Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **April 2020**
Sponsored by **VMware Carbon Black**

Cyber Security in Financial Services

Executive Summary

The financial services industry is under cyber attack. It is subjected to the highest rates of attack of any vertical market, the source of one-third of all data breaches, and it is vulnerable due to both negligence and carelessness of employees and other insiders. Compounding the problem is the sudden "work-from-home" phenomenon that began in March 2020 and that has forced many financial advisors and others into working from home with security solutions that are not always as robust as when they are in the office.

Cyber criminals are attracted to financial services' firms storehouses of confidential data, along with the potential for quick payoffs through fraudulent money transfers after credential theft or unauthorized system access. And, cyber attacks are getting worse: the Financial Industry Regulatory Authority (FINRA) noted in 2019 that "cybersecurity attacks continue to increase in both number and level of sophistication."

This white paper provides best practices guidance on defending against and recovering from various types of cyber-attacks and threats, in order to strengthen preparedness and improve resilience across the industry.

KEY TAKEAWAYS

- The financial services industry and its various sectors are essential to a well-functioning society. Weaknesses in the financial system weakens businesses and consumers.

- The financial services industry is consistently ranked as the most attacked vertical industry, being subjected to an ongoing barrage of cyber-attacks year-on-year. The industry is attractive for cyber criminals due to the potential for access to sensitive financial data, along with the possibility of triggering covert malicious financial transactions.

- Key threats against the industry include ransomware, ransomware plus data exfiltration, phishing and spear phishing, supply chain compromise, and insecure cloud storage services. Many threats are directed against the industry by cyber criminals, and several are the result of negligence by employees and other insiders.

- We expect ongoing threats from data breaches and ransomware, with phishing a key vector of attack. Ransomware cyber criminals are stepping up their efforts to force victims to pay the ransom by coupling a ransomware attack with a data breach.

- The COVID-19 crisis has forced tens of millions of employees to suddenly work from home, creating a number of security, authentication and other problems. Because this will become the new norm for many of these employees over the long term, and because remote workers are increasingly becoming targets of bad actors, robust security and secure multi-factor authentication (MFA) will be essential.

- Financial services organizations need to strengthen security defenses against ransomware (e.g., through ransomware-resistant backups), use stronger identity and authentication approaches (e.g., MFA using hardware tokens), and stopping phishing attacks across multiple channels.

- Technology solutions alone will not solve the cyber security challenges facing the industry. Investments in people (e.g., security awareness training, retaining cyber security talent) and processes (e.g., enterprise risk assessment, breach detection and notification) are also essential.

> ***The financial services industry is under cyber attack.***

ABOUT THIS WHITE PAPER

This white paper was sponsored by VMware Carbon Black; information about the company is provided at the end of this paper.

Why Financial Services?

Financial services firms are the perfect target for cyber criminals. The sector presents a constellation of reasons why it is under sustained attack, such as:

- **High-value data**
  Financial services organizations collect, store and process enormous quantities of confidential and sensitive data that is valuable to cyber criminals. Identity data can be used for identity theft and phishing attacks, financial records leveraged to identify high-payoff victims, and transaction data analyzed for patterns to hide malicious payment requests and inform spear-phishing campaigns.

- **Direct access to money**
  Financial firms are the conduit for gaining access to the financial assets of customers. Forged payment requests can be extremely lucrative, such as the $1 million fraudulent transfer out of a customer's account controlled by Phillip Capital, Inc. after a phishing incident.

- **Long-term data retention requirements**
  Organizations are required to retain high-value financial and customer data for many years and also to have ready access to it. Long-term retention and access requirements increase the vulnerability of unauthorized access, encryption or destruction by ransomware, and data exfiltration.

- **Complex systems landscape**
  Financial services organizations collect, transact, and transfer money through a byzantine web of interconnected financial systems, supply chain members, and uncontrollable mobile devices used by consumers. Many have lax cyber security standards for third parties involved in developing financial software and systems.

