ASYMMETRICAL SECURITY THREATS OF BANKING IN THE CLOUD

March 2020



Sponsored by:

Booz | Allen | Hamilton

Independently produced by:

JAVELIN

TABLE OF CONTENTS

Foreword 3
Overview 3
Executive Summary 4
Key Findings 4
Recommendations 5
International Events Increase Threats of Cyberattacks 7
Public or Private, Banking Data is in the Cloud 9
Financial Institutions are Not Prepared to Secure the Cloud 12
Asymmetrical Threats Require Unconventional Defenses 14
Securing the Cloud and Digital Transformation 17
Appendix 18
Methodology 18
Endnotes 19

TABLE OF FIGURES

Figure 1. Type of Cloud Used, by Financial Institution 9
Figure 2. Applications Where Public and Private Cloud Services are Used 9
Figure 3. Types of Customer Information Stored in the Cloud 11
Figure 4. Location of Data When it is Breached 12
Figure 5. Reasons for Adopting or Not Adopting Cloud Services 12
Figure 6. Top Concerns About Use of Cloud Services, by Type of Cloud Used 13
Figure 7. Reasons for Adopting Cloud Services 14

FOREWORD

This original report, sponsored by Booz Allen Hamilton, explores how geopolitical tensions affect financial institutions' threat landscape, the state of cloud usage in financial services and what financial institutions need to do to prepare for a heightened threat scenario. For more information about Booz Allen Hamilton, contact their Cybersecurity Division.

This research report was independently produced by Javelin Strategy & Research. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

OVERVIEW

A vast majority of financial institutions (85%) in the United States use cloud processing services for various components of financial services. With the growing number of threats against cloud infrastructure, is your organization prepared for the multipronged attacks that can impede your business? Can you withstand ransomware, which holds your data hostage and prevents you from providing critical services? Do you have redundant infrastructure for distributed-denial-of-service (DDoS) attacks? Can you restore critical infrastructure if an intruder deletes information? Are you truly prepared for the asymmetrical attacks that make up today's cyber threats?

The threats to the financial-services ecosystem now extend beyond traditional hacking and include targeted attacks, including from insiders, designed to create systemic failures of financial institutions with the added bonus of potentially striking it rich. The very nature of asymmetrical warfare being full of insurgents who are at opposite ends of an ideology is how security professionals at financial institutions need to address the cybersecurity threats that are occurring. This report evaluates how financial services decision makers go about making—banking, payments, and cybersecurity decisions. It further explores current state concerns and how the market needs to shift to address a rapidly changing security environment.

EXECUTIVE SUMMARY

Key Findings

Cyber-threats can be state-sponsored, which means political and economic interests can drive action. As cyberwarfare between governments escalates and economic conditions worsen, the financial systems can be a lucrative target to attack the economy of a nation or a large source of funds for nation states.

Rising geopolitical tensions have implications for the cloud as companies move technologies to cloud infrastructures. Financial institutions that move infrastructure and data to cloud applications need to be aware of configuration risks that occur if the deployment of technology is not well thought through and data is not accurately mapped.

Cyber-threats in the cloud are not just about data confidentiality. Yes, there have been multiple data breaches in the cloud, with hundreds of millions of records exposed or stolen. But cybercriminals are also interested in leveraging the scalability of cloud computing for mining cryptocurrency through a technique called "cryptojacking," as well as hosting malware and command-and-control infrastructure. Both threats can negatively affect banks' bottom lines and reputations if criminals hijack banks' cloud resources.

Cloud usage is the norm for businesses in financial services. Approximately 85% of financial institutions use cloud services, with cost reduction being the primary driver for the migration. Cloud computing is leveraged for core banking purposes and, not surprisingly, storing payment and PII data, which makes cloud repositories attractive to cybercriminals.

Financial institutions are not prepared for the types of threats that are occurring globally. Wiper attacks, which delete all data, and ransomware attacks, which prevent the usage of systems, could cripple a financial institution, yet most do not have plans to prevent asymmetrical cyberwarfare.

Over 40% of financial institutions are concerned about user authentication into cloud applications. Having security policies that cover who has access and how access is authenticated needs to be a key priority of organizations to ensure access is revoked for people who no longer have business purposes to use the data or are external to organizations and departments that develop, deploy, or monitor the technology.

Poor configuration management and poor understanding of cloud environments are the biggest vulnerabilities that companies face. This is true for any cloud environment, but it is accentuated when companies are dealing with a multi-cloud environment—which is often the case to avoid vendor lock-in.

Automation is also for security teams. Automation is one of the defining features of cloud computing, one that enables faster, more efficient deployments. Security teams should embrace automation, whether to scan for misconfigured cloud components or for security alerts management.

Cloud computing enables digital transformation and innovation—if your cybersecurity practices keep up. Security on premise and in the cloud pose different challenges and thus require a different set of skills and operational processes. Get outside help if needed, but make sure to train and develop internal staff if you do.

Recommendations

Improve the tone at the top of the organization to make cybersecurity a corporate priority. Have a senior leader (CISO or CSO) dedicated to cybersecurity—someone who is high enough in the hierarchy to influence key business decisions. Be mindful of the conflict of interest that could arise from this security leader reporting to the CIO. What gets monitored gets managed.

