FINTALK REPORT

IT Insights for the Financial Services Industry

SUMMER 2016

REGULATORY COMPLIANCE

Technology Lightens the Load

CDW

THE POWER OF TECHNOLOGY

No matter what financial services category your business falls into, regulatory compliance continues to be top of mind for banks, credit unions, capital markets and insurance providers. Adhering to regulations can be a strain on both staffing and budget resources. But how can technology be a game-changer in addressing these issues? In this *FinTalk Report*, we take a closer look at the latest findings on this topic and learn more about how fintech companies are shaking up small business loans, especially in the community bank industry.

This issue of the *FinTalk Report* is filled with the best practices that both your peers and current industry leaders are applying to get ahead. Additionally, we'll share more on upcoming trends like blockchain that are gaining momentum in the financial services industry. We hope these tips and techniques will help your organization leverage IT to your advantage and drive your business forward with innovation.

Whether you're preparing to ramp up your data center, optimize your network, tap into the cloud or refresh your voice and data technology, CDW Financial Services is here and ready to support you with these and other IT initiatives. From talking with our financial services customers, we understand that everyone is at a different stage of their IT journey. Your dedicated CDW Financial Services account team is prepared to help choose the right blend of technology, services and support to gain — and sustain — a strategic and competitive advantage. We look forward to connecting soon about your IT needs.

Ben Weiss
Director, Financial Services

ONLINE RESOURCES

STAY INFORMED
Follow us on Twitter **@CDW_Finance** and check out our blog, **CDW.com/FinTalk**, for breaking fintech news, the latest trends, new infographics and insights from financial services experts.

CDW FINANCIAL SERVICES
To learn more about how CDW solutions and services can help financial services firms meet their regulatory requirements, visit **CDW.com/finance**.

CDW DIGITAL APP
All the IT resources you need — all available in one app. This app puts financial IT expertise at your fingertips!
CDW.com/digitalapp

WHITE PAPERS
"How Technology Helps Meet Regulatory Mandates"
See how the right solutions and services can help financial firms navigate the compliance minefield.

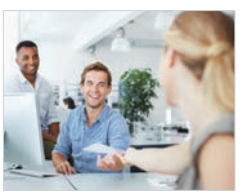
Capital Markets:
CDW.com/regulatory-compliance-cap

Banks and Credit Unions:
CDW.com/regulatory-compliance

CONTENTS

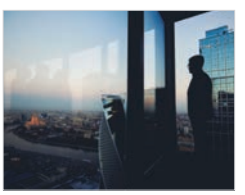
LIFTING THE WEIGHT OF REGULATORY COMPLEXITY WITH ADVANCED TECHNOLOGY

FinWatch provides an overview of what's top of mind in financial services regulatory compliance and finds that technology can be integral in addressing the issues. **2**



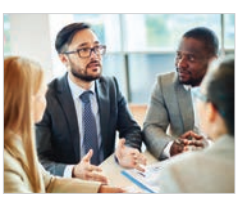
FINANCIAL INSIGHTS

Fintech Companies and Community Banks: Friend or Foe?
Fintech companies are targeting the small business loan industry. Should community/small banks collaborate with them or remain competitors? **6**



INFOGRAPHIC

Blockchain in Financial Services: The Experiment Begins
We provide a quick primer on the state of blockchain in financial services. **10**



TECH TIPS

Maintaining a "Core" Advantage
CDW expert Dan Hansen discusses the importance of keeping your core systems running efficiently. **8**

PARTNER CORNER

Setting the Bar for Cybersecurity
Security Evangelist and Strategist Jeff Man from Tenable discusses cybersecurity challenges, best practices and regulatory compliance. **12**

LIFTING THE WEIGHT OF REGULATORY COMPLEXITY

WITH ADVANCED TECHNOLOGY

Our overview of what's top of mind in financial services regulatory compliance finds that technology can be a game-changer in addressing the issues — from ever-increasing regulations to the challenging role of compliance, protecting consumer data, the value of encryption and implementing recent mortgage regulations.

