regular training on the warning signs of cyberthreats, common social engineering tricks, and best-practice security hygiene to reduce the likelihood of a successful attack.

Best-in-class security awareness training programs include assessment methods in addition to training content in order to gauge the efficacy of employees at detecting and mitigating attacks. Employees or groups of employees showing low efficacy despite recent training interventions can be offered additional training, stronger process protections, and better security technologies. If employees refuse to follow security policies, reassess ongoing employment status.

MANAGED SECURITY SERVICES

Managed security services offer a pathway for firms to gain access to advanced security services, address the severe shortage of cybersecurity talent, and add layers of prevention and detection to increase overall security posture. Some services offer a comprehensive collection of services—including Managed Security Service Providers (MSSPs) and Managed Detection and Response (MDR) services. Other services take a narrower but specialized focus to complement internal activities with specialist external services, such as protection against DDoS attacks.

SECURITY AUTOMATION, ENCRYPTION, AND INFORMATION GOVERNANCE SOLUTIONS

Financial services organizations should consider a range of other cybersecurity solutions to improve their security posture. These include:

- **Security automation for triage and response**
  Security teams are frequently overworked and under-resourced, resulting in security alerts remaining unaddressed. Security automation solutions offer tools for triaging alerts to assign relative priority, playbooks to follow automatically when responding to certain types of threats, and aggregation of isolated alerts into more comprehensive and cohesive cases. Security automation solutions decrease the amount of manual effort required by cybersecurity professionals to rise above the noise.
- **Strong data encryption**
  Modern cryptographic solutions enable data to be encrypted when stored, when in transit, and when in use. Designing the use of strong encryption into financial systems and apps means that cleartext data is not accessible by internal or external threat actors.
- **Information governance solutions**
  Many regulations require that data is retained securely for a certain timeframe and protected from unauthorized access, modification, and deletion. Information governance solutions enable retention policies to be defined and enforced on data across multiple repositories, with automated or on-approval deletion of data after the required timeframe has elapsed. Minimizing the retention of older data reduces the data footprint available for breach.

Employees need regular training on the warning signs of cyberthreats, common social engineering tricks, and best-practice security hygiene.

Best Practices in Cybersecurity

Readiness to handle cybersecurity threats requires a healthy mix of the right technology, attentive and well-trained people, and strong processes. In this section, we look at a range of practices that combine and leverage all three factors.

REVIEW AND UPDATE CYBER RISK ASSESSMENT

While financial services organizations have common attributes and must comply with a range of similar regulations, each firm faces a different set of specific cybersecurity threats, risks, and concerns. Broad and general guidance, as outlined in this white paper and other sources, is good for sparking a reconsideration of cyber risk but not for enumerating the specific risk context of a given firm. Leading such a review is the responsibility of the Chief Information Security Officer (CISO) or someone holding an equivalent role.

Every organization acting in or supporting others in the financial services sector needs to review and update their assessment of cyber risk. Specifying the steps in undertaking a cyber risk assessment is beyond the scope of this white paper, and there are enough risk assessment checklists by government agencies and industry regulators that doing so is unnecessary. The best practice we call out is to ensure your cyber risk assessment is current, comprehensive, and relevant to your organization.

STRENGTHEN PRACTICES FOR INTERACTING WITH CUSTOMERS

Customers of financial services organizations are also under attack, with threat actors leveraging valid communication channels for malicious purposes. Examples include phishing emails purporting to come from their bank, telemarketing calls to "warn" of suspicious account activity, and account checkups to "gauge satisfaction" with banking products. When customers find it increasingly difficult to differentiate valid email messages and phone calls from malicious ones, problems escalate.

All financial services organizations should revisit how customers authenticate with their financial products and how financial institutions contact customers about their accounts. Newer and stronger methods of assuring the authenticity and integrity of communication channels are essential to avoid lost funds, compromised personal data, and degraded trust with financial providers. The growing availability of biometric controls built into smartphones and mobile devices is increasing awareness among customers of newer forms of authentication.[86]

Revisit how customers authenticate with financial products and how contact with customers can be made more secure.