Establish a formal strategy for understanding and accepting international risks. The perception of international actors of the United States government can place added risks onto financial services companies as a critical infrastructure to the national economy. Financial institutions need to accept that a coordinated attack by a nation-state could occur.

Formalize your cloud strategy and risk appetite. Create clear guidelines for business initiatives that want to leverage the cloud. Define your cybersecurity risk appetite, and determine where data will reside and the policies for securing the information.

Map your data to meet privacy and data security requirements. With the launch of the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), be mindful of where the data resides and why data retention is required. It is imperative that data not needed to perform business operations is not stored unnecessarily. Understanding what data is available, where it is stored, and retention policies helps enable adequate protection and compliance with privacy laws.

Ensure visibility of technology development and deployment. Minimize shadow IT risks by deploying a cloud access security broker (CASB) solution. If processing and database infrastructures are not visibly monitored, systems can be built without explicit approval under the guise of being test systems, creating emergency fixes, and patching system issues. Think about processes and procedures to apply when you detect shadow IT within your environment—because you will.

Make sure your security surveillance keeps up with your digital transformation. The Security Operation Center (SOC) team needs to be fully aware of cloud risks, which include malware, ransomware, and wiper attacks. Security Information and Event Management (SIEM) solutions, which receive log data from the cloud services you are using, are essential. Develop use cases using cloud logs and measure the performance (e.g., false positives, detection rates) of those use cases.

Update your security awareness program. It should cover cloud security for various types of employees, including end users, business leaders, software developers, and IT operations. Security awareness needs to be a

priority for every organization, monitoring on premise, in the cloud, and hybrid platforms.

Embrace data analytics across all technology models. Although automation and artificial intelligence can seem to be buzzwords, they are critical to real-time monitoring of the various threats that are directed at the financial-services industry. Security teams that are dealing with a deluge of data should embrace AI and engage with fraud colleagues, who have been leveraging analytics for decades.

Have a breach response plan ready—and use it. Adopt an "already breached" mindset and make sure you have a breach response plan ready. Test your response plan using tabletops exercises, involve cloud providers, and adjust your plan. If a breach does happen, use the plan. A company will often be judged on its breach response, even more so than on the fact that a breach occurred.

INTERNATIONAL EVENTS INCREASE THREATS OF CYBERATTACKS

Political unrest, a global pandemic, and a recession—these are all aspects of the pressure cooker that increases cyberattacks. The beginning of 2020 saw the death of an Iranian leader, which increased the threat of nation state cyberattacks. As geopolitical tensions rise, critical infrastructure—including the financial services sector—is under threat from many kinds of cyberattacks, including disruption, fraud, and data theft. The following serve as examples:

1. **Disruption.** One of the most famous pieces of malware in history, Stuxnet, is believed to be the work of American and Israeli cybersecurity services. Stuxnet's objective wasn't data theft, but rather to disrupt Iran's nuclear program through the destruction of centrifuges used in uranium enrichment.[1]
2. **Fraud.** The 2016 Bank of Bangladesh heist, in which cybercriminals attempted to steal almost $1 billion in fraudulent SWIFT transfers, is thought to be the work of cybercriminals working for North Korea.[2] This case, in which $81 million was eventually stolen, highlights the convergence of cybersecurity (the intrusion), fraud (sending wire transfers), and money laundering (laundering the proceeds of fraud through accounts and casinos in the Philippines).
3. **Data theft.** In February 2020, the U.S. Department of Justice announced charges against four members of China's People Liberation Army.[3] These members were allegedly behind the 2017 Equifax data breach.

A recent example of rising geopolitical tensions is the U.S.-Iran conflict. While this conflict isn't new—it started in 1979 after the Iranian Revolution—we've seen an increase in cyber activity related to it over the past decade. This threat was exacerbated by the death, in early 2020, of a top Iranian general. While overt military operations from Iran appeared to have slowed down after an initial outburst, cyber operations, and their well-known attribution problem, offer a great alternative to overt intervention, which is why we expect to see most of the response within the cyber sphere.

Analyzing tactics, techniques and procedures (TTPs) of state-sponsored groups can shed light on the motivations behind attacks while also providing useful insights to help improve defenses against them. It is believed that at least four of these groups have ties to Iran:[4] APT33, APT34, APT35 and APT39 (see Appendix for more details). While we focus on APT groups believed to have ties with Iran, many other APT groups are linked to other nation-states. Some of these APT groups, like FIN7, target the financial sector. State-sponsored groups are not exclusively targeting the financial-services sector. Government agencies with their own digital transformation initiatives, like the Pentagon's $10 Billion Joint Enterprise Defense Infrastructure (JEDI) project, will be targeted as well. The threat of nation states and, more generally, Advanced Persistent Threat (APT) against cloud providers and managed service providers, has led the Cybersecurity and

Infrastructure Agency (CISA) to release guidance to help companies improve their defenses.[5]

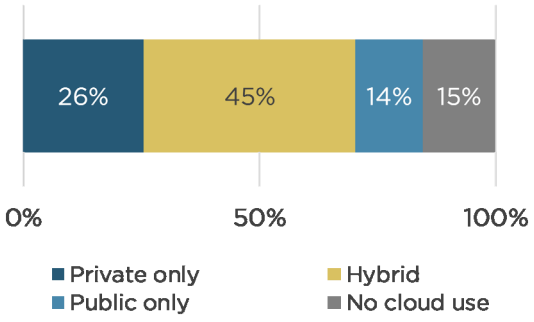
Nation state threats can also occur when economic conditions worsen. From international pandemics, which affect free trade and impede movement, to a global recession, which includes stock market slides and negative interest rates, cyber threats can be a lucrative way to raise necessary funds to support a struggling nation.