For financial services executives, no matter what the industry segment (banks, credit unions, capital markets or insurance), regulation continues to be a top concern as a threat to their organizations' growth prospects. So it's no wonder that staying on top of regulations and the seemingly never-ending updates, testing and audits are straining resources to the max, from staff and budgets to IT. Many firms are finding that technology can be a powerful resource for reducing risk, streamlining the regulatory and reporting process in an efficient and cost-effective manner to better manage today's regulatory challenges, augment limited staffing, and reduce cyberthreats.

of bank and capital markets CEOs surveyed are concerned about over-regulation.[1]

of insurance CEOs surveyed are concerned about over-regulation.[2]

COMPLIANCE LEADERS: IN THE HOT SEAT

In the thick of it all is the compliance department, and leading the charge is the chief compliance officer (CCO). Compliance is being stretched to its limits and demands are intensifying as resources are cut and new responsibilities are added. It must not only maintain an objective control function, but also must carefully balance that with the role of front-office strategic business advisor. Many CCOs have found a seat at the board with CEOs and other C-level executives, but in 2016 they must prove their worth and chart a path toward tangible, sustainable outcomes that will reaffirm compliance's strategic positioning within the organization.[3]

Today, compliance officers are expressing regulatory fatigue and overload in response to those ever-increasing regulations, resource staffing challenges, increasing pressure on budgets, and continuous regulatory testing with heightened scrutiny and accountability from regulators.[4]

Despite these challenges, compliance officers are under pressure to deliver high-quality outcomes, with the added stress of potentially being held personally liable for organizational behavior and conduct.[3]

There is good reason for their concern, since the cost of non-compliance is high. The law firm Sutherland Asbill & Brennan reports that overall sanctions imposed by the Financial Industry Regulatory Authority alone, including fines and restitution, increased 14% in 2015 — jumping from $166 million in 2014 to $190 million.[5]

81%

of compliance officers say compliance needs to optimize operations in order to manage a more complex set of risks under tighter resourcing conditions (using technology).[3]

Regulatory burden is the second biggest challenge credit unions will face (behind loan growth).[6]

TECHNOLOGY: THE CHALLENGE AND THE SOLUTION

Additionally, compliance risks related to privacy, cybersecurity and customers are multiplying as services and transactions are increasingly delivered via digital channels. Yet the compliance department is challenged to deliver high-quality results utilizing an often outdated data and technology architecture that lags the standards required to manage the emerging risk landscape.[3]

As Accenture strongly advises, moving forward compliance must optimize operations in order to manage a more complex set of risks under tighter resourcing conditions. Leveraging the power of technology to manage risk will not only reduce costs but also enhance the consistency of controls. Financial services firms must prioritize the development of high-quality data and technology architecture to maximize compliance risk management capabilities. Compromise is not an option.

DATA: BATTEN DOWN THE HATCHES

A key regulation for financial services firms is The Gramm Leach Bliley Act, which established a "financial privacy rule." This rule governs the collection and disclosure of consumers' personally identifiable information (PII). It also includes vendor management controls as well as the "safeguards rule," which requires all financial institutions to implement controls that protect PII.

That regulation has proven to be extremely challenging in a world where financial services firms are hit by security incidents a staggering 300 times more frequently than businesses in other industries, with attack patterns changing frequently to outwit IT pros.[7] Financial services firms are not the only ones concerned about this — so are tech-savvy consumers, according to an Experian Consumer Services study that revealed 93% of consumers feel identity theft is a growing problem.[8]

Securing data has never been more important to protect customers, members and clients, and to comply with regulations and avoid penalties. Encryption is gaining recognition as a powerful IT solution to address this growing problem. In fact, according to a Ponemon Institute survey, 61% of business and IT managers said compliance was the main driver of encryption, while 47% cited protecting customers' personal information. The percentage of companies with an enterprise-wide encryption strategy applied consistently throughout the enterprise has risen from 15% in 2005 to 37%.[9]

THIRD-PARTY VENDORS

Another serious risk gaining visibility in 2016 is third-party vendors. A PwC survey found that financial services executives ranked the assessment of third-party vendors' security capabilities as the top challenge to their information security efforts. To improve this situation, more than half said they would increase spending to better monitor third-party security in the coming 12 months. Other financial services firms are improving third-party cooperation through the use of risk-based security frameworks. These guidelines can help companies more easily exchange information with third-party business partners and suppliers, and communicate expectations and concerns about the services that are provided.[10]

Many organizations are implementing strategic initiatives such as risk-based frameworks and cloud-enabled cybersecurity to improve security and reduce risks:[9]

RISK-BASED SECURITY FRAMEWORK

FORMALLY COLLABORATE WITH OTHERS

CLOUD-BASED CYBERSECURITY

BIG DATA ANALYTICS

MORTGAGE REGULATION

Since October 3, 2015, the mortgage industry has been contending with the Consumer Finance–issued rule that combines mortgage disclosures previously established by the Truth-in-Lending Act (TILA) and the Real Estate Settlement Procedures Act (RESPA).