STRENGTHEN RISK MANAGEMENT FRAMEWORKS WHEN WORKING WITH THIRD-PARTY FIRMS

Third-party compromise and supply chain incidents are casting a more significant shadow over financial services organizations, as we have highlighted in this white paper. Yet, working with third-party firms is here to stay because they offer cost and process efficiencies that are unattainable using in-house resources and systems. What can change, however, is to shift away from loose data security arrangements when contracting with third-party firms and to enforce proactive systematic auditing procedures to identify areas of weakness and vulnerability before a threat actor does. Such an approach relies more stridently both on attestation by the third party of good security practice and audited compliance.

TIGHTEN INTERNAL RISK MANAGEMENT PROCESSES

While most financial services organizations have strong internal risk management processes, several recent cybersecurity incidents have pointed to critical weaknesses remaining unaddressed for too long. For example, internal security reviews at both First American Financial[87] and the Reserve Bank of New Zealand[88] identified weaknesses months before the vulnerability was publicly disclosed (First American) or exploited (Reserve Bank of New Zealand). Both institutions had the opportunity to resolve the issue in advance of a breach, but neither assigned sufficient priority or resources to doing so.

It is worth asking the question again: what critical issues have our internal processes highlighted that have not been resolved yet? For added assurance, commission an external review of the current internal risk management process to uncover systematic weaknesses in the identification and prioritization of risks.

DESIGN FOR REPEATED DISRUPTION, NOT JUST TESTING

The increasing drive to ensure operational resilience in the face of relentless cyberthreats means that financial institutions must think beyond scenario planning to how systems are designed to embrace systematic disruption. Concepts from earlier generations of failover, disaster recovery, and redundant network connections can be leveraged to create resilient systems across hybrid and multi-cloud platforms. Firms should be systematically but unpredictably creating points of failure and disruption in their systems to ensure resilience is a reality. Practicing for real-world disruption using software-defined networking and system failover techniques enables higher assurance than annual scenario testing will ever offer.

CYBERSECURITY TRAINING IS GOOD, HUMAN RESILIENCE IS BETTER

Addressing the people factor is an integral part of increasing cyber resilience in the financial services industry. People with inadequate training, awareness, competency, and skill to deal with stressful cybersecurity incidents will hamper recovery efforts. Intentional and proactive exposure of key people to systematic but unpredictable disruption builds the mental, physical, and emotional resilience to respond appropriately when facing the heat of an actual event. Financial services institutions will benefit from embracing the training, simulation, and scenario practices used in the military to build human resilience.

What critical cybersecurity issues have been highlighted by internal processes but remain unresolved?

Conclusion

Financial services is too important a sector to leave unprotected from enduring and emerging cyberthreats. Organizations in the sector must take warning from the changing nature of threats, assess the next wave of weaknesses and vulnerabilities, and implement solutions and best practices to protect and defend themselves, their customers, and the wider financial system.

Sponsored by BIO-key International

BIO-key is a trusted provider of Identity and Access Management (IAM) and Identity-Bound Biometric solutions that offer an easy and secure way to authenticate the identity of employees, customers, and suppliers while managing their access across devices and applications.

Over 1,000 global customers, including the federal government and 200+ higher education institutions, trust BIO-key PortalGuard IDaaS, an award-winning IAM platform, to reduce password-related help desk calls by up to 95%, eliminate passwords, secure remote access, prevent phishing attacks, and improve productivity for the IT team. PortalGuard provides the simplicity and flexibility required to secure the modern digital experience with options for single sign-on, self-service password reset, and multi-factor authentication, and is the only IAM platform to offer Identity-Bound Biometrics.

Backed by decades of expertise, BIO-key has a proven track record of successful IAM project delivery and strong customer relationships.

Learn more at www.BIO-key.com.

www.BIO-key.com

info@BIO-key.com

+1 732 359 1100

---

[1] Stephanie Walden and Mitch Strohm, What Is a Neobank?, June 2021, at https://www.forbes.com/advisor/banking/what-is-a-neobank/

[2] US Department of Justice, Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency: Government Seized $3.6 Billion in Stolen Cryptocurrency Directly Linked to 2016 Hack of Virtual Currency Exchange, February 2022, at https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency

[3] Mason Wilder, Are You Ready to Seize Some Cryptocurrency?, March 2022, at https://www.acfeinsights.com/acfe-insights/2022/3/7/are-you-ready-to-seize-some-cryptocurrency

[4] Megan Leonhardt, Online fraud attempts are up 25% in the US - here's why, June 2021, at https://www.cnbc.com/2021/06/03/why-online-fraud-attempts-are-up-25percent-in-the-us.html

