THE CLOUD ON THE HORIZON

Cloud computing is bringing new cybersecurity concerns to financial services

JOHN MEYER | Senior Director
Cornerstone Advisors

COMMISSIONED BY
TABLE OF CONTENTS

Why Are Cybersecurity Concerns Declining? ................................................ 1

Financial Institutions Are Finally Integrating Cybersecurity: Now How Do They Improve? ................................................................................... 4

The Impact of the Cloud: Risks and Opportunities ................................... 8

Conclusions & Recommendations .................................................................... 11

About the Author ........................................................................................................ 14

About Cornerstone Advisors .............................................................................. 14

About DefenseStorm ................................................................................................ 14

© 2020 Cornerstone Advisors. All rights reserved. Reproduction of this report by any means is strictly prohibited without written permission.
WHY ARE CYBERSECURITY CONCERNS DECLINING?

Cybersecurity has become a concern among bank and credit union executives, as well it should.

As banking evolves into a digital-first world, cybersecurity attacks remain high. VMWare’s Carbon Black group reported that cyber criminals increasingly targeted the financial services sector during the early part of 2020, with “attacks on banks and other financial institutions spiking by 38% between February and March to account for 52% of all attacks observed.”

According to a survey of financial institutions, nearly half (46%) see more than 1,000 daily security alerts while just 43% of legitimate alerts are resolved. In addition, financial services firms face the highest expenses—more than $1,400 per employee—across a range of industries (Figure 1).

**FIGURE 1: Cybersecurity Costs**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cybersecurity Costs per Employee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial services</td>
<td>$1,436</td>
</tr>
<tr>
<td>Utilities</td>
<td>$1,344</td>
</tr>
<tr>
<td>IT/Telecom</td>
<td>$1,258</td>
</tr>
<tr>
<td>Government</td>
<td>$959</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>$745</td>
</tr>
<tr>
<td>Retail</td>
<td>$689</td>
</tr>
<tr>
<td>Healthcare</td>
<td>$585</td>
</tr>
</tbody>
</table>

Source: Kaspersky Labs
Cybersecurity-related costs include:

- **Operational costs.** Across all debit and general-use prepaid card transactions for covered issuers, fraud losses to all parties as a share of the transaction value were 11.2 basis points, or $11.20 per $10,000 in transaction value, up from 10.3 basis points in 2015.”¹ In addition, total debit card fraud in the United States was over $1.2 billion in 2018.² Wire fraud losses in 2019 were reported at over $1.7 billion with less than $260 million recovered. ACH fraud losses made up about 7% of the volume of fraud losses in 2018, growing almost 50% each year. The cost of closing an account, investigating a Reg E dispute, and reissuing cards and checks can easily total over $150 per account before any recoveries of losses are made.

- **Reputational costs.** A study by The Ponemon Institute found that among people affected by a data breach, 27% took steps to terminate their relationships with the breached organizations. Eleven percent of respondents say the data breach resulted in a criminal act such as credit card fraud or identity theft. That same study found that, on average, companies saw a 5% share price drop directly following a breach.

- **Productivity loss.** According to IBM’s 2019 Cost of a Data Breach Report, each breach includes hundreds of cost factors, from legal, regulatory and technical activities, to loss of brand equity, customer turnover, and the drain on employee productivity. The average breach in the United States in 2019 cost $8.19 million to resolve.

**Costs Are Rising, Yet Cybersecurity Concerns Are Falling**

Despite the prevalence of attacks and high costs, the percentage of financial institution executives citing cybersecurity as a top concern has declined over the past few years. According to Cornerstone Advisors’ annual *What’s Going On In Banking* report, nearly half of the executives surveyed put cybersecurity on their list of top three concerns going into 2018. That percentage declined to 36% for 2019 and to 21% in 2020 (Figure 2).
Financial institution executives are being lulled into a false sense of security regarding cybersecurity. This sense of security is driven by increasing integration of cybersecurity into the operational areas of the business and compliance with regulatory guidelines. But it’s a false sense of security because financial institutions have yet to feel the impact of cloud computing on cybersecurity.