Lessons learned from implementing these regulations should make implementation of the Home Mortgage Disclosure Act (HMDA), a federal law that requires certain financial institutions to provide mortgage data to the public, a bit easier. HMDA is effective in 2018 for loans originated in 2017, so all the new data points will have to be in place with the various loan origination systems used in the industry in 2016.

Ann Savage, SVP of Compliance at Mountain West Financial Inc., recently shared key insights on the use of technology in meeting mortgage industry regulations in an *MReport* interview.[11] Savage stated that, " ... compliance is integral to loan quality and profitability. The lenders that can and do manufacture compliance loans with the least amount of human intervention will be the most successful."

Although Savage may be speaking about lenders, her advice can be applied universally when it comes to regulations and technology. She notes that the best way to ensure compliance is:

1. To ensure you have people on your compliance team who understand the rules and can work with production and operations to simplify processes and ensure systems are working properly; and
2. Automation, automation, automation.

Compliance can be an opportunity for innovation: The lenders with the best technology focused on ensuring compliance have and will continue to have a competitive advantage. Take note, financial services firms, no matter what your industry – this is excellent advice.

Accenture surveyed leading compliance officers at global banking, capital markets and insurance institutions, asking them:

What types of change do you feel are likely to become the most important in your organization within the next 12 months?

67%
TECHNOLOGY
Improvements to systems and adoption of new tools and technology

51%
DATA
Investment in data management, analytics and related controls

50%
COMPLIANCE OPERATING MODEL
How compliance is organized internally, including streamlining, re-scoping, etc.

47%
COLLABORATION WITH THE BUSINESS
How the relationship between the first and second lines of defense is reviewed and/or clarified

44%
RECRUITMENT OF NEW SKILLS
How relevant skills for the compliance function are identified in the marketplace and recruited

44%
DEVELOPMENT OF EXISTING SKILLS
Skills development for compliance professionals, including training and development

42%
COLLABORATION WITH OTHER FUNCTIONS
How compliance works with other functions including HR, audit, technology and finance

30%
LOCATION STRATEGY
Changes to how compliance headcount is distributed among being co-located with the business, near-shored and far-shored

62%
CHALLENGES TO COMPLIANCE ROLE
Fear that stronger front-line processes will create risk for the function's independence

Which risk types do you believe will be the most challenging for the compliance function?

50%
CYBER RISK
Challenges to information security, resilience and privacy

41%
REGULATORY COMPLIANCE RISK
Failure to keep pace with compliance regulations

Sources: [1]pwc.com, New York, NY, "19th Annual Global CEO Survey: Creating a Platform for Competitive Regeneration," (Banks and Capital Markets), February 2016 [2]pwc.com, New York, NY, "19th Annual Global CEO Survey: Creating a Platform for Competitive Regeneration," (Insurance), February 2016 [3]accenture.com, New York, NY, "Compliance at a Crossroads: One Step Forward, Two Steps Back?" 2016 [4]thomsonreuters.com, "Thomson Reuters Annual Cost of Compliance Survey Shows Regulatory Fatigue, Resource Challenges and Personal Liability to Increase throughout 2015," May 2015 [5]thinkadvisor.com, FINRA's 5 Biggest Fine Categories in 2015, February 2016 [6]nafcu.org, "Credit Union Challenges," 2015 [7]infosecurity-magazine.com, "Finance Hit by 300 Times More Attacks than other Industries,' June 2015 [8]experian.com, "Leveraging Customer Intelligence to Ensure Data Privacy," January 2016 [9]csoonline.com, "Report: Compliance Biggest Driver of Encryption," February 2016 [10]pwc.com, "Turnaround and Transformation in Cybersecurity: Financial Services," 2016 [11]themreport.com, "What the Mortgage industry Needs to Know About Regulatory Compliance," March 2016

FINTECH COMPANIES AND COMMUNITY BANKS:

FRIEND OR FOE?

