Seizing Opportunity in the New Age of Financial Services

White Paper

Prescriptions for Challenges that Stand Between Financial Services Providers and Digital Success

Digital transformation represents US$1.3 trillion of value at stake in the financial services industry.

A New Era of Opportunity

Digital transformation is reshaping every country, city, industry, and organization. Connecting people, process, data, and things with innovative digital and Internet of Things (IoT) technologies creates abundant opportunities for organizations to increase revenues and lower costs to the tune of US$14.4 trillion dollars of value at stake in the private sector between 2013 and 2022. No industry is impervious to this transformation, and the financial services industry, sitting at the heart of the global economy, will figure prominently in the equation. Nine percent of the value at stake in digital transformation and the rise of the IoT—US$1.3 trillion—resides in the financial services industry alone.[1]

The growth of the IoT itself is nothing short of staggering. It's estimated that the IoT will mushroom from 2 billion objects in 2006 to 200 billion by the year 2020, or approximately 26 smart objects for every human being on our planet.[2] While the impact of this growth is highly visible in the retail, manufacturing, and transportation industries, its effects on the financial services industry are not always as apparent.

However, when you consider that the real power of the IoT and its increased connectivity is gathering and disseminating information to and from a nearly infinite number of sources, its influence becomes more evident. The financial services industry depends on its ability to collect and analyze data. The expansion of that ability through digitization won't just be disruptive—it's likely to transform the industry as we know it.

Meanwhile, banks and other financial institutions are investing significant sums of money and resources to build up their internal infrastructures and customer-facing technologies. According to IDC Financial Insights, retail banks are spending roughly

1. 2014, *Intel® IoT Gateway* Product Brief
2. 2015, *As the Internet of Things Grows Exponentially, National Cyber Security Awareness Month Focuses on Securing our Connected Devices and Networks*

Seizing Opportunity in the New Age of Financial Services

US$16 billion on digital information technology initiatives—a number that continues to grow. And in PricewaterhouseCoopers' (PwC's) sixth annual digital IQ survey, financial services is among the top 10 industries investing in IoT innovations.[3]

With New Opportunities Come New Challenges

The real test for financial services organizations isn't how much money they can throw at technology. It's how they invest it. With every new opportunity, new challenges arise, and the solutions won't be uncovered with conventional thinking and spending. If companies—especially industry incumbents in investment, commercial, and consumer banking—wish to thrive in the new digital era, they'll need to rapidly and securely capitalize on the proliferation of digital communications tools, such as smartphones, tablets, and the countless applications they enable. They'll also need to innovate and adapt quickly as new revenue streams, value drivers, business models, and customer requirements begin to take shape.

The real test for financial services organizations isn't how much money they can throw at technology. It's how they invest it.

One challenge is the rise of new types of competitors. As industries digitize, new players are emerging and establishing a foothold within the industry. PayPal has become the number one online payment method, not just in the United States, but in numerous countries. Over at Google, a plastic debit card has been launched to accompany Google Wallet now used by millions of consumers. Bitcoin is opening eyes, too. Traditional banks, such as UBS and others, are testing the blockchain processes used by Bitcoin as it looks to capitalize on innovation. Even retailers are getting into the action, such as Starbucks whose loyalty card handles nearly one-third of its U.S. transactions. As the lines between conventional roles begin to blur, technology companies are becoming financial services companies, and financial services companies are becoming technology companies. The mandate for incumbent financial services providers is clear: if they don't evolve and adapt, their influence and relevance will diminish as competitors offer the innovative financial services IoT customers demand.

A second challenge is regulation. As a rule, financial services are subject to strict regulations, so employing new tactics and deploying new technologies can take longer than it does in most other industries.

"Multiple compliance guidelines and regulations apply to financial services organizations. However, these organizations cannot assume that complying with the many regulations provides sufficient defenses. Even though these regulations can spark change in the sector, they are not all encompassing and not systematically effective across all subsectors in all countries. In addition, it takes time for them to take effect….Because online criminals are constantly targeting this industry, security professionals need to adapt faster than new regulations can be written."[4]

3. 2015, *The "Fin"-ternet of Things: How IoT affects Financial Services*
4. 2015, *Security for Financial Services: Addressing the Perception Gaps in a Dynamic Landscape*

Changing customer demand presents a third obstacle. As financial services customers adopt mobile and cloud services, organizations must be willing and able to meet their needs. Competitors are already intently focused on meeting customer demands. So for banks and other financial institutions, rethinking the way and the speed with which they respond to customers is absolutely imperative.

The risk for financial services providers is clear: if they don't evolve and adapt, their influence and role will diminish as competitors offer digitized financial services their customers demand.

Incumbents also need to emphasize the simplicity and quality of the experience they provide when customers use their services. If trends continue, customer experience and service efficiency will be more critical than service cost, or even loyalty, as organizations attempt to differentiate their brands. Customers will choose services they find engaging, smart, fast, and effortless.