PUBLIC OR PRIVATE, BANKING DATA IS IN THE CLOUD

Nation states and cybercriminals in general, evolve as companies evolve. They will try to find the easiest way to commit their crimes and maximize the impact of their illicit activities—whether through monetization or disruption. At the same time, where data is being stored, shared and used has become a large question within financial services because of the sensitive nature of the information needed to process financial transactions and conduct commerce. However, executives would be better served if they also asked how the data is protected, not only where it is stored. The location of the storage, unless governed by law, isn't as critical as who has access, what data is retained, what is it used for, and how the data is protected. Cloud computing has changed the way companies develop, deploy, and maintain software and IT infrastructure. Due to its scalability, ease of use and accessible marketplaces, cloud computing is a pillar of any digital transformation initiative.

Cloud Usage is now the Norm for the Financial Services Sector

Figure 1. Type of Cloud Used, by Financial Institution

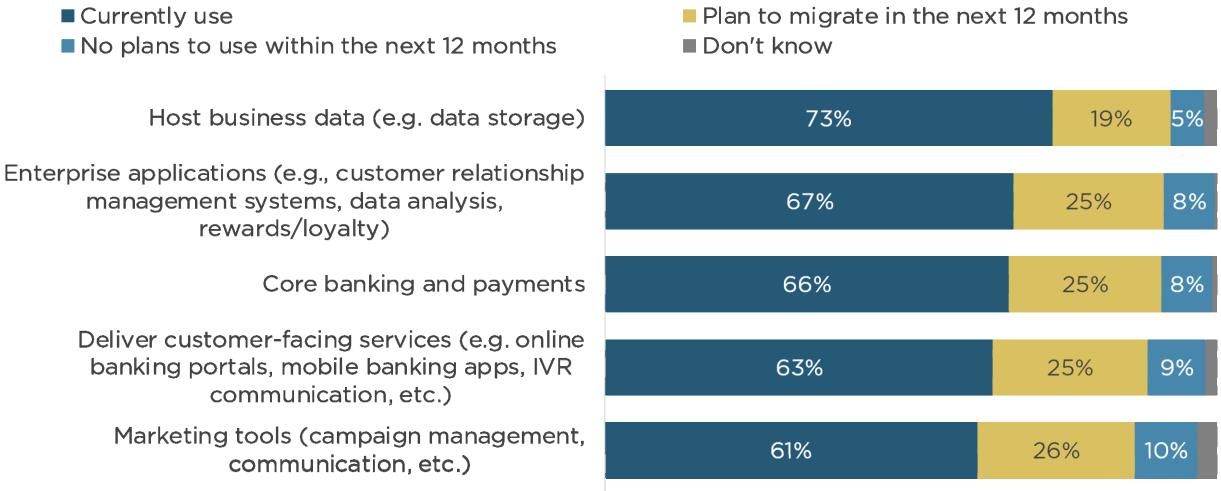


Source: Javelin Strategy & Research, 2020

Questions remain about how and for what purposes cloud services are used today. In 2019, 85% of financial services leverage some form of cloud infrastructure. While 15% of

Cloud is Leveraged for Mission-Critical Banking Services

Figure 2. Applications Where Public and Private Cloud Services are Used



Source: Javelin Strategy & Research, 2020

financial services do not leverage cloud computing today, we expect most of those financial institutions will leverage cloud computing in the next few years, as software-as-a-service (SaaS) becomes omnipresent.

An industry misconception is that mostly ancillary systems, those that are not critical to day-to-day business, are what leverage cloud infrastructure. Actually, 66% of core banking and payments are processed in cloud infrastructure, with an additional 25% planned to move in the next 12 months (Figure 2). Given the prevalence of SaaS solutions and increasing reliance on third parties to accelerate innovation, it is not surprising to see that the majority of organizations we surveyed are using the cloud. Cloud computing represents a unique opportunity for financial services companies to transform their businesses and delight their customers, as the cloud offers scalability, automation, and the ability to quickly deploy best-of-breed software solutions. These solutions can help financial institutions offer enhanced digital experiences to consumers, better manage risk and incorporate artificial intelligence into their decision-making. Thus, we expect that core banking systems and data will continue their migration to the cloud in the near future.