Small business loans have historically been the centerpiece of community banks. In fact, community banks account for more than half of small business loan volume, according to Harvard's Kennedy School.[1] But there are other more compelling reasons why these loans are a significant part of community banks' revenue. Small businesses rate community banks high in their delivery and servicing of such loans. According to a Federal Reserve Bank survey, community banks received the highest satisfaction score – higher than credit unions, large banks and online lenders.[2]

Enter fintech firms, shaking up the status quo in the financial services industry and driving disruption, innovation and competition. They're targeting lending, with a focus on small business and consumer loans, and they're succeeding. Funding Circle is just one prime example – an online small business loan platform that originated $800 million in loans in 2014 (roughly the size of a community bank's portfolio). In 2015, Funding Circle forecast that its originations would reach $1 billion for the year.[3]

Fintech companies' innovative and advanced technology enables the rapid submission of loan applications and approvals, all via digital platforms. This very efficient and automated underwriting process, driven by data analytics and cutting-edge technology, delivers a simple, seamless and rapid consumer experience. However, this is the very thing that many community banks find challenging to deliver, because they are hampered by their legacy operating systems in an industry traditionally lacking innovation, agility and advanced technology.[3]

Competitors though they may be, fintech companies and community banks are beginning to see the potential of collaboration. Fintech firms see the advantages of leveraging banking's large and loyal customer bases, experience with risk and regulations, broad product sets, established trust and deep financial pockets.[4] Community banks can benefit from fintech firms' technological advances and seamless customer experience delivery.

Fintech companies' innovative and advanced technology enables the rapid submission of loan applications and approvals, all via digital platforms.

"There's no question that fintech is changing the landscape of financial services," says Charie Zanck, Chief Executive Officer of American Community Bank and Trust. "In order to remain competitive, it's important that we create a digital platform that delivers a seamless, efficient experience for our customers, particularly for services critical to our business model. Whether you choose to do that by upgrading legacy systems and infrastructure with advanced technology, or by partnering with a fintech company, the time has come to develop and implement a strategy."

BY THE NUMBERS:

FINTECH AND COMMUNITY BANKS SMALL BUSINESS LENDING

Over 90% of bankers believe fintech firms will have a significant impact on the future landscape of banking.[7]

Small business lender satisfaction scores[2]

SMALL BANK
75%

LARGE BANK
51%

CREDIT UNION
56%

ONLINE LENDER
15%

OTHER
33%

Why are successful loan applicants dissatisfied with their lenders?[8]

LONG WAIT FOR DECISION
43% small bank
45% large bank
22% online lender

UNFAVORABLE REPAYMENT TERMS
15% small bank
16% large bank
51% online lender

DIFFICULT APPLICATION
52% small bank
51% large bank
21% online lender

HIGH INTEREST RATES
15% small bank
16% large bank
70% online lender

Choosing to partner with a fintech company may be the best method for some community banks to deliver more cutting-edge services and remain competitive. Options range from affiliating with fintech firms that can make operations more efficient or partnerships focused on the front end, like loan transactions.

In considering a partnership with a marketplace lender, "Different banks really need different things," says ABA Vice President Rob Morgan (quoted in a recent *ABA Banking Journal* article). He advises that there are five key issues to keep in mind: the customer experience, the financial trade-offs, the operational process, reputational effects and the regulatory response — and the process needs to be complemented by robust due diligence.[5]

For community/small banks considering a technology upgrade, work with a technology partner that has deep understanding of the marketplace, is knowledgeable about industry vendors and can give you an edge on the competition.

Perhaps the most compelling reason to take action is provided by the survey results in the *World Retail Banking Report* that show how quickly fintech firms are catching up with traditional banks in the area of trust. Banks view customers' trust as their greatest strength, but today the percentage of customers who somewhat or completely trust fintech firms is up to 87.9%. It's time to take some action.[6]

Choosing to partner with a fintech company may be the best method for some community banks to deliver more cutting-edge services and remain competitive.