About This Report

Cornerstone Advisors interviewed 10 bank and credit union chief information security officers (CISOs) to understand how financial institutions are integrating cybersecurity across the enterprise, the impact of cybersecurity integration on operational performance, the effect of these efforts on compliance and reporting, the influence of cybersecurity on channels, and the common obstacles that institutions face while trying to make cybersecurity policies and procedures an enterprise-wide initiative, particularly when looking at cloud-based applications.
Financial Institutions Are Finally Integrating Cybersecurity:

NOW HOW DO THEY IMPROVE?

Cornerstone Advisors’ 2018 report Debunking Cybersecurity Myths: What Bank and Credit Union CEOs Need to Know About Managing and Measuring Cybersecurity identified the commonly held belief among executives that cybersecurity was IT's job. At the time, Aite Group Research Director Julie Conroy commented:

“The number one mistake banks make is not bringing fraud and cybersecurity people into projects during the innovation cycle. Cybersecurity personnel should be an integral part of every technology project—not an afterthought.”

The times they are a-changin’.

CISOs are increasingly seeing greater cooperation across the enterprise regarding the adoption of cybersecurity policies within their institutions. The CISO of a $266 million bank told us:

“It took the new CIO three years to educate the executive team on the importance of cybersecurity, but now it’s just a part of how we do business.”

The CISO of a $5 billion bank added:

“Risk management and cybersecurity permeate through the whole organization. You cannot just hand off these critical areas to a third party to dictate that some of the controls are in place. You have to get staff and leadership involvement.”

In response to the recent coronavirus crisis, for example, one CISO needed to roll out a new virtual private network (VPN) solution to the expanded work from home force at her bank, which employed a significant upgrade to the multi-factor authentication (MFA). She commented:

“I expected a lot more pushback from the team and got none. Everyone, including the displaced tellers, were receptive and understanding of the need for better remote access security.”

SO WHAT

Cybersecurity policy is becoming business as usual for more financial institutions across their enterprises. Executives are more confident today than they were three years ago that their cybersecurity policies are being well designed and executed within their own walls.
Organizational Changes Can Impact Cybersecurity Effectiveness

With these attack vectors increasing, several institutions are adopting new organizational structures. According to the CIO at a $6 billion bank:

“Cybersecurity used to live within our IT team. Now it reports up through the risk team at the bank. That change has helped us put cybersecurity first in all our lines of business. With all the fraud and scams out there, our management and front-line employees are so much more aware of how the bad guys are trying to hurt our customers.”

At another institution, a CISO shared:

“We moved our fraud team to work alongside the cybersecurity team since so much of the activity is happening online or via card skimmers. The effect is that we’re catching bad actors much more quickly and can move to block IP addresses and even countries. We recently blocked Sweden.”

Compliance and Reporting Are Becoming More Demanding

Cybersecurity integration is due, in part, to clarity from regulators as to how the organization needs to think about cybersecurity. In 2015, the Federal Financial Institutions Examination Council (FFIEC) released the Cybersecurity Assessment Tool (CAT) as a voluntary framework for financial institutions to use to determine their cybersecurity readiness.

After a breach of the SWIFT wire services in 2016, the FFIEC released guidance that stressed that:

Financial institutions should review risk-management practices and controls related to information technology systems and wholesale payment networks, including risk assessment; authentication, authorization and access controls; monitoring and mitigation; fraud detection; and incident response.
Executives interviewed for this study shared mixed feedback on regulatory pressure, however. Many said their institutions are reviewed for cybersecurity readiness every 18 months by their primary regulators (e.g., Federal Reserve Bank, FDIC, OCC or NCUA). Several months prior to an exam, regulators typically sent a five to six page request list of what they will review. One CISO shared:

“Our regulators want a visual tool of what our bank is monitoring, an inventory of software we use, our cybersecurity policies, and our change management policies. What I want is no board attention items.”