For financial services companies, hosting core banking applications in the cloud means they need to think about availability, which is a core tenet of security, alongside confidentiality and integrity. Because of its scalability, flexibility, and global presence, the cloud is often thought to be immune to availability issues. However, several incidents have shown otherwise:

- In 2017, AWS's Simple Storage Service (S3) suffered a widespread outage due to a human error.[6]
- In 2019, Google Cloud Platform suffered a major outage caused by a configuration issue.[7]
- In 2019, Microsoft Azure had a global outage due to a DNS migration.[8]

Another major threat to availability is ransomware. Ransomware has crippled many organizations, from cities to health care providers to financial services. And while ransomware is often thought to be an on premise problem, it will undoubtedly continue to move to the cloud as organizations continue their cloud transformation. Recent examples of ransomware attacks include:

- An attack on CyrusOne, a major data center provider, which affected six managed-service customers, including a brokerage firm.[9]
- An attack on Travelex, a foreign exchange company. Nearly a month after the attack, some of Travelex's services were still offline.[10]
- An attack on the city of Baltimore, expected to cost the city more than $18 million in recovery cost and lost revenue.[11]

Proof of concepts for ransomware attacks in the cloud have been developed, highlighting the fact that the threat is very real.[12] Financial services, especially the 85% already in the cloud, should make sure they have assessed their exposure to cloud ransomware – for example by looking at how they are securing their cloud accounts, how they are backing

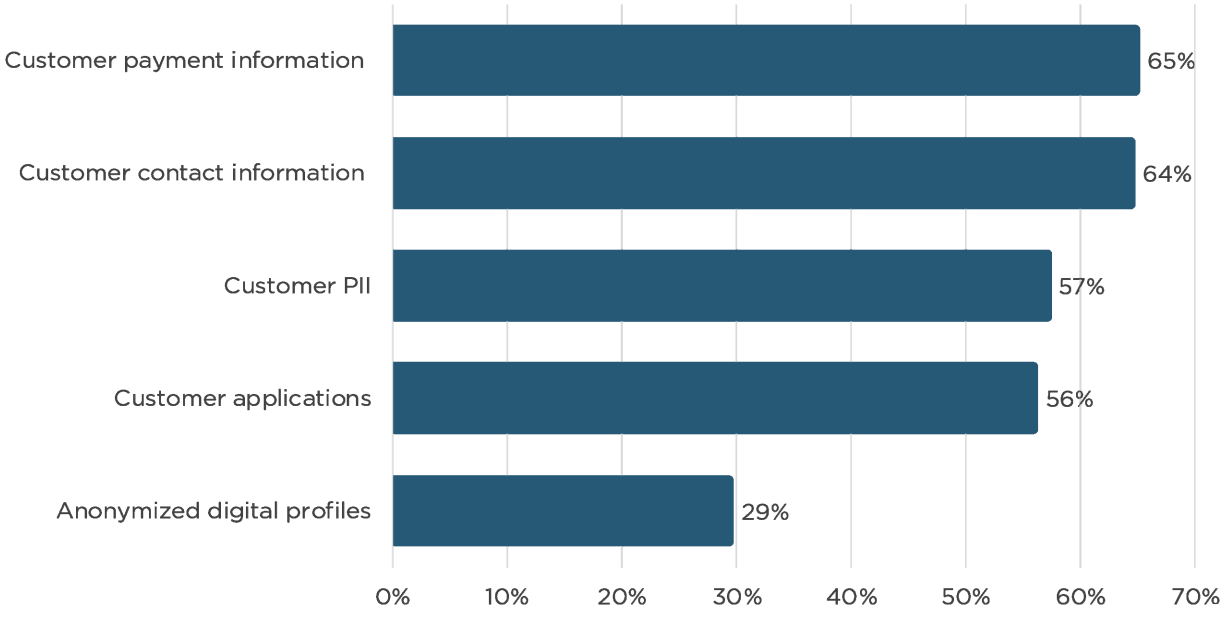
up data and how they are monitoring cloud activity. Companies not already in the cloud should take this opportunity to proactively include ransomware assessment as part of their cloud risk assessment before making the move.

As they lead their organizations in the cloud, banking, payments, and security professionals need to think about recovery and backup plans, including establishing thresholds for parameters like recovery point objective (RPO) and recovery time objective (RTO). Response plans need to be in place before migration to the cloud, including how to handle communication with customers and third parties during and after the outage. As in dealing with a data breach, effective and transparent communication during an outage can go a long way toward ensuring your customers continue to do business with you.

As mission-critical banking applications are used in the cloud, it's no surprise to see that sensitive data is stored and processed in the cloud. 65% of respondents say their company stores customer payment information in the cloud (Figure 3), 64% store customer contact information, and 57% store customer PII. In an EMV world, where static card data is less attractive than personal information, the presence of customer information in the cloud means that cybercriminals will try to steal it. Thus, companies need to be aware of the tool and tactics cybercriminals use—including phishing, malware and SIM swapping[13]—so defenses can be built.

Payment Data is Most Often Stored in the Cloud

Figure 3. Types of Customer Information Stored in the Cloud



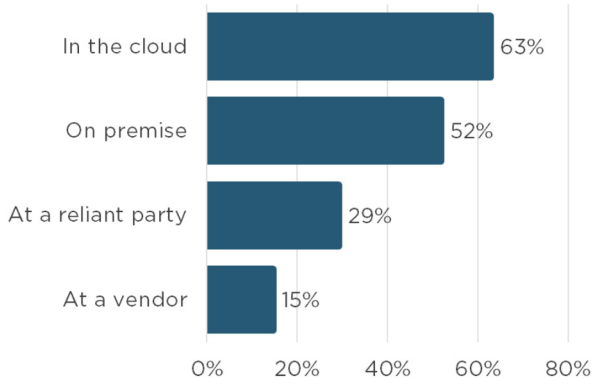
Source: Javelin Strategy & Research, 2020

FINANCIAL INSTITUTIONS ARE NOT PREPARED TO SECURE THE CLOUD

On premise infrastructure and cloud computing both have risks and vulnerabilities. Where valuable data is stored is where criminals will focus their attention. Cloud computing hosts critical banking systems, but financial institutions are not ready to secure it. Compromised infrastructure is 63% in the cloud and 52% on premise, which indicates the compromise of hybrid infrastructures (Figure 4). Among public cloud users, 64% think their organizations lack the tools and talents needed to effectively secure cloud services, 79% think they can more effectively secure on premise infrastructure and 59% have slowed cloud adoption for security concerns (Figure 5). Clearly, financial services professionals do not feel prepared to secure the cloud. Some of the cost reduction financial institutions are achieving by migrating to the cloud should be invested in security, covering people, process and technology.