Sources: [1]bankingjournal.aba.com, "Small Business: A Competitive Edge for Community Banks," April 2016 [2]stlouisfed.org, "Small Businesses More Satisfied with Small Bank Lending," March 2016 [3]frbatlanta.org, "Fintech Companies: Banks' Allies or Rivals?" March 2016 [4]thefinancialbrand.com, "Banking and Fintech: An Uncommon Partnership," November 2015 [5]bankingjournal.aba.com, "How to Understand and Partner with Marketplace Lenders," February 2016 [6]worldretailbankingreport.com, "World Retail Banking Report 2016" [7]thefinancialbrand.com, "Banking and Fintech: An Uncommon Partnership," November 2015 [8]bankingjournal.aba.com, "Which Lenders Are Small Businesses Most Satisfied With?" March 2016

MAINTAINING A "CORE" ADVANTAGE

Core systems must run efficiently for financial services firms to remain competitive in today's marketplace. We spoke with CDW Business Development Manager Dan Hansen to learn how to keep your core in top condition.

DAN HANSEN,
CDW Business Development Manager

What should financial services organizations do to maintain a robust, efficient, secure and agile core infrastructure?

A: To maintain a healthy core infrastructure, financial services organizations need to do the basics right. They need to ensure that their storage and network infrastructures are up to date and ready to scale with flexible storage and network solutions. This prepares them for unexpected bursts of growth. Banks and credit unions also need to be sure that their Windows platforms are robust. This is very important because some core providers are adding new capabilities to the Windows platform, *not* to the core system.

They also need to be running server virtualization software, such as VMware or Hyper-V, which gives them the capability to quickly add servers, typically in minutes. Hyperconvergence is the latest and greatest technology infrastructure system with a software-centric architecture that tightly integrates computing, storage, networking, virtualization and other technologies in a single box. Efficiency is greatly increased with this solution.

Business continuity and disaster recovery capability systems also need to be modernized along with the production network. Surprisingly, tape is still being used in some financial institutions as primary backup. Customers, members and clients are expecting very quick disaster recovery times and recent recovery data (RTO/RPO), and you cannot get a rapid recovery time with tape. Of course, long-term archiving is still a viable use for tape for any financial institution.

How can they modernize/augment their core systems to keep up with the demands of digitalization?

A: Mobile is a "must have" for staying competitive in today's financial services marketplace. In the U.S., the regulatory safeguards are limiting financial institutions' development of mobile capabilities beyond basics. However, the exploration continues. For example, an Eastern Bank commercial customer recently applied for a $100,000 loan via a mobile app in less than 10 minutes. When will that begin to happen on a wider scale?

Data management and analytics are essential to building an advantage. Capital markets firms and larger financial firms require greater speed. More and faster data dictates that you have better data management capabilities, and more data requires better storage.

Cloud solutions can help with storage. Many financial institutions trust their core providers to do that for them, but it is important to note that the core provider doesn't have any better or different safeguards, security or third-party audits of their systems than other cloud providers. Understanding this allows you the freedom to build a cloud solution to fit your unique business requirements.

What are the advantages and disadvantages of augmenting core systems versus replacing them? When is it time to replace a core system?

A: Core systems aren't going away anytime soon because core providers are putting practically all of their ancillary and complementary product applications on Windows servers. That puts financial services organizations into the augmentation business. The main disadvantage to augmenting core systems instead of improving them is that core providers set a maintenance fee if the bank has its core system in house, or they charge a fee for the use of the outsource capabilities of the core system. So, you're not getting more capabilities, but you're still paying the same fee – along with paying for every ancillary product software *and* the infrastructure to support it. That means you're losing money.

What many financial services firms don't realize is that you don't have to go with your core provider to get infrastructure services. This is an area where a third-party expert like CDW can help out. We know the trusted sources that will work well with your core provider and that can provide the best and most secure products, at the best prices, to meet your unique needs.

You should replace your core system when your customers/clients/members are demanding real-time processing versus end-of-day processing and/or when your core system can no longer provide the types of services your institution needs to grow. A limited number of the top core providers are now offering real-time processing.

How does core infrastructure relate to regulatory compliance?

A: Data is a key area. Regulations require that you maintain the confidentiality, integrity and availability of data – which all ties into core systems. So you must ensure that your routers, switches and firewalls are all up to date, configured properly and patched. Make sure your active directory is correctly configured and data access authority is properly managed. Have an external penetration test every year, and have an internal penetration test (often called a vulnerability assessment) about every other year. If you make any system changes, make sure to have your internal system penetration tested. Some financial institutions have "ongoing" testing of all these components, which is better yet.