[5] ABA Banking Journal, Survey: Cyber Fraud Tops List of Bank Concerns about Global Economy, January 2022, at https://bankingjournal.aba.com/2022/01/survey-cyber-fraud-tops-list-of-bank-concerns-about-global-economy/ and World Economic Forum, What are the biggest business risks of 2022? Experts explain, January 2022, at https://www.weforum.org/agenda/2022/01/biggest-business-risks-2022

[6] ICO, Data security incident trends: Q2 2021-22, October 2021, at https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[7] Office of the Comptroller of the Currency, OCC Assesses $80 Million Civil Money Penalty Against Capital One, August 2020, at https://www.occ.treas.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html

[8] Karen Hoffman, The high cost of mishandling data breaches, security reporting for financial services, January 2022, at https://www.scmagazine.com/analysis/breach/the-high-cost-of-mishandling-data-breaches-security-reporting-for-financial-services

[9] NTT Application Security, AppSec Stats Flash - 2021 Year in Review, February 2022, at https://info.whitehatsec.com/stats-flash-year-in-review.html

[10] Regina Mihindukulasuriya, PNB denies cybersecurity firm's claim that 180 million customers' data was breached, November 2021, at https://theprint.in/tech/pnb-denies-cybersecurity-firms-claim-that-180-million-customers-data-was-breached/770455/

[11] NTT Application Security, AppSec Stats Flash - 2021 Year in Review, February 2022, at https://info.whitehatsec.com/stats-flash-year-in-review.html

[12] Zach Whittaker, FTC settles with data analytics firm after millions of Americans' mortgage files exposed, January 2022, at https://techcrunch.com/2022/01/05/ftc-settle-mortgage-files-exposed/

[13] Commissioner Rebecca Kelly Slaughter, Dissenting Statement of Commissioner Rebecca Kelly Slaughter, December 2021, at https://www.ftc.gov/system/files/documents/public_statements/1599131/1923126ascensionslaughterdissent.pdf

[14] Brian Krebs, NY Charges First American Financial for Massive Data Leak, July 2020, at https://krebsonsecurity.com/2020/07/ny-charges-first-american-financial-for-massive-data-leak/

[15] Jaclyn Jaeger, First American Financial settles SEC charges for cyber-security failures, June 2021, at https://www.complianceweek.com/regulatory-enforcement/first-american-financial-settles-sec-charges-for-cyber-security-failures/30480.article

[16] New York State Department of Financial Services, Department of Financial Services Announces Cybersecurity Charges Against a Leading Title Insurance Provider for Exposing Millions of Documents