Data is Breached Regardless of Where it is Stored

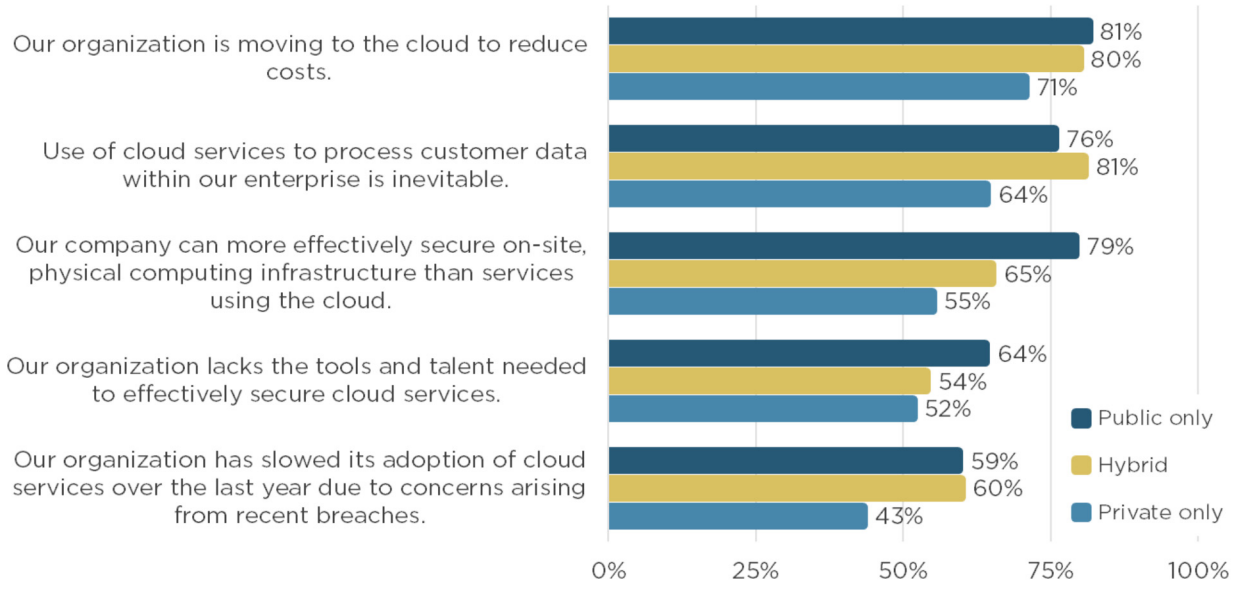
Figure 4. Location of Data When it is Breached



Source: Javelin Strategy & Research, 2020

Companies Incorrectly Believe On Premise Infrastructure is Safer than Cloud

Figure 5. Reasons for Adopting or Not Adopting Cloud Services



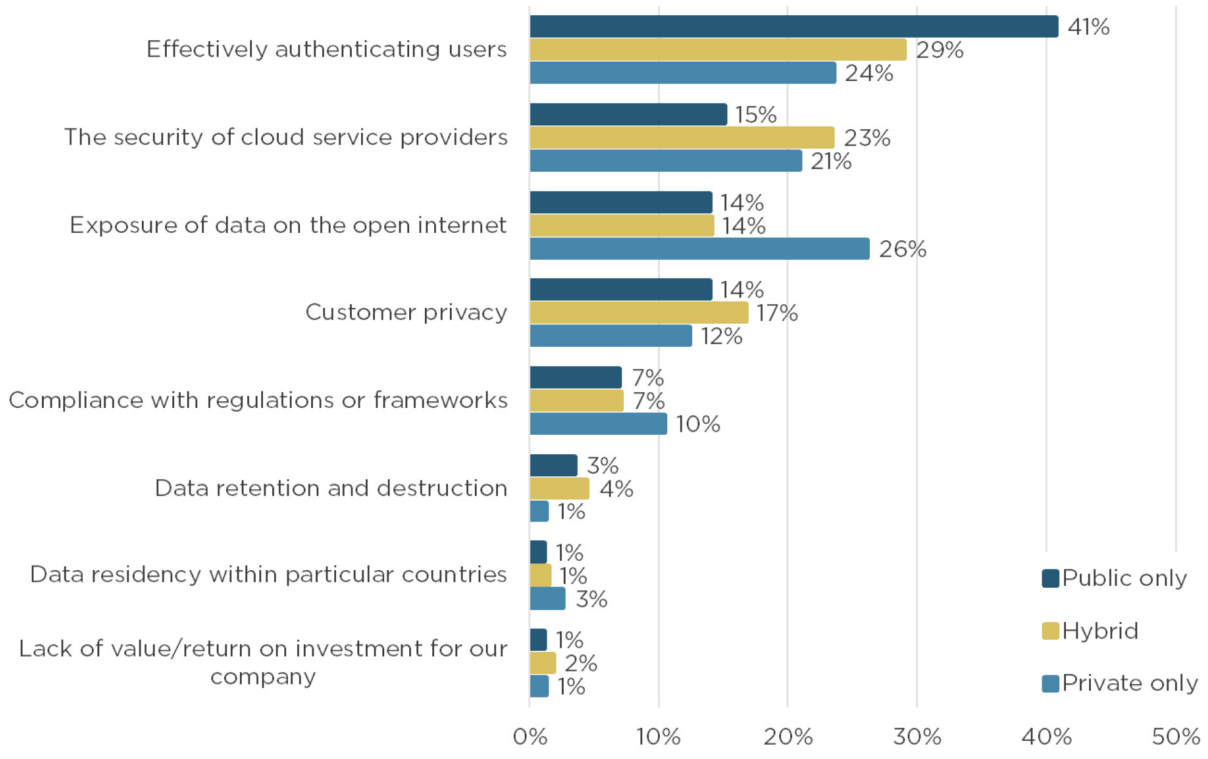
Source: Javelin Strategy & Research, 2020