Also, there's one more very important consideration before you take action. *All* decisions surrounding the topics discussed above need to be based upon a robust risk assessment of your entire infrastructure, and the solutions should be based on protecting your data and growing your institution.

48% **of bankers surveyed said legacy issues are their biggest challenge – one preventing them from realizing the potential benefits of their data.**

Source: finextra.com, "Banks' Legacy Systems Holding Back Omni-Channel," February 2016

BLOCKCHAIN IN FINANCIAL SERVICES: THE EXPERIMENT BEGINS

2016 is the year that blockchain technology is under the microscope in financial services. We provide a quick primer on the state of blockchain and the benefits it can provide to your bank, credit union, capital markets firm or insurance organization.

BLOCKCHAIN: ARE YOU ON BOARD?

57% of financial services executives are unsure about or unlikely to respond to blockchain technology.[1]

83% of financial services executives are at best "moderately" familiar with [blockchain].[1]

Distributed ledger technologies offer financial services institutions a once-in-a-generation opportunity to transform the industry to their benefit, or not.[1]

WHO'S IN IT TO WIN IT?

Over **40 companies** have joined R3, one of the most high-profile consortiums, to drive bitcoin innovation and standards.[2]

Groundbreaking collaborations have taken place with the World Economic Forum, Singularity University and MIT Media Lab Digital Currency Initiative.[2]

$1B has been invested in blockchain projects by over 100 financial institutions.[3]

THE BENEFITS OF BLOCKCHAIN

Opportunities include:[4]

- Automated processes and reduced compliance errors
- Improved compliance with "Know Your Customer" regulations and creating secure digital identities

Blockchain has the potential to transform financial services infrastructure and offer:[2]

- Potential cost savings
- New revenue opportunities

IMAGINE THE POSSIBILITIES

Potential applications:[1]

- Increase efficiency by removing the need for reconciliation between parties
- Speed up the settlement of trades
- Enhance efficiency in loan origination and servicing
- Improve clearing house functions used by banks
- Facilitate access to securities

OPPORTUNITY KNOCKS IN 2016

Deloitte predicts that **blockchain will become a reality** for many in 2016.[2]

37% of Deloitte's cryptocurrency community believe a product launch will be the biggest breakthrough in the blockchain space in 2016.[2]

Sources:
[1]pwc.com, New York, NY, "Blurred Lines: How FinTech is Shaping Financial Services," March 2016
[2]coindesk.com, "Deloitte: Blockchain Will Become a Reality in 2016," January 2016
[3]magisteravisors.com, San Francisco, CA, "Blockchain & Bitcoin in 2016: A Survey of Global Leaders," December 2015
[4]deloitte.com, "Blockchain Applications in Banking," 2016

PARTNER CORNER

SETTING THE BAR FOR CYBERSECURITY

JEFF MAN,
Security Evangelist and Strategist, Tenable

Security Evangelist and Strategist Jeff Man of Tenable discusses cybersecurity in the financial services industry. He shares insights on securing your organization and best practices for tightening your defenses and improving your security posture beyond regulatory compliance standards.

tenable® network security

About Jeff

Jeff Man offers over 30 years of information security experience, compiling a rich knowledge base in cryptography, information security and PCI.

What cybersecurity challenges are you seeing in the financial services industry? How is Tenable helping to secure these organizations?

The paradigm for cybersecurity has changed. In the past, cybercriminals took a break-and-enter approach to stealing data. Today, they can launch remote attacks that embed malware in your network that may be hidden in your systems, secretly harvesting data for days, weeks or months. The traditional method of securing your network and operations against vulnerabilities isn't working against this type of cybercrime. Now you must work harder to find the malware and detect when it sends your data out of your network.

To do that, you need to establish a baseline of what is "normal" for your network operations, network traffic, network activity, user activity, user behavior, critical data flows and data repositories. Then you can detect what's abnormal and what a malicious attack might look like. It requires skill, but also technology, because there's so much data now that it's impossible to analyze all the traffic manually.

That's where Tenable can help. Our technology provides three ways of detecting data flows, network traffic and network activity information. First, our static vulnerability detection finds the systems attached to your network, analyzes them for vulnerabilities and sets your baseline. Our Nessus® scan engine can detect more systems such as servers, network devices, servers, workstations, notebooks, tablets and mobile devices — whether you're on a traditional network, a virtual network or operating in the cloud.