With Consumers' Personal Information, July 2020, at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221
[17] Dave, Security incident at Dave, July 2020, at https://www.dave.com/blog/post/
[18] Karl Flinders, Digital bank customer data breached through third party, July 2020, at https://www.computerweekly.com/news/252486767/Digital-bank-customer-data-breached-through-third-party
[19] U.S. Risk, The Risk of Employee Theft and Crime in Financial Institutions, February 2020, at https://www.usrisk.com/about-us-risk/news-and-articles-all/2-11-20-the-risk-of-employee-theft-and-crime-in-financial-institutions/
[20] Frederic Tomesco, Desjardins Says Data Breach Also Affects 1.8-Million Credit-Card Accounts, December 2019, at https://montrealgazette.com/business/local-business/desjardins-says-data-breach-also-affects-1-8-million-credit-cardholders
[21] Office of the Privacy Commissioner of Canada, Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019, December 2020, at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/
[22] Kugler Kandestin, Settlement of Class Actions Related to the Personal Information Breach Announced by Desjardins in 2019, December 2021, at https://www.newswire.ca/news-releases/settlement-of-class-actions-related-to-the-personal-information-breach-announced-by-desjardins-in-2019-844138744.html
[23] American Bankers Association, Phishing Scams, February 2022, at https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/phishing
[24] Cisco Umbrella, 2021 Cybersecurity Threat Trends: Phishing, Crypto Top the List, April 2021, at https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
[25] Vade, Vade Report Reveals Meteoric Rise in Phishing in H1 2021, July 2021, at https://www.vadesecure.com/en/company/news/vade-report-reveals-meteoric-rise-in-phishing-in-h1-2021
[26] AtlasVPN, PayPal and Mastercard most impersonated in financial phishing schemes in 2021, March 2022, at https://atlasvpn.com/blog/paypal-and-mastercard-most-impersonated-in-financial-phishing-schemes-in-2021
[27] Lawrence White and Iain Withers, Welcome to Britain, the bank scam capital of the world, October 2021, at https://www.reuters.com/world/uk/welcome-britain-bank-scam-capital-world-2021-10-14/
[28] Marc Shoffman, UK is branded the 'bank scam capital of the world' with a lack of police resources blamed for rampant fraud, December 2021, at https://inews.co.uk/inews-lifestyle/money/saving-and-banking/uk-bank-scam-capital-world-lack-police-resources-1351256
[29] Philip Heijmans, OCBC to Give S$13.7 Million of Goodwill Payouts After Scam, January 2022, at https://www.bloomberg.com/news/articles/2022-01-30/ocbc-completes-s-13-7-million-of-goodwill-payouts-from-sms-scams
[30] Kevin Shalvey, A hacker stole more than $55 million in crypto after a bZx developer fell for a phishing attack, November 2021, at https://www.businessinsider.com.au/hacker-steals-55-million-in-crypto-after-bzx-phishing-attack-2021-11
[31] Catalin Cimpanu, More than 1,200 phishing toolkits capable of intercepting 2FA detected in the wild, December 2021, at https://therecord.media/more-than-1200-phishing-toolkits-capable-of-intercepting-2fa-detected-in-the-wild/
[32] Digital Shadows, 15 Billion Usernames And Passwords For Internet Services Including Bank And Social Media Accounts On Offer To Cyber Criminals, Finds New Research From Digital Shadows, SOURCE, 20200707, at https://www.digitalshadows.com/press-releases/15-billion-usernames-and-passwords-for-internet-services-including-bank-and-social-media-accounts-on-offer-to-cyber-criminals/
[33] Akamai, Financial Services, Credential Stuff & Web Application Attacks, May 2021, at https://www.akamai.com/newsroom/press-release/-akamai-security-research--financial-services-continues-getting-
[34] Office of the New York State Attorney General Letitia James, Business Guide for Credential Stuffing Attacks, January 2022, at https://ag.ny.gov/sites/default/files/businessguide-credentialstuffingattacks.pdf
[35] Financial Crimes Enforcement Network, Financial Trends Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, October 2021, at https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf
[36] Trend Micro, Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats, September 2021, at https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats
[37] SonicWall, Sonicwall: 'The Year of Ransomware' Continues With Unprecedented Late-Summer Surge, October 2021, at https://www.sonicwall.com/news/sonicwall-the-year-of-ransomware-continues-with-unprecedented-late-summer-surge/
[38] Trellix, Trellix Advanced Threat Research Report: January 2022, January 2022, at https://www.trellix.com/en-us/threat-center/threat-reports/jan-2022.html