As for top concerns regarding cloud services, the effective authentication of users remains a key issue, with 41% of public cloud users saying it is a top concern (Figure 6). One key solution to address authentication concerns should be to enable multifactor authentication, especially for highly privileged users and users with access to sensitive information, whether on the cloud or on premise.

As major security incidents have shown over the years, cybercriminals and nation states will find a way to infiltrate organizations to steal customer data, steal intellectual property or disrupt activities. Their arsenal includes malware, exploitation of known vulnerabilities left unpatched, 0-day vulnerabilities, phishing, fake phone calls, and, more recently, "deepfakes". Cybercriminals can also just take advantage of confidential data stored in the cloud and left available to anyone on the Internet, as seen in recent breaches. As we will detail in the next section, security professionals face an uphill battle because of the asymmetric nature of cyberwarfare.

User Authentication is the Top Concern in Leveraging Cloud Services

Figure 6. Top Concerns About Use of Cloud Services, by Type of Cloud Used



Source: Javelin Strategy & Research, 2020

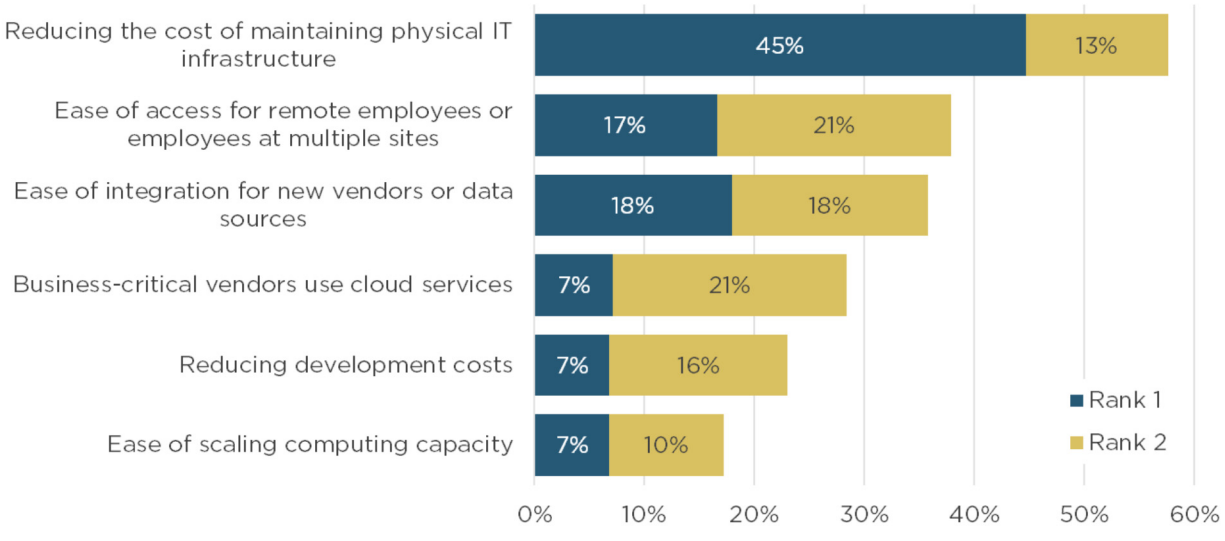
ASYMMETRICAL THREATS REQUIRE UNCONVENTIONAL DEFENSES

For years, cybersecurity was essentially a matter of protecting the enterprise perimeter from the Wild West, also known as the Internet. And for good reasons—years ago, the vast majority of information a company collected was stored within that perimeter, on the company's own IT infrastructure. Protecting the perimeter from outside attackers was essentially the security strategy that was adopted for years, until cloud services and "bring your own device" (BYOD) programs began to appear. Another legacy issue with the traditional perimeter-based security model is that, by trusting authenticated users blindly and by essentially focusing only on external threats, the door is left wide open for insiders to wreak havoc on a company's network.