- **Strict regulatory environment**
  Financial services firms are subject to an alphabet soup of strict regulations, including GDPR (data protection for people in Europe), anti-money laundering (evidence of non-malicious usage of the monetary system), PCI DSS (security for credit card details), the FINRA (capture and storage of communications), Gramm-Leach Bliley Act (protections for customer information), and Security and Exchange Commission (SEC) 17a-4 (retention of communications), among many others. Getting it wrong results in costly financial penalties, and it's possible that financial organizations making surreptitious usage of customer data in violation of these regulations could be outed by a data breach.

- **Legacy technology**
  Widespread usage of legacy technology across the sector, including Windows 7 embedded in networks of ATM devices, opens the door for cyber criminals to exploit known and unpatched code vulnerabilities.

- **Market disruptions forcing fast responses**
  Digital banks and fintech start-ups are attempting to disrupt the sector, which creates tremendous pressure for established providers to fight for continued relevancy and to retain current customers. Cyber security can easily become an afterthought in new product and service innovation efforts.

> ***Financial services firms are the perfect target for cyber criminals.***

Threats in Financial Services

The financial services industry has consistently rated as being under high levels of cyber-attack. For example:

- An IBM X-Force study pegged it as the most attacked industry for the four years from 2016 to 2019, and noted that is the target of just under 20 percent of total cyber security incidents and attacks.
- A Forbes study found that more than one-third of all data breaches were in the financial services industry, and the Financial Conduct Authority in the United Kingdom noted that data breaches increased 500 percent from 2017 to 2018.
- Also in the UK, Vanson Bourne in late 2019 noted that 70 percent of financial services organizations had suffered a security incident over the past 12 months, with employees not following security protocols or data protection policies as the leading cause of these incidents.
- The Boston Consulting Group reported that financial services firms are 300 times as likely to be targeted by a cyber-attack as other industries.

Cyber-attacks against financial services firms are many and varied, as discussed below:

UNSECURED REMOTE WORKER ACCESS

Employees who work from home often do so without appropriate authentication protocols in place. The problem has been magnified dramatically as a result of the COVID-19 crisis as millions of previously in-office employees are now working from home. An April 2020 Osterman Research survey found that as a result of the COVID-19 crisis, 57 percent of organizations with a suddenly at-home workforce have implemented additional security measures, such as MFA, but 43 percent have not done so. This has created an enormous problem for organizations attempting to manage access to critical data and other resources, and it opens numerous opportunities for bad actors to exploit these security holes.

> ***…financial services firms are 300 times as likely to be targeted by a cyber-attack as other industries.***

RANSOM DENIAL-OF-SERVICE

Cyber-attackers threaten to unleash a sustained denial-of-service or distributed denial-of-service attack against a financial institution's online assets unless a ransom is paid in advance. Banks and financial organizations in Singapore, South Africa and Scandinavian countries were threatened in October 2019, and several organizations in the banking and financial sector in Australia were likewise threatened in February 2020. Often the threat turns out to be empty and not carried through, although some attack activity has been observed.

RANSOMWARE

Threat actors encrypt the victim's data and demand a ransom payment for the recovery keys, after using a malicious email attachment or exploiting software vulnerabilities to gain control of target systems. Travelex, for example, was subject to a ransomware attack in late December 2019, and took its website and other internal systems offline in order to prevent spread and minimize overall damage. The threat actors against Travelex also claimed to have exfiltrated five gigabytes of customer data over a six-month period before unleashing the ransomware attack. A recent example is Jamaica National Bank, which was disrupted by ransomware in mid-March 2020 and had some customer data breached. Few organizations are highly confident of their ability to withstand a ransomware attack, and most firms pay the ransom to get back to business as quickly as possible.

MULTI-FACTOR AUTHENTICATION-RESISTANT PHISHING

Bad actors have designed phishing attacks that can circumvent certain types of MFA protections. Some phishing campaigns will link to fake-but-realistic destination login sites and are able to bypass both SMS-based and authenticator-app-based second factor approaches. This has enabled the successful credential compromise of numerous accounts.