More and more, however, regulators are shifting their focus in exams to banks that use fintechs in the cloud. Another CISO commented:

“Regulators are increasing their scrutiny of fintech cloud vendors and that is a good thing. Even before COVID-19, the pain point of remote access was moving more banks to the cloud. With cloud services, innovation is changing so fast it is a challenge to get all of the due diligence information in a short period. AWS/Azure is easy from a deployment perspective, but how do we monitor these platforms for cybersecurity? A lot of the tools are open source, but these tools might not be fully vetted.”

In 2017, the FFIEC updated the CAT to clarify this section (Figure 3).
To echo these statements, the FFIEC recently published a joint statement on Security in a Cloud Computing Environment, in which it shared:

*Financial institution management should engage in effective risk management for the safe and sound use of cloud computing services. Security breaches involving cloud computing services highlight the importance of sound security controls and management’s understanding of the shared responsibilities between cloud service providers and their financial institution clients.*

**SO WHAT**

While regulators are working within the FFIEC CAT standards in their reviews with financial institutions, there is significantly more interest in the cloud vendors that service these institutions.
THE IMPACT OF THE CLOUD: RISKS AND OPPORTUNITIES

Cloud computing offerings will grow significantly over the next three years. Bankers have used outsourced processing via secure data centers for decades, but with the advancements of Amazon Web Services (AWS) and Azure, more fintech providers are promoting new services within both private and public clouds.

According to Bloomberg, 22% of all fintech applications now run in the cloud, and that figure is expected to grow to over 80% by 2025. Fintechs have adopted a cloud-first mentality, which requires financial institutions to more thoroughly examine the cybersecurity that these providers offer.³

Following the money tells a strong story about cloud adoption in banks. Today, a third of respondents allocate less than 6% of their IT budgets to cloud services. In three years, the percentage of banks spending between 11% and 15% of their IT budgets on the cloud will expand from 29% to 46% as the percentage spending between 1% and 5% drops from a third to about one in 10 (Figure 4).

FIGURE 4: IT Spending on Cloud Services

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Current</th>
<th>3 Years</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5%</td>
<td>17%</td>
<td>11%</td>
</tr>
<tr>
<td>6-10%</td>
<td>29%</td>
<td>26%</td>
</tr>
<tr>
<td>11-15%</td>
<td>46%</td>
<td>17%</td>
</tr>
<tr>
<td>16-20%</td>
<td>34%</td>
<td>20%</td>
</tr>
</tbody>
</table>

Source: Accenture
According to Quintin Sykes, managing director at Cornerstone Advisors:

“Thanks to continued deployments of cloud-based CRM, loan origination and other business applications, financial institutions continue to gain comfort with hosting non-public personal information in the cloud. Use of private clouds such as Microsoft Azure and Amazon Web Services to host licensed apps will continue to increase as institutions push hosting out of their owned/leased data centers. For those that don’t already have them on staff or via a partner, cloud deployment/integration skills will become a ‘must-have’ for CIOs this year.”

As cloud computing within banks grows, the prevalence of cyber breaches for cloud services is growing significantly as well. According to a Verizon study:

“Cloud assets were involved in about 24% of breaches this year, while on-premises assets are still 70% in our reported breaches dataset. Cloud breaches involved an email or web application server 73% of the time. Additionally, 77% of those cloud breaches also involved breached credentials. This is not so much an indictment of cloud security as it is an illustration of the trend of cybercriminals finding the quickest and easiest route to their victims.”

Cloud Computing is Creating Channel Challenges

The fastest adoption of cloud technology is within the digital channels followed by online deposit origination and online lending. Online lending has proved troublesome for several of the survey respondents. One CISO stated:

“We had such a bad experience with online lending and bad actors that we just shut the whole thing down. Since that time, we’ve been reluctant to even look at online lending again.”

Other significant challenges with small fintech third-party providers regarding cybersecurity include:

- **Over-reliance on providers.** There is an over-reliance on the provider to complete the cybersecurity checklists from the institution during due diligence. “It would be pretty easy for them to dupe us,” stated one CISO.