Finally, we need to consider the business value of all these new models and services—the data. As the IoT connects a rapidly growing number of objects, more data will be generated, collected, and transformed into usable analytics and insights. Because they can lead to business growth and profit, the insights provided by smart agents and linchpin algorithms will often be far more useful than the objects and services that acquire them. Many analysts foresee a US$15 trillion opportunity over the next 5 to 10 years as all this data is combined with sensors and analytics to unleash its true value.[5] The question is how organizations will protect their information assets as they share them with strategic partners.

Security is no longer merely a threat-centric issue. In the Internet of Things, security is also a people-centric and a things-centric concern. Where the firewall was once the security perimeter, the proliferation of endpoints has now extended that barrier. Device and personal identity has become the security perimeter in the new digital age.

The risk for financial services providers is clear: if they don't evolve and adapt, their influence and role will diminish as competitors offer digitized financial services their customers demand.

Security in the Digital Age

While the future of the financial services industry appears promising, organizations still face some monumental security challenges. While innovation increases and the digital economy expands, so do the frequency and sophistication of security incidents. In fact, one 2015 industry report contends that financial-services businesses encounter security incidents 300 percent more frequently than other industries.[6]

As more financial data becomes available, the desirability of that data to cybercriminals increases. But securing the rapidly expanding variety of endpoints and associated applications is no simple task. Security is a highly complex and involved undertaking for financial institutions. Digitization is creating more information handoffs and more attack vectors—and the hackers know it.

5. 2014, *Making connections: An industry perspective on the Internet of Things*
6. 2015, *2015 Industry Drill-Down Report - Financial Services*

"...the requirement of those in the financial services industry to maintain their real-time connection to the global economy can impair certain logical security precautions. For instance, eliminating a known vulnerability in one bank's system can break necessary continuity with banks that have not yet upgraded their own." [7]

In light of the factors standing between incumbent financial services and success in the digital economy, this paper takes a brief look at seven insights that organizations should examine as they march forward into the world of connected people, devices, services, and data.

Customer trust, corporate control, and data privacy are also at risk as third parties become more involved. With large amounts of valuable financial and personal information at risk through third-party transactions, IT leaders need to strengthen their defense and remediation practices on an ongoing basis. Information sharing throughout the entire financial services value chain creates risk for all parties involved. Handoffs open up security gaps, and information security relies on the strength of the least-developed defenses in the chain.

There's no doubt that incumbent financial services organizations face a multitude of hurdles as they become digital. They have more conservative risk profiles, more barriers to entry, and far more to lose from security failures. Security threats need to be neutralized. Intense regulation and compliance requirements need to be met. The speed and innovation exhibited by competitive start-ups need to be matched. And incursions from technical giants, such as Apple and Google, have to be confronted.

In short, systematic obstacles are now preventing financial services incumbents from digitizing assets and innovating fast enough for them to take hold of the enormous IoT opportunity in an increasingly digital world.

Seven Insights for Overcoming the Challenges

In light of the factors standing between incumbent financial services and success in the digital economy, this paper takes a brief look at seven insights that organizations should examine as they march forward into the world of connected people, devices, services, and data. These are not the only actions to consider, but they are measures that may hold the greatest promise for enabling organizations to capitalize on the coming digital business opportunities and to maintain leadership despite a competitive assault on all fronts.

Insight No. 1: Focusing efforts on security as a value-add to new technologies rather than on in-house innovation.

Incumbent financial services providers can use their strengths to become stronger competitors. Security is one area where incumbents have a clear advantage. By adopting parallel strategies—competing aggressively with new companies on innovation while simultaneously partnering with them as providers of security—incumbents can expand their revenue options. Legacy assets, security infrastructure, and access to existing services are all elements that startup financial technical companies are lacking.[8]

7. 2015, *Finding Security Among The Internet of Things*
8. 2014, Banking At A Digital Crossroads

Organizations must learn to visualize the intelligence so decision makers can determine the ideal outcomes for their customers and shareholders.

Insight No. 2: Strengthening capabilities through partnership with, or acquisition of, third-party innovators.

If you can't beat them, join them. As digitization becomes the norm, stand-alone financial products and services will become more common, making it increasingly difficult for incumbents to cross-subsidize their offerings. But if financial-services institutions join forces with innovators, startups, and even established organizations—through partnership, acquisition, incubation, or investment—competing with these emerging standalone products and services will become more viable. In the financial-services marketplace, technical acquisitions will be commonplace. Trading, sharing, and monetizing smart algorithms will become the norm. Intelligence sharing will be monetized and benefit all parties. Organizations must learn to visualize the intelligence, so decision makers can determine the ideal outcomes for their customers and shareholders. These leaders will also need to secure their smart algorithms as they keep certain ones private while sharing others with partners. By carefully choosing how to secure their algorithms and how to use third-party partners, incumbent organizations can increase the strength of their services and capabilities portfolio.[9]

Insight No. 3: Moving beyond the conventional notion that "prevention is better than cure."