PHISHING, SPEARPHISHING AND BEC

Phishing, spear phishing and business email compromise (BEC) use social engineering lures to trick people into giving up their account credentials, installing malware or ransomware on their device, or paying a falsified but realistic invoice to the criminal's bank account. The financial services industry is targeted by more phishing attempts than other industries. Phishing can be a lucrative win for threat actors; for example, a single phishing email to Phillip Capital Inc. gave the cyber criminals the ability to transfer $1 million to their bank account in Hong Kong. As phishing, spear phishing and CEO fraud attempts become ever more difficult to identify, fewer firms are confident in their ability to thwart such attacks.

DATA BREACHES

From established banks to new entrant fintechs and cryptocurrency players, personal and financial data for customers is being breached. Details on more than 200,000 credit cards (including PIN and CVV numbers) were stolen from top banks in Singapore, Malaysia, the Philippines, Vietnam, Indonesia and Thailand in March 2020. In the same month, compromising the database at Trident Crypto Fund resulted in data on more than 250,000 customers being breached. And in Iran in late 2019, account details for the debit cards of about 20 percent of the population were available for unauthorized access. Financial services firms that are breached face customer backlash, regulatory fines, and financial and reputational consequences.

SUPPLY CHAIN COMPROMISE AND DATA BREACH

Financial institutions rely on a variety of third-party systems and service providers to conduct their own business, and these supply chain partners create cyber security risks of compromise and breach. A marketing service provider for Nedbank in South Africa was compromised in February 2020, resulting in the personal information on 1.7 million Nedbank customers being breached. TD Bank in 2019 had internal data breached when Attunity – an IT firm in Israel – failed to correctly secure its cloud storage accounts at Amazon. In Brazil, 250 gigabytes of sensitive identity data held by a financial services provider on behalf of various local banks was found on an unprotected server. Similarly, customer mortgage information provided to the Idaho Central Credit Union was breached when a third-party system was compromised. Financial institutions have shared data believing it to be stored securely by supply chain partners, but are left facing the consequences when customer data is breached in systems outside of their direct control.

Gaining access to valid login credentials for systems provides an easy way for cyber criminals to work under the radar.

COMPROMISED ACCOUNT CREDENTIALS

Gaining access to valid login credentials for systems provides an easy way for cyber criminals to work under the radar. Hacking attempts, keystroke loggers, and other malware installed on a victim's device will often trip security safeguards more easily than logging in with stolen credentials gained through a phishing attack or purchased from other criminals who have done so.

INAPPROPRIATE SHARING IN OFFICE 365

Microsoft's success with driving the adoption of Office 365 has been well-documented over the past decade; millions of new users now get Office 365 credentials every month. Office 365 makes it simple to work collaboratively with both internal colleagues and external partners, sharing files, folders and even entire workspaces. Two threats, however, have increased in intensity. The first is the atrophy of access privileges where the access rules initially set up on a shared workspace make less sense over time. The net consequence is that the wrong people gain access to data and documents due to organizational changes and employee turnover that is not reflected in the access rules for Office 365 constructs. The second is the greater ease of data exfiltration by employees, particularly when they move to a new employer and take corporate data with them.

INSECURE CLOUD STORAGE SERVICES

As financial services organizations race to the cloud, security considerations are too often being overlooked. Poor security includes the absence of access privileges leaving storage accounts open for public access, code vulnerabilities in cloud services that can be exploited for unauthorized access, and misconfigurations in security settings. The breach of more than 100 million customer records at Capital One in 2019 was due to a misconfigured web application firewall on a storage account at Amazon Web Services (AWS), which was exploited by an ex-employee of AWS who had cloud engineering skills. The data breach at the European Central Bank in 2019 was the result of malware being installed by hackers on an externally hosted server. Two research reports in the past year have noted an expected increase at least 50 percent in code vulnerabilities affecting cloud services, meaning the very foundation of at-a-service offerings are vulnerable in ways that financial services organizations and other customers cannot control, but are deeply affected by.

CLOUD BACKUPS COMPROMISED, EXFILTRATED AND DELETED

One of the most effective safeguards against a ransomware attack is cloud backup services because they are isolated from production systems and enable restoration without having to pay the ransom. Cloud backups, however, are now under attack. Cyber criminals are using an initial account compromise – often achieved through a phishing attack – to move laterally across the network to gain admin account access for both network and cloud resources. Once they have access to cloud backups, they have access to the sensitive and confidential data stored in those systems, and the immaturity of breach sensing in cloud backups provides an open window to exfiltrate data and even delete the backups.