[39] Cisco Umbrella, 2021 Cybersecurity Threat Trends: Phishing, Crypto Top the List, April 2021, at https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list
[40] Ron Shevlin, Banks' False Sense of Cybersecurity Will Be Shattered by Cloud Computing, Forbes, August 2020, at https://www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/
[41] Prasad Chaudhari, Recognizing the Customer's Responsibily in a Shared Responsibility Model, January 2022, at https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/recognizing-the-customers-responsibility-in-a-shared-responsibility-model
[42] Jessica Haworth, Millions of South Africans caught up in security incident after debt recovery firm suffers 'significant data breach', September 2021, at https://portswigger.net/daily-swig/millions-of-south-africans-caught-up-in-security-incident-after-debt-recovery-firm-suffers-significant-data-breach
[43] David Heun, Banks confront new type of phishing: 'Salami' attacks, September 2021, at https://www.americanbanker.com/news/banks-contend-with-new-type-of-phishing-salami-attacks
[44] FBI, FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report, Including COVID-19 Scam Statistics, March 2021, at https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
[45] LexisNexis, Small and Mid-sized Business Lending Fraud Study Results, February 2022, at https://risk.lexisnexis.com/insights-resources/research/smb-lending-fraud-study
[46] Kyle Wiggers, Studies show cybersecurity skills gap is widening as the cost of breaches rises, July 2021, at https://venturebeat.com/2021/07/28/studies-show-cybersecurity-skills-gap-is-widening-as-the-cost-of-breaches-rises/
[47] FBI, CEO's Theft Leads to Closure of Credit Union: Leader Spent $2.1 Million on Personal Purchases, Including a Pig Farm, February 2022, at https://www.fbi.gov/news/stories/ceos-theft-leads-to-closure-of-credit-union-021722
[48] United States Department of Justice, Former Federal Credit Union President Sentenced to More than Four Years in Prison for Embezzlement and Failing to File Taxes, January 2022, at https://www.justice.gov/usao-wdpa/pr/former-federal-credit-union-president-sentenced-more-four-years-prison-embezzlement-and
[49] Bob Van Voris, Morgan Stanley to Pay $60 Million to Settle Data-Breach Suit, January 2022, at https://www.bloomberg.com/news/articles/2022-01-03/morgan-stanley-to-pay-60-million-to-settle-data-breach-claims
[50] Annie Massa, Robinhood Data Breach Nightmare Hinged on Customer Service Slip, November 2021, at https://www.bloomberg.com/news/articles/2021-11-08/robinhood-data-breach-exposes-data-on-millions-of-customers
[51] Hannah Levitt and Benjamin Bain, JPMorgan Bosses Hooked on WhatsApp Fuel $200 Million Penalty, December 2021, at https://www.bloomberg.com/news/articles/2021-12-17/jpmorgan-bosses-addicted-to-whatsapp-fuel-200-million-in-fines
[52] Harry Wilson, HSBC Under Investigation in U.S. Over WhatsApp Use, February 2022, at https://www.bloomberg.com/news/articles/2022-02-22/hsbc-says-it-s-under-investigation-in-u-s-over-whatsapp-use
[53] Steven Arons and Macarena Munoz Montijano, Deutsche Bank Warns Staff Not to Delete WhatsApps Amid Scrutiny, February 2022, at https://www.bloomberg.com/news/articles/2022-02-21/deutsche-bank-warns-staff-not-to-delete-whatsapps-amid-scrutiny
[54] Kugler Kandestin, Settlement of Class Actions Related to the Personal Information Breach Announced by Desjardins in 2019, December 2021, at https://www.newswire.ca/news-releases/settlement-of-class-actions-related-to-the-personal-information-breach-announced-by-desjardins-in-2019-844138744.html
[55] Help Net Security, Financial services need to prioritize API security to protect their customers, November 2021, at https://www.helpnetsecurity.com/2021/11/01/financial-services-api-security/
[56] Australian Cyber Security Centre, ACSC Aware of DDoS Threats Being Made Against Australian Organisations, February 2020, at https://www.cyber.gov.au/threats/acsc-aware-ddos-threats-being-made-against-australian-organisations
[57] John Anthony and Tom Pullar-Strecker, NZX back online as Government assists in helping it address cyberattacks, August 2020, at https://www.stuff.co.nz/business/industries/122593041/nzx-back-online-as-government-assists-in-helping-it-address-cyberattacks
[58] Catalin Cimpanu, DDoS extortionists target NZX, Moneygram, Braintree, and other financial services, August 2020, at https://www.zdnet.com/article/ddos-extortionists-target-nzx-moneygram-braintree-and-other-financial-services/
[59] Sygnia, Elephant Beetle: Uncovering an Organized Financial-Theft Operation, January 2022, at https://blog.sygnia.co/elephant-beetle-an-organized-financial-theft-operation?hsLang=en
[60] Karen Hoffman, The high cost of mishandling data breaches, security reporting for financial services, January 2022, at https://www.scmagazine.com/analysis/breach/the-high-cost-of-mishandling-data-breaches-security-reporting-for-financial-services
[61] National Credit Union Administration, Catastrophic and Incident Reporting, October 2021, at https://www.ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/catastrophic-and-incident-reporting
[62] National Credit Union Administration, NCUA's Information Security Examination and Cybersecurity Assessment Program, October 2021, at https://www.ncua.gov/regulation-supervision/regulatory-

compliance-resources/cybersecurity-resources/ncuas-information-security-examination-and-cybersecurity-assessment

[63] Federal Register, Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, November 2021, at https://www.fdic.gov/news/board-matters/2021/2021-11-17-notational-fr.pdf and David Heun, Report data breaches within 36 hours? Banks are OK with that, November 2021, at https://www.americanbanker.com/news/report-data-breaches-within-36-hours-banks-are-ok-with-that

[64] Bank of England, Prudential regulation, February 2022, at https://www.bankofengland.co.uk/prudential-regulation