- **Due diligence.** CISOs discovered incorrect completion of the due diligence cybersecurity requests for third party risk management from the providers.

- **Transparency.** CISOs stated a lack of willingness to show any of the provider’s security policies or audits.
• **Confusion regarding provider responsibilities.** For example, when asked for a SOC-2, the provider gave the institution the AWS SOC 2. When the CISO questioned the vendor as to whether it had its own SOC 2, the provider was unaware it even needed to do its own.

• **Limitations.** Many cloud vendors have cybersecurity limitations. For example, they cannot IP-restrict or require MFA for third parties.

According to Jim Trautwein, senior director at Cornerstone Advisors:

“Recognizing the common objection of security in a shared-, remote- or out-of- control environment, cloud operators have to put particular emphasis on cybersecurity. Most good cloud providers: 1) Have dedicated information security officers (ISOs) and robust teams of information security engineers, administrators, monitoring systems and incident response procedures; 2) Run frequent or almost continual network scans, penetration tests and other security verifications; and 3) Provide independently prepared SSAE 16 SOC 2 reports that opine on the existence, quality and effectiveness of their internal control environments.”

**SO WHAT**

Good cloud providers dedicate significant effort to ensure they are compliant and secure in their offerings for financial institutions. However, many fintech startups struggle with cybersecurity policies and procedures.
CONCLUSIONS AND RECOMMENDATIONS

Don’t Lose Focus on Operational Integration

While many of the CISOs we spoke with talked of improvements in the integration of cybersecurity and operations in their organizations, banks and credit unions shouldn’t let up on the pedal on these integration efforts.

More financial institutions are seeing greater cooperation across the enterprise with adopting cybersecurity policies and practices, but there is still some resistance from the “revenue generators.” According to one CISO:

“The biggest area for pushback is in lending, where the need for speed in closing conflicts with the extra steps they have to take with cybersecurity. For example, lenders and their administrative assistants that feel deadline pressure were against the adoption of two-factor authentication and Dropbox. No one wants the friction of cybersecurity slowing down their ability to close business.”

A CISO of another institution added:

“Retail pushed back the hardest since they had to deal with some elderly customers who do not use SMS and cannot employ multi-factor authentication the way we wanted to.”

According to Sean Atkinson, CISO for the Center for Internet Security:

“Culture will make a CISO’s life easier if you can make it a point to address the fact that cybersecurity is a shared responsibility. If we frame the culture as key to implementing security controls, cybersecurity should become an inherited trait within your organization, leaving you less focused on dictating the need for security. Focus on a holistic approach for your organization that integrates policy with real practices. You’ll need a cybersecurity program that anyone in the organization can understand and actually implement. Consider minimum-level security awareness training for every employee.”

Overcoming the Cloud Challenges

The focus for bankers and regulators is moving toward fintech providers spinning up new offerings in the cloud for their financial institution partners. Many of these providers lack the understanding and experience the financial institutions have regarding cybersecurity policy and program integration.
That lack of understanding cannot dictate the cybersecurity posture for financial institutions as the cost of a data breach and the rising fraud attacks will continue to plague consumers and businesses.

Banks and credit unions should take the following steps to deal with the looming cybersecurity challenges posed by the adoption of cloud computing:

• **Establish a Technology, Compliance and Risk Committee or Cybersecurity Committee.** The committee should meet at least quarterly to discuss new products, services and service providers coming in the next three to six months. Invite representatives from each line of business/department to be on this committee. Ensure that the agenda includes each team member being responsible for not just outlining the product or service, but any cybersecurity-related issues that might arise from offering this new product or service. Once you have your committee established, ensure you determine the controls you expect the committee to monitor, the metrics that will be leveraged to monitor those controls, the cadence for validation of the controls, and the reporting of activities for senior management in your organization.