UNSECURED AND INAPPROPRIATELY SECURE BANKING APPLICATIONS

Analysis by ImmuniWeb in 2019 on the security of banking applications at the world's 100 largest banks painted a worrying picture. Of the e-banking applications tested, 83 percent failed compliance tests under the European Union's General Data Protection Regulation (GDPR), 48 percent failed compliance tests for Payment Card Industry Security Standards Council (PCI DSS), and 25 percent were not protected by a web application firewall. For mobile banking applications, 92 percent contained at least one medium-risk security vulnerability. Another ticking time bomb is the growing number of third-party financial apps that rely on the user's username and password to gain access to their financial accounts, instead of using more secure API-based approaches.

THREAT ACTORS MASQUERADING AS FINANCIAL SERVICES ORGANIZATIONS

Domain cybersquatting is a threat for financial services organizations, where cyber criminals create lookalike domains to trick consumers into giving up their account credentials and other personal details. ImmuniWeb discovered more than 6,500 related cybersquatting domains in their 2019 analysis of the security of cyber offerings by the world's 100 leading banks; these were being used for illicit, fraudulent and other deceptive purposes. In February 2020, the brand names of both American Express and Chase were used in fake fraud protection emails to trick users into opening fake sites and entering personal financial details and account credentials.

COMPLEXITY AND DATA PROLIFERATION

Sensitive and confidential data is authoritatively and securely stored in core banking applications and sanctioned storage locations, but is also duplicated to other locations without the same level of cyber security protections. Backup services, test environments, development systems, and data protection systems frequently contain copies of sensitive data. The proliferation of this data across a complex of systems creates new channels for compromise. Monzo, a new style digital bank in the United

> ***The people who work inside financial institutions and have access to financial systems are a frequent source of cyber security threats and incidents.***

Kingdom, discovered that some customers' PIN numbers were being stored in log files external to its core systems, and although these log files were encrypted, engineers at Monzo could nonetheless gain access. While no evidence of misuse was found, the duplicated data resulted in a data breach notification being sent to 20 percent of its customers.

INSIDER ATTACKS AND HUMAN ERROR

The people who work inside financial institutions and have access to financial systems are a frequent source of cyber security threats and incidents. In the United Kingdom, Gallagher (an insurance company) recently said that human error causes 60 percent of all data breaches and cyber-attacks. At Wells Fargo in 2019, a bank teller used his access privileges to steal money from several customer accounts. At the National Australia Bank in mid-2019, an employee erroneously uploaded data on 13,000 customers to external companies. At Desjardins in Canada in mid-2019, an employee used internal data illegally and without authorization, compromising the confidential and sensitive personal and financial data on more than six million accounts. Fifth Third Bank in the United States faced a similar breach of customer information by several employees in 2018, including having the stolen data given to an external party without authorization. Use of unauthorized mobile apps, cloud services, and personal email accounts for business purposes is also common. In financial services call centers where agents have access to customer account data and financial information, if agents are using mobile phone-based MFA like OTP, then they can use their phones to take photos of customer account details and other information.

WEAPONIZED CLOUD SERVICES

Cyber criminals are becoming customers of public cloud services, using them to host web attacks against targets. Imperva found that web attacks originating from public cloud services grew by 16 percent from November to December 2019, with almost all of the attacks coming from Amazon Web Services.

Financial services organizations have seen sustained cyber-attacks in recent years.

CUSTOMERS USING COMPROMISED MOBILE DEVICES

Customers of the financial system use laptops, tablets and mobile phones to interact with e-banking and mobile banking applications, but financial institutions have little ability to control the security hardiness of these endpoints. In terms of ad fraud, Upstream reported that it had to block 93 percent of transactions as fraudulent in 2019, mostly due to ad fraud malware installed on the devices, with Android devices the key vector of compromise. Cyber criminals also use SIM swapping techniques to steal control of a device in order to circumvent one-time codes used for MFA, a process that can be accomplished within one to two hours and before the victim has time to react.