Rather than expending more operating expenses (OpEx) or capital expenditures (CapEx) on preventative security products and services, financial-services providers should prepare themselves for the IoT by focusing more on detection and response. In the past, an estimated 80 percent of security budgets were committed to preventative technologies. Today, the balance should be closer to 40 percent on prevention and 60 percent on detection and response technologies. To compensate, some companies opt for bimodal business operations, employing legacy solutions alongside new cloud technologies. However, these short-term fixes are doomed to fail. Retrofitting legacy solutions, or current tech stacks, and combining them with newer technologies simply won't keep pace with the emerging threats of the digital age.

Insight No. 4: Using digital communication tools to establish control and ownership of customer spending data.

Financial services institutions possess enormous volumes of information. Much of it is valuable data about financial trends, consumer transactions, and spending habits. By combining this data with personal information from social media and other sources collected through smartphones and tablets, incumbent organizations can provide an indispensable service to clients. By creating an information-value framework with embedded security controls—both in the value models as well as the IoT sensors deployed at ATMs, point-of-sale (POS) terminals, digital wallets, and other social media payments—this valuable new hybrid information can be used to influence consumer buying decisions and cement brand loyalty.[10]

9. 2015, *The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed*
10. 2015, *The Future of Financial Services: How disruptive innovations are reshaping the way financial services are structured, provisioned and consumed*

Insight No. 5: Exploring solutions for monitoring connected devices and IoT services.

The IoT shines a bright spotlight on the relationships between connected devices, the applications they run, and the information that flows between them. Nowhere is that more apparent than in the connection between information security, information technology security, operational technology security, and physical security. IT executives must now confront that reality and determine how their future enterprises' security will be governed, managed, and operated. According to Gartner by the end of 2017, one in five organizations will deploy digital security measures devoted solely to IoT devices and services. Simply put, financial institutions can no longer afford to delay researching such initiatives.[11] Furthermore, they need to be in the forefront of setting up standard frameworks for IoT manufacturers to establish standard digital security measures and build long-term trust.

According to Gartner by the end of 2017, one in five organizations will deploy digital security measures devoted solely to IoT devices and services.

Insight No. 6: Creating single framework for identity and access segmentation of IoT entities.

This is a new era driven by identity-centric security—or security associated with people, things, and virtual software—unlike our current generation driven by data-centric security. Yet, financial services institutions aren't currently using process and data modeling tools to identify and accommodate various relationships between IoT entities, such as devices, services, users, and data. Consequently, identity access management (IAM) and technology leaders, as well as service providers, can't take full advantage of the added business value the IoT can deliver. And that business value is about to skyrocket. By the end of 2016, the Internet of Things will drive device and user relationship requirements in 20 percent of all new identity and access management implementations. By the end of 2017, that number will soar to 50 percent. The existing approaches to identity management won't capture the full potential of business value. Yet by rethinking and rearchitecting their approaches, IAM and other security leaders will find greater success.[12]

Insight No. 7: Evaluating the security impact of blockchain technology on the Internet of Things.

As blockchain technology continues to proliferate, the IoT implications will be many, and security will play a critical role. For example, a blockchain-enabled exchange platform can serve as a catalyst for international development, sustainable investment, and peer-to-peer lending through a globalized financial network the size of the Internet. After blockchains and decentralized networks begin enabling tasks, such as tracking the histories of devices and physical assets, documenting data exchanges, and turning smart devices into independent agents, financial organizations will need to consider the impact of blockchains, assess the risks, and determine the role security will play.

11. Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015
12. 2014, The Identity of Things for the Internet of Things

Seizing Opportunity in the New Age of Financial Services

White Paper

The Promise of the Digital Transformation Awaits

Uncertain changes lie ahead for the financial-services industry. However, one thing is certain: if incumbents do not rethink their services, IT, and security strategies for the digital era, new players will emerge quickly to steal their market share. Even more important is the golden opportunity right in front of financial services companies. If they're willing, they can seize everything digitization enables, secure their established market positions, and capitalize on the many lucrative possibilities. Incumbents have a clear mandate, as well as the necessary resources, to dominate security in the financial-services space. They can use that dominance as a competitive advantage over startups and nontraditional financial-services companies entering the industry.

To make that happen, incumbents must digitize their assets quickly and innovate even faster as our digital world accelerates forward. The bolder financial organizations will surely take notice and act accordingly. The intention of this white paper is to provide the critical first steps forward in a long, profitable, and essential journey into digital transformation and the Internet of Things.

The intention of this white paper is to provide the critical first steps forward in a long, profitable, and essential journey into digital transformation and the Internet of Things.

Learn More

Take a closer look at the financial-services infrastructure threat landscape. Download our free white paper Security for Financial Services: Addressing the Perception Gaps in a Dynamic Landscape.

Read more about security in the financial services industry and what Cisco Security Services is doing about it at www.cisco.com/go/securityservices.

Cisco Security Advisory Services help you use security technologies and services to protect performance, create competitive advantage, and capture long-term sustainable business values. Make better decisions about how you connect, communicate, and collaborate. Contact our advisors today, and learn more about the IoT and the vast opportunities it presents for financial-services organizations.

DEC15CS4807 12/15