• **Develop a realistic or pragmatic cybersecurity review policy.** One CISO we interviewed said he knew that the 200+ item vendor cybersecurity questionnaire he received from a larger FI near him would be rejected by his team as way too draconian and overbearing. He stated: “Cybersecurity is a journey, and the worst thing I can do is lose buy-in from my peers.” Adapt policies and procedures that your institution can and will adopt. Make policy checklists that are simple to follow and easy to execute. Once you have these checklists, structure your controls for automatic monitoring and reporting to ensure compliance. With so few resources, cybersecurity professionals do not always have the time to review the controls in place. Partnering with a third-party provider with experience in these types of cybersecurity policies and controls can save your institution from costly mistakes and wasted effort.

• **Monitor your entire network infrastructure, including on-premise and cloud-based systems.** Ensure you have visibility into all network assets across the enterprise. Central monitoring is critical in ensuring your institution has a complete picture of your cybersecurity assets for security log and audit purposes. Being able to correlate data across systems allows your institution to better detect anomalies and manage threat vectors. Recruiting and hiring cybersecurity expertise can be expensive and challenging for many financial institutions. Even the largest firms find it daunting to try and monitor both their on-premise systems and their cloud-based providers. For many smaller and mid-sized institutions, partnering with a trusted cybersecurity firm can add the talent and expertise required to sufficiently monitor all your assets.
• **Employ an enterprise-wide training and continuous testing program.** Successful CISOs utilize a variety of educational tools for the FI’s staff including annual in-person training, quarterly online training, monthly phishing tests, and ad hoc real-world examples of the latest scams such as business email compromise (BEC) and social engineering sent out to the entire organization.

• **Continue business and consumer education and integration efforts.** Some of the CISOs we interviewed have partnered with their cybersecurity providers to co-host training on the latest scams out there including BEC and account takeover for their consumers and businesses.
ABOUT THE AUTHOR

John Meyer heads up Cornerstone Advisors’ BI/Data Analytics practice. In this role, John helps banks and credit unions better utilize their data to improve cross sales, retention, profitability and operational efficiency. Before joining Cornerstone, John developed product strategy for anti-money laundering and fraud detection for over 1,000 U.S. financial institutions as well as teller, new account origination, MCIF, mobile banking and Internet banking applications used by more than 2,500 U.S. institutions. He has held several senior positions at Harland Financial Solutions and served as chief strategy officer and product officer at Abrigo.

ABOUT CORNERSTONE ADVISORS

Cornerstone Advisors delivers consulting services, industry insights and executive forums focused on helping financial institutions improve profitability and elevate performance quickly and efficiently.

Cornerstone’s multidisciplinary team is backed by the experience that comes from hundreds of thousands of in-the-trenches client hours. We live by the philosophy that you can’t improve what you don’t measure, and we know that with laser-focus measurement, financial institutions can develop more meaningful business strategies, negotiate better vendor contracts, make educated technology decisions and strategically re-engineer critical processes.

Cornerstone publishes a variety of industry research and hosts executive roundtables for bank and credit union executives.

ABOUT DEFENSESTORM

DefenseStorm is a uniquely specialized cybersecurity and cybercompliance company built for banking. We help banks and credit unions achieve real time Cyber Safety and Soundness through the only co-managed, cloud-based and compliance-automated solution of its kind—delivered as both a technology system and a service supported by experts in financial institution security and compliance.

We unify detection, investigation, resolution, reporting and compliance into a single system of record to deliver complete, transparent and real-time cyber exposure readiness. We help security teams stay smart and executives stay informed, so they can easily prove they are secure as well as compliant with their own policies and with evolving industry regulations and guidelines, including the FFIEC-CAT and NCUA’s ACET frameworks, both of which are built on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
ENDNOTES


3 https://www.bloomberg.com/professional/blog/adoptionevolution-cloud-technology-changing-fintech-landscape

4 Verizon 2019 Data Breach Investigation Report
Have questions about this report?

CONTACT:

John Meyer
Senior Director | Cornerstone Advisors

jmeyer@crnrstone.com
480.990.5768