COMPROMISED THIRD-PARTY ENDPOINTS

In addition to the threats posed by mobile devices owned by customers, financial institutions are also dependent on millions of third-party endpoints for initiating and securing financial transactions, such as point-of-sale (PoS) devices, ATM terminals and gas pumps. Cyber criminals have used malware on PoS devices to steal transaction details, and card skimmers appear frequently on ATM terminals and in gas stations to steal debit card details and PIN numbers.

STATE ATTACKS TO STOKE ECONOMIC INSTABILITY

Given the key role played by financial institutions in promoting economic stability within a country or region, foreign governments have frequently targeted such institutions to stoke instability across the population and undermine economic and political confidence. The ongoing cyberwar between Iran, the United States and Israel is but one such example.

REGULATORS ARE PENALIZING FOR CYBER SECURITY INFRACTIONS

It's important to note that financial services regulators are highly focused on cyber security and penalizing firms whose security posture is inadequate. For example, in 2018 LPL Financial was censured and fined $2.75 million because it experienced various security incidents and failed to report them to FINRA. In January 2017, FINRA fined 12 firms a combined $14.4 million for cyber security-related failures that were the result of inadequate recordkeeping. In 2018, the Financial Conduct Authority fined Tesco Personal Finance plc £16.4 million following a security incident that impacted 8,261 personal accounts and exposed flaws in the firm's debit card business processes.

Expectations of Changing Threat Dynamics

Financial services organizations have seen sustained cyber-attacks in recent years. In looking at the threat trends in cyber security, we expect to see several threat dynamics against financial services organizations over the next 24 months:

- **Ransomware with data exfiltration**
  Landing a successful ransomware attack doesn't benefit the cyber-attackers if the victim is sufficiently prepared and able to recover without paying the ransom. Attackers have in recent months introduced additional "motivation" for victims to pay, such as the threat to publish data that was exfiltrated before the systems were ransomed (hence driving publicity around a data breach), and the threat of automated notifications to stock markets after a ransomware attack in an attempt to manipulate market valuations. Threats of such publicity reduces the ability for a ransomed firm to ignore the attackers' ransom demands. We expect these added "motivators" to remain in play, and new ones to be added.

- **People under attack (and negligent)**
  People remain the weakest link in the security chain, and we expect to see sustained attacks using phishing, spear-phishing and other social engineering means to bypass security safeguards. On the other side, insider threats from careless and negligent use, such as storing confidential and sensitive data in unauthorized cloud services, are expected to continue.

- **Attacks against cloud services**
  Customers migrating data to cloud services create an intense concentration of confidential and sensitive data, along with globally accessible user accounts. For cyber criminals, compromising cloud services through credential theft gives direct access to the customer's data, along with high-reputation messaging capabilities for subsequent phishing and spear-phishing attacks against the customer's supply chain. Exploiting code vulnerabilities in as-a-service offerings enables bypassing the use of stolen credentials altogether.

- **Cyber security professionals overwhelmed**
  The majority of cyber security professionals already feel overworked. Unless they have access to greater threat intelligence and more automated tools that reduce the requirement of manual efforts, new attacks will be successful more often than they are thwarted. Cyber criminals will be able to use the "fog of war" against cyber security professionals.

Modern authentication approaches that rely on biometrics and use strong multi-factor authentication mechanisms are essential.

Solutions to Consider for Improving Cyber Security in Financial Services

Every financial services organization needs its own assessment of cyber security threats and risks; we have outlined common threats facing the industry earlier in this white paper, but each firm needs to conduct and regularly update its own analysis. We strongly recommend the adoption of the following solutions for financial services organizations facing related cyber security risks, threats and incidents:

RANSOMWARE-RESISTANT BACKUPS

The best way of recovering from a ransomware attack without paying the ransom is to have ransomware-resistant backups available. Offsite backups held by a third-party, using an immutable storage option to decrease the likelihood of backups being deleted without recourse, is currently the best approach. Appropriate separation and monitoring of access privileges between the organizational network and the offsite backup service provides early warning of potentially compromising actions.