Cloud infrastructure was adopted for several reasons, most notably the cost and time it took to set up new servers and deploy new software solutions (Figure 7). As innovation and digital transformation have become a matter of survival for many industries, being able to quickly deploy new software, add processing power, and add storage on demand is a hot commodity. Moreover, as organizations adopt artificial intelligence as a means to transform their business model, having a scalable IT infrastructure is a requirement, not a nice-to-have. The reason is that machine learning algorithms, what has been fueling artificial intelligence progress in the past decade, require data and lots of it. Training machine learning algorithms on large amounts of data requires a lot of computing power, on demand, which makes the cloud the perfect environment to reap the full benefits of AI.

Cost Reduction is the Primary Driver for Cloud Adoption

Figure 7. Reasons for Adopting Cloud Services



Source: Javelin Strategy & Research, 2020

As noted, cloud computing is a key element of digital transformation. However, recent events have shown that insiders and outsiders can exploit security issues in the cloud. Data breaches in the cloud are often the results of configuration errors and show that some of the main benefits of cloud computing—speed and automation—can also lead to security risks. When done on premise, change management used to be a longer, slower, manual process, involving multiple steps. Automation in the cloud changes that, and companies need to be prepared to address security risks that come with that speed and automation.

Data breaches are not the only threat to cloud computing. Criminals are always trying to find the easiest way to monetize their attacks. Selling data has been one way to monetize cyberattacks, but it is not the only one. At the height of Bitcoin's frenzy, criminals found another way to monetize cybercrime by using a cryptocurrency mining technique called "cryptojacking". Since mining cryptocurrency takes a lot of computing power, the elasticity and scalability of cloud computing provides a great environment for cryptominers to thrive in, especially malicious cryptominers using banks' cloud resources, for example. Aside from supporting criminal activities, cryptojacking has the potential to disrupt system availability, to increase the cost of cloud computing resources consumption and to negatively affect the reputation of banks using the cloud.

Cryptojacking does not pose a threat to data confidentiality. However, the risk of sanctions violations of having illegal transactions processed within the technology infrastructure could result in regulatory violations.

Cybercriminals also use the cloud to host malware, as well as command-and-control (C2) infrastructure. Through C2 infrastructure, cybercriminals control botnets and can launch DDoS attacks, send phishing and spam emails, distribute malware, and launch disinformation campaigns on social media. Another threat companies face comes from within—the threat of cloud shadow IT. Shadow IT, the use of software solutions without the information technology group's involvement, is not new. It was, and still is in some cases, an issue that occurs when regular users can develop and install software on their computers. Through sound identity and access management (IAM) practices, including the adoption of a least-privilege approach, the risk to confidentiality, integrity, and availability posed by traditional shadow IT can be reduced. But traditional shadow IT is not cloud shadow IT. With cloud services gaining traction, especially SaaS solutions, shadow IT is rising as a top cybersecurity risk. With SaaS, non-IT users can deploy full-fledged software solutions quickly, without the need for IT to get involved. This has potentially disastrous consequences—from a lack of knowledge of where PII data resides to the adoption of multiple software solutions that essentially address the same business requirements, and the recurring costs associated with them.

This rapid adoption of SaaS solutions, and the risks associated with them, led to the adoption of cloud access security brokers (CASB). CASB solutions enable companies to have much better visibility into which cloud providers and SaaS solutions are used. It is not uncommon for companies that have just installed a CASB solution to discover that many users have been using cloud-based shadow IT solutions. Thus, deploying a CASB solution is only a starting point, and companies should think about the procedures to apply when they detect access to unofficial cloud services. Security awareness programs should include the company's expectations with regard to cloud usage and the steps to follow to acquire and deploy new solutions.

Looking ahead, companies seeking to leverage the cloud securely should think about how cybercriminals will evolve. As security technologies and processes mature, cybercriminals will increasingly turn to social engineering, a form of attack already very popular and effective. Cybercriminals increasingly leverage information stolen in many data breaches to craft personalized emails, known as spear phishing, to potential victims, increasing the chance victims will click on malicious attachments or links. Spear phishing, although effective, is not the only tool in the social-engineering toolkit. In one documented case, a deepfake audio was used to trick a company into sending $243,000 to an account under the control of a fraudster.[14] As companies increasingly move to the cloud, we expect cybercriminals to step up their social engineering attacks on cloud targets like cloud administrators, cloud security professionals, and cloud developers.

SECURING THE CLOUD AND DIGITAL TRANSFORMATION

Have financial institutions really moved away from relying on traditional, perimeter-based security? Do they have enough visibility into what's taking place in the cloud? Do they leverage data from multiple sources (e.g., context, network, behavioral) to drive authentication and authorization decisions? Have they invested enough in people, process, and technology to secure their digital transformation? The answer seems to be a resounding no, but there are steps they can take to rectify that.

Securing the cloud is a journey, not a destination. Too often, companies buy technology solutions to address security issues without spending enough time and effort thinking about making those solutions operational. In an environment where threats, vulnerabilities, and cybercriminals are always evolving, deploying new solutions should never be the end of a security initiative. It should be the start, and cloud security is no different.