A second method for detecting network activity is our Passive Vulnerability Scanner (PVS), which acts much like a network sniffer to monitor network traffic at strategic points. The continuous monitoring that PVS provides helps to identify systems that might have been offline during static scans and also to identify malware that's designed to elude the detection of a static scan. We also can detect unintended sensitive data flows both within and outbound from your network.

The third component, Log Correlation Engine, gives us the ability to look at every system and event log generated by the systems on your network. Using analytics, we review log traffic and identify exploitation attempts, additional vulnerabilities and malware. The system logs enable the technology to track user behaviors like successful and failed log-ins, which helps us identify malicious activity and compromised user accounts.

All the data our collectors produce can be formatted in numerous dashboards and reports — or what we call "Assurance Report Cards" (ARCs) — to allow easy review and presentation to system owners, management, senior executives and board members.

What are some cybersecurity best practices that could help financial services firms better defend their organizations?

Education and cybersecurity awareness is an important defense tactic no matter the size of your financial services organization. You need a great technical team, documented processes and technology solutions. However, it's equally important to have everybody in your organization understand the risks involved with conducting commerce on the Internet, and the impact of their behavior as individuals and as company employees.

Every employee in your organization can have an impact on your business based on the things they do — and equally important, what they don't do. Human error is a frequent cause of cybercrime, whether it's not following policies/procedures, not utilizing policies/procedures or worse yet, using weak passwords, sharing passwords or downloading unknown attachments. Every single employee must be educated that their actions have a real impact, and should be aware of attempts to gain access to your network — whether through suspicious emails inviting them to open an attachment or click on a link (called "phishing" emails) or other "social engineering" attempts to steal their log-ins or access badges.

Also, collaboration across the enterprise with business units working together to help solve the larger cybersecurity problem needs to be a priority, particularly in financial services organizations. For example, fraud and cybersecurity business units often work independently of each other, yet working together could offer the potential for great synergy. Theft of data — a cybersecurity problem — is relatively meaningless until a cybercriminal figures out a way to use that data or monetize that data. However, that aspect of the crime is typically handled by the fraud unit. Working together, cybersecurity and fraud units could streamline and eliminate duplication of efforts and share combined resources, experiences and lessons learned to reduce cybercrime.

63%

of confirmed data breaches involve using weak, default or stolen passwords. Basic defenses continue to be lacking in many organizations.[1]

What cybersecurity advice could help financial services organizations better meet regulatory compliance?

Most financial services organizations are focused on their compliance "grade" — "What's our percentage of compliance?" "Are we showing signs of improvement?" This tends to create an attitude of meeting the bare minimum of regulatory standards: "What can I do to get by?"

> Employee, customer and "soft" IP data are the top targets of cyberattacks.[2]

The PCI Data Security Standard, which has been around since 2004, is based on a pass-or-fail, "you're doing it or you're not" approach, and could actually be used as the framework for securing any of your sensitive data. The PCI DSS offers a fairly comprehensive cybersecurity framework that sets a higher standard of metrics for an information security or cybersecurity program by assuring that good security practices are built in to the "business as usual" fabric of the organization. The companies I've worked with over the years that have treated PCI seriously and attempted to do it well have been far better off than the companies that treated it as a nuisance or burden.

The PCI DSS is very familiar to most organizations in the financial services world, whether they report on PCI compliance or not. Treating PCI DSS as a framework for your entire cybersecurity program is a good idea and actually reinforces the original intent of the PCI DSS — which was to measure your data or cybersecurity program as it related to payment card data. The underlying assumption has always been that the organization already had a functional cybersecurity program, so the PCI DSS was designed to assure consumer payment card data was properly protected.

Sources: [1]verizonenterprise.com, "Verizon's 2016 Data Breach Investigations Report Finds Cybercriminals Are Exploiting Human Nature," April 2016 [2]pwc.com, New York City, NY, "Turnaround and Transformation in Cybersecurity: Financial Services," 2016

One CDW Way
230 N. Milwaukee Avenue
Vernon Hills, IL 60061

888.706.4239

CONNECT WITH CDW FINANCIAL SERVICES!

Visit our website CDW.com/financial

Check out our blog CDW.com/FinTalk

Follow us on Twitter @CDW_Finance

CDW Financial Services

MKT14J891