STRENGTHEN IDENTITY AND AUTHENTICATION

Gaining access to systems needs to be strengthened, with the current reliance on usernames and passwords dumped in favor of stronger approaches. Passwords are too easily guessed, brute-forced, breached, compromised, or even copied from a Post-It Note attached to the user’s laptop. Modern authentication approaches that rely on biometrics and use strong MFA mechanisms are essential. Any time a firm faces a breach, strengthening identity and authentication is quickly undertaken, and given the high percentage of overall breaches happening within the financial services industry, waiting for further breaches reflects poor judgment. On the MFA front, both SMS codes and authenticator app codes have been compromised in recent years – for example, through SIM swapping for SMS codes and the Cerberus Android banking trojan. The most secure approach currently available for MFA relies on hardware tokens following the FIDO2 standard.

STRONG MULTI-FACTOR AUTHENTICATION

If access credentials can be compromised simply by asking for them through a phishing campaign, an attacker can take whatever data they want, when they want it, or use modular malware to extend from an initial foothold to compromising additional systems and planting malware for a subsequent and more devastating attack. Approaches for MFA are available on a good-better-best continuum, with good (SMS code, email notification) and better (Authenticator app) approaches still being vulnerable to carefully designed phishing attacks. At present, the best approach, which ideally would be provisioned for all employees who have access to sensitive data, is to use modern hardware security keys based on FIDO2/WebAuthn that use public-key cryptography. These also provide an additional promise of secure passwordless logins – the “holy grail” for authentication. Some security keys provide multi-protocol support so that organizations can easily bridge between legacy systems and those supporting modern authentication protocols. While any approach to MFA is better than doing nothing, continuing with approaches that have already been compromised and expecting a different outcome is not advised.

Phishing and spear phishing are the most common ways used by cyber criminals to trick employees.

ANTI-PHISHING PROTECTIONS

Phishing and spear phishing are the most common ways used by cyber criminals to trick employees into giving away their credentials, installing malware, or letting ransomware creep onto their device. Phishing protections definitely need to protect email accounts, but more broadly, also messages received through social media channels and messaging apps. Advanced phishing protections should highlight lookalike and soundalike domains intended to slip past an employee’s casual glance, provide visual warnings of abnormal email addressing patterns on mobile devices (where email addresses are often hidden given the small screen real estate available), and even use language pattern analysis to detect falsified messages due to abnormal sentence construction for the supposed sender. While phishing messages are not solely sent by email, failing to have strong email authentication in place is unwise.

THREAT INTELLIGENCE

Threat intelligence services aggregate data points on cyber security threats and incidents across a broad network of customers, using analytics to identify trends and assess growing risk factors. For cyber security professionals who only have visibility into security trends within their own organization, it offers deep insights on how to ward off emerging attacks and strengthen defenses in light of forecasted trends. Threat intelligence offers expert views on actual threat levels, for example, whether a ransomware denial-of-service threat is real (because the cyber criminals behind the threat have actual capability to carry out the threat) or only a scare tactic to fool victims into paying the ransom.

SECURITY AUTOMATION AND PLAYBOOKS

Automated responses that contain, remediate and sanitize identified threats frees up cyber security professionals to address the more challenging security threats facing the firm. Alerts, notifications and escalation pathways have their place, but there aren't enough professionals available to manually remediate every security threat. Solutions that offer automation capabilities using the best available threat intelligence to complement the human element are essential.

VULNERABILITY SCANNING AND AUTOMATED PATCHING

Vulnerabilities in web and mobile banking applications, Microsoft Office, and Windows Server - among other applications used within the financial services sector - are exploited by cyber criminals, usually on a faster cadence than most firms are able to deploy patches using manual processes. Proactive scanning for vulnerabilities provides early warning of the size and scale of the enlarged attack surface in light of vulnerability notifications by the software vendor. Automated patching enables high priority issues to be shut down as early as possible. Some advanced vulnerability and patching solutions offer virtual patching before the vendor has released an actual patch, where identified vulnerabilities gain extra shielding from cyber-attack. Virtual patching is highly relevant for embedded devices in the industry that are based on older operating systems, such as Windows 7.