[65] Bank of England, Letter from Nathanael Benjamin and Rebecca Jackson 'International banks active in the UK: 2022 priorities', January 2022, at https://www.bankofengland.co.uk/prudential-regulation/letter/2022/january/artis-2022-priorities

[66] Financial Conduct Authority, About us, February 2022, at https://www.fca.org.uk/about

[67] Norton Rose Fulbright, Cybersecurity: Not just an IT issue, but a regulatory one too, August 2020, at https://www.nortonrosefulbright.com/en/knowledge/publications/b8178be8/cybersecurity-not-just-an-it-issue-but-a-regulatory-one-too

[68] Financial Conduct Authority, Apache Log4j cyber vulnerability, December 2021, at https://www.fca.org.uk/news/statements/apache-log4j-cyber-vulnerability

[69] Gov.uk, Data protection, at https://www.gov.uk/data-protection

[70] ICO, Data security incident trends, October 2021, at https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[71] Australian Prudential Regulation Authority, Information security requirements for all APRA-regulated entities, June 2019, at https://www.apra.gov.au/information-security-requirements-for-all-apra-regulated-entities

[72] Australian Prudential Regulation Authority, APRA sets out policy and supervision priorities for 2020, January 2020, at https://www.apra.gov.au/news-and-publications/apra-sets-out-policy-and-supervision-priorities-for-2020

[73] Londiwe Buthelezi, Standard Bank on delay in telling public about data breach: 'We complied with the law', December 2021, at https://www.news24.com/fin24/Companies/Banks/standard-bank-on-delay-in-telling-public-about-data-breach-we-complied-with-the-law-20211213

[74] Osterman Research, Achieving the Operational Resilience Agenda in Financial Services, November 2021, at https://ostermanresearch.com/2021/11/01/whitepaper-operational-resilience-nutanix/

[75] Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation, Sound Practices to Strengthen Operational Resilience, October 2020, at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf

[76] Kaitlan Collins, Phil Mattingly, Kevin Liptak, and Donald Judd, White House and EU nations announce expulsion of 'selected Russian banks' from SWIFT, February 2022, at https://edition.cnn.com/2022/02/26/politics/biden-ukraine-russia-swift/index.html

[77] BBC, Credit Suisse denies wrongdoing after big banking data leak, February 2022, at https://www.bbc.com/news/business-60456196

[78] Reserve Bank of Australia, Financial Stability Review - October 2021, October 2021, at https://www.rba.gov.au/publications/fsr/2021/oct/pdf/financial-stability-review-2021-10.pdf

[79] Russell Hotten, Ukraine conflict: What is Swift and why is banning Russia so significant?, February 2022, at https://www.bbc.com/news/business-60521822

[80] CISA, Shields Up, February 2022, at https://www.cisa.gov/shields-up

[81] Reuters, ECB tells banks to step up defences against hacks, February 2022, at https://www.reuters.com/business/finance/ecb-says-six-banks-come-up-short-its-capital-demands-2022-02-10/

[82] Carolyn Cohn, Insurers run from ransomware cover as losses mount, November 2021, at https://www.itnews.com.au/news/insurers-run-from-ransomware-cover-as-losses-mount-572963

[83] Aon, 2021 Cyber Security Risk Report, January 2021, at https://www.aon.com/2021-cyber-security-risk-report/

[84] FFIEC, Authentication and Access to Financial Institution Services and Systems, August 2021, at https://www.ffiec.gov/press/pdf/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf

[85] Robert Lemos, Enterprises Remain Riddled With Overprivileged Users -- and Attackers Know It, April 2021, at https://www.darkreading.com/vulnerabilities---threats/insider-threats/enterprises-remain-riddled-with-overprivileged-users----and-attackers-know-it/d/d-id/1340576

[86] David Heun, Weary of passwords, mobile banking users warm to biometrics, August 2021, at https://www.americanbanker.com/news/weary-of-passwords-mobile-banking-users-warm-to-biometrics

[87] Brian Krebs, NY Charges First American Financial for Massive Data Leak, July 2020, at https://krebsonsecurity.com/2020/07/ny-charges-first-american-financial-for-massive-data-leak/

[88] Chris Keall, Reserve Bank hit with compliance notice from Privacy Commissioner over data breach, September 2021, at https://www.nzherald.co.nz/business/reserve-bank-hit-with-compliance-notice-from-privacy-commissioner-over-data-breach/GSMMPOPR2SCWIIYFFPR36OGAEU/