APPENDIX

APT Groups

- **APT33:** Also known as Elfin, has been active since 2013 and uses custom malware and common techniques including brute force, spear-phishing and privilege escalation. Through its usage of wiper attacks, it's been linked to the Shamoon[15] malware.
- **APT34:** Also known as Helix Kitten or OilRig, has been active since 2014 and focuses on critical infrastructure. APT34 compromises email accounts to send spear phishing emails with malicious attachments in order to gain access to a company's network. It then uses common lateral movement and privilege escalation techniques.
- **APT35:** Also known as Charming Kitten, has been active since at least 2013. One of the hackers involved in Charming Kitten has been linked to the 2017 HBO hack, where 1.5 terabytes of data, including scripts of future episodes of popular shows like *Game of Thrones*, were leaked after the multimillion-dollar ransom wasn't paid. Monica Witt, a former U.S. intelligence officer, has been linked to APT35.
- **APT39:** This group has been active since 2014 and has been focused on the theft of personal information, which differs from the aims of other Iranian APT groups. While its objectives seem to differ, APT39 shares common TTPs with other sponsored groups, including spear phishing and the use of Mimikatz, a popular Windows credentials dumper.

METHODOLOGY

To assess how financial institutions are migrating to the use of cloud services and modernizing their payments infrastructure and capabilities, Javelin fielded three surveys covering different areas of responsibility within the enterprise.

Sample includes:

- **300 banking decision-makers:** Adoption of and concerns around cloud services, vendor selection considerations
- **300 payments decision-makers:** Adoption of and concerns around payments modernization, issues around faster-payments initiatives, key risks facing payments initiatives
- **300 cybersecurity decision-makers:** Use of outsourced security services, prevalence of breaches, type and location of data compromised, planned cybersecurity investment/initiatives

ENDNOTES

1. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, Published June 2, 2012. Accessed February 20, 2020.
2. https://www.reuters.com/article/us-cyber-heist-bangladesh-northkorea/cyber-security-firm-more-evidence-north-korea-linked-to-bangladesh-heist-idUSKBN1752I4. Published April 3, 2017. Accessed February 20, 2020.
3. https://www.theverge.com/2020/2/10/21131362/doj-justice-barr-china-equifax-breach, Published February 10, 2020. Accessed February 20, 2020.
4. https://attack.mitre.org/groups/. Accessed February 24, 2020.
5. https://www.us-cert.gov/APTs-Targeting-IT-Service-Provider-Customers, Accessed February 17, 2020.
6. https://www.theverge.com/2017/3/2/14792442/amazon-s3-outage-cause-typo-internet-server, Published March 2, 2017. Accessed February 13, 2020.
7. https://www.zdnet.com/article/google-details-catastrophic-cloud-outage-events-promises-to-do-better-next-time/, Published June 7, 2019. Accessed February 13, 2020.
8. https://www.zdnet.com/article/azure-global-outage-our-dns-update-mangled-domain-records-says-microsoft/, Published May 3, 2019. Accessed February 13, 2020.
9. https://www.zdnet.com/article/ransomware-attack-hits-major-us-data-center-provider/, Published December 5, 2019. Accessed February 25, 2020.
10. https://www.reuters.com/article/us-britain-travelex/travelex-recovers-uk-website-after-ransomware-hit-idUSKBN1ZU2DZ, Published January 31, 2020. Accessed February 25, 2020.
11. https://www.bankinfosecurity.com/baltimore-ransomware-attack-costing-city-18-million-a-12584, Published June 7, 2019. Accessed February 25, 2020.
12. https://rhinosecuritylabs.com/aws/s3-ransomware-part-1-attack-vector/, Accessed February 25, 2020.
13. https://www.javelinstrategy.com/coverage-area/new-criminal-toolbox-tools-and-tactics-modern-crimeware, Published August 22, 2019. Accessed February 25, 2020.
14. https://threatpost.com/deep-fake-of-ceos-voice-swindles-company-out-of-243k/147982/,Published September 4, 2019. Accessed February 13, 2020.
15. https://www.zdnet.com/article/shamoons-data-wiping-malware-believed-to-be-the-work-of-iranian-hackers/, Published December 20, 2018. Accessed February 24, 2020.

ABOUT JAVELIN STRATEGY & RESEARCH

Javelin Strategy & Research is a research-based advisory firm that helps clients make informed decisions in the digital financial world. It provides strategic insights for financial institutions, government, payments companies, merchants, fintechs and technology providers.

Authors: Mathieu Auger-Perreault, Director of Fraud and Security
Krista Tedder, Director, Payments

Contributors: Jacob Jegher, President
Tyler Brown, Research Analyst, Digital Banking
Crystal Mendoza, Production Manager

Publication Date: March 2020

ABOUT BOOZ ALLEN HAMILTON

At Booz Allen Hamilton, our singular purpose is to empower people to change the world. Nowhere is that more critical than in the world of cybersecurity today. For our Commercial clients, we are singularly focused on delivering world-class cyber, with a mission to defend and enable society's most critical industries and companies. Our passion is solving the complex and the consequential: those cybersecurity challenges that enable businesses to thrive in the marketplace. Booz Allen currently delivers advanced cyber defense solutions to one quarter of the Fortune 100, including eighty percent of the top ten North American financial institutions.

For more information contact the Booz Allen Hamilton Cybersecurity Division or get additional information at Booz Allen Hamilton.

© 2020 Escalent and/or its affiliates. All rights reserved. All rights reserved. No portion of these materials may be copied, reproduced, distributed or transmitted, electronically or otherwise, to external parties or publicly without the written permission of Escalent Inc. Escalent may also have rights in certain other marks used in these materials.