> ***Of significant benefit to employees in the financial services space…is the concept of a secure and portable "root of trust".***

SECURITY AWARENESS TRAINING

With such a high proportion of security incidents being directed at employees or caused by their negligence, security awareness training is essential. In combination with smart technology to prevent or identify cyber security risks, security awareness training helps to create another layer of defense against attacks. On the attack front, employees who can identify the red flags in phishing emails and other social engineering attempts can help prevent data breaches, ransomware attacks, and financial loss. For combatting carelessness and negligence, developing and sharing the policies that explain the reasons for security defenses reduces the incidence of making poor choices. Security awareness training often includes simulation capabilities to gauge readiness and pinpoint who needs additional training, additional automated safeguards, or other such interventions.

A SECURE ROOT OF TRUST

Of significant benefit to employees in the financial services space and across all industries, particularly those who are frequently out of the office, is the concept of a secure and portable "root of trust". Because employees lose devices and may want to use new ones periodically, a secure root of trust in the form of an internal (e.g., a fingerprint pad on a laptop) or external (e.g., a USB device) key enables more rapid recovery for the user when the device is lost or when they need to access a new platform.

CASB FOR AUTOMATED ADHERENCE TO SECURITY PROCESSES

As cloud services are increasingly used to store data responsive to data protection requirements, financial services organizations need to ensure appropriate security settings are maintained at all times. A Cloud Access Security Broker (CASB) offers the ability to automatically discover cloud resources being used by people within the firm and check for adherence to security protocols, e.g., for Amazon S3 storage buckets which frequently have inappropriate security settings. Out of tolerance settings can be automatically fixed or escalated for human review through an alerting process.

PEOPLE, PROCESS AND TECHNOLOGY

There are many technology solutions, as noted above, that offer heightened cyber security capabilities for financial services organizations. However, any technology solution has to work together with the people and process aspects. On the people side, alignment around a common vision and approach across IT security, the regulatory compliance team and the legal department is essential, along with senior leadership accountability for the cyber security strategy. Organizations also need to plan how they will hire and retain cyber security talent in an era of global shortages of people with the right mixture of technical and leadership cyber security skills.

PROCESSES AND PRACTICES FOR CYBER SECURITY

The third strand of the people, process and technology grouping are the business processes that specify how a given organization will translate technical capabilities into standard patterns for its people. Developing, testing and refining processes for security risk assessments, breach remediation, breach notification, vulnerability assessments and certification mechanisms for supply chain partners, physical security rights, and cyber intrusion drills, among others, are a core part of strengthening cyber security capabilities. Firms need processes for regularly reviewing user access rights to sensitive and confidential data, and a way of asking employees to certify that the information they have access to is suitable and appropriate for their job role. Developing processes across these areas helps to create security as a culture and as an integral element of developing new technology-enabled business systems.

Summary

Cyber criminals continue to focus on the financial services industry, with threats covering the gamut from ransomware, data breaches, fraudulent transactions, and compromised cloud storage services. Firms across the industry need to keep getting the basics right, while strengthening security defenses against account compromise, phishing attacks, ransomware attempts, and external and insider threats to confidential and sensitive data. The cyber security threats are not going away, and lack of action is unconscionable.

Sponsor of This White Paper

VMware Carbon Black is a leader in cloud-native endpoint protection dedicated to keeping the world safe from cyberattacks. The VMware Carbon Black Cloud consolidates endpoint protection and IT operations into an endpoint protection platform (EPP) that prevents advanced threats, provides actionable insight and enables businesses of all sizes to simplify operations. By analyzing billions of security events per day across the globe, VMware Carbon Black has key insights into attackers' behaviors, enabling customers to detect, respond to and stop emerging attacks. More than 6,000 global customers, including approximately one third of the Fortune 100, trust VMware Carbon Black to protect their organizations from cyberattacks. The company's partner ecosystem features more than 500 MSSPs, VARs, distributors and technology integrations, as well as many of the world's leading IR firms, who use VMware Carbon Black's technology in more than 500 breach investigations per year."

vmware® Carbon Black

www.carbonblack.com
@vmw_carbonblack
+1 866 257 4949
sales@carbonblack.com

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.