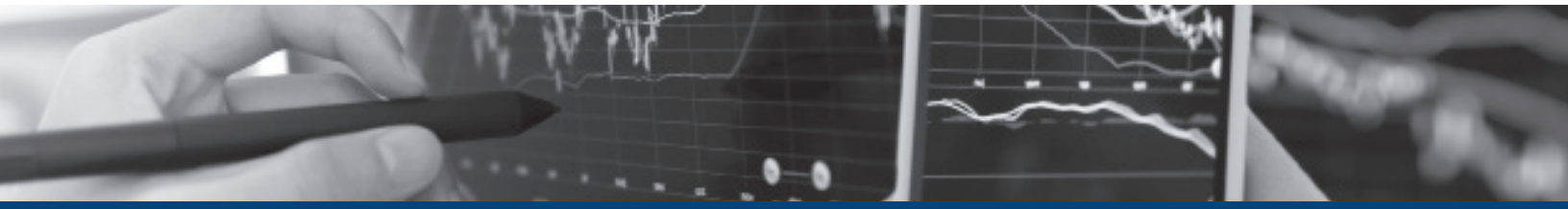
SOLUTION BRIEF

Transform Financial Services While Protecting Reputation and Data



SecureWorks®

Introduction

The financial services industry is diverse, encompassing banking, insurance, real estate and investment management firms. While up-to-date numbers are difficult to estimate with precision, analysts estimate that the financial services industry generated $13.1 trillion in revenues in 2014, with industry profits comprising 25-35 percent of all corporate profits.[1] And as the immediate after-effects of the financial crisis have subsided, the current outlook for the worldwide financial services industry is one of cautious optimism and rapid transformation.

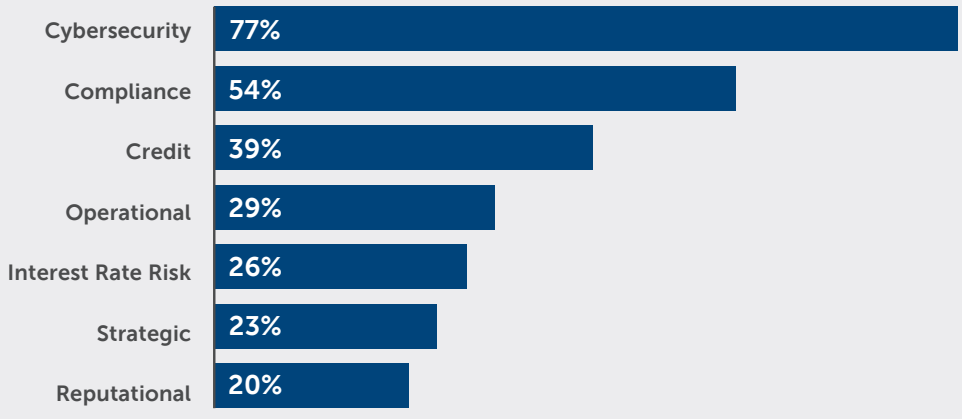
Changing consumer demographics and reduced banking institution loyalty among customers since the global financial crisis have led to an increase in the number of financial services providers.

Digital disruption — from artificial intelligence to machine learning to block chain payment — is upending the financial services industry, requiring you to invest more in technology for service differentiation, personalization and a frictionless user experience. Consumers and corporate customers alike are adopting mobile banking and "fintech" tools to harness big data and personalize investment or upsell recommendations. Cost pressures abound as you allocate significant amounts of IT and security resources and staff to maintaining aging systems instead of innovating new services and financial tools.

Traditional financial firms hampered by legacy systems and cost structures are facing intensified competition as firms capitalize on changing consumer preferences and new payment methods to usher in new financial services technology and related complexity.

Top Three Risk Categories That Banks Are Most Concerned About[2]

Respondents were asked to select no more than three.



Financial Services Industry Challenges

Since the financial crisis, traditional banking institutions with established track records have seen a decline in trust and brand reputation among their customers. What's more, the once labor-intensive financial services industry, built on personal relationships and trust, has continued the transformation brought about by retail bank consolidations and automated computer trading, resulting in hundreds of thousands of fewer jobs in the industry. In addition, compliance mandates continue to increase, which contribute to an environment of regulatory uncertainty for banking and insurance companies. Other challenges facing the financial services industry include minimizing the risks associated with supply chain and technology partners, protecting mobile and cloud-based data and maintaining privacy across global boundaries.

Financial Services Technology Brings Opportunity and Risk

The wealth of data and intellectual property (IP) that your company possesses is a lucrative prize to professional hackers. Cyber criminals are evasive and persistent as they target your proprietary trading algorithms and highly sensitive customer data. Financial services companies face real risk of being blackmailed to release this data or seeing IP sold on the criminal underground to the highest bidder — perhaps even to a competitor. According to the Identity Theft Resource Center, finance and banking have been key segments of the industry for threat actors due to the gold mine of valuable credit card and personally identifiable information (PII).[3] A misstep in the public eye can also cause investment capital to erode and your supply chain partners to avoid doing business with you. Clearly, the cyber attacks in the financial services industry should serve as a wakeup call to enhance your security framework and data privacy methods.

Top financial services challenges include:

- **Securing an increasingly-complex technology infrastructure.** The financial services industry is intertwined with other banks, investment management firms and governing bodies like the U.S. Federal Reserve, creating a web of interdependence. Security threat experts have already seen cyber attackers attempting to first breach a weak link — often smaller, community banks — as an entry point to compromising larger financial institutions. New technologies layered on top of legacy systems can also create gaps in security. Continuous monitoring of these security systems is essential to balance threat prevention and detection, but as the amount of data increases exponentially from year to year, 24x7 monitoring can stretch thin even the most committed IT and security teams. For the second year in a row, 77 percent of bank executives and board members polled in a recent industry-wide survey say cybersecurity is their top concern.[4]
- **Keeping pace with regulatory scrutiny.** Financial services is one of the most heavily-regulated industries, with mandates such as FFIEC, OCIE, PCI DSS, EU GDPR and National Information Security Directive in Europe demanding significant time and attention from your internal compliance teams. The interconnectedness of systems and technology means that cybersecurity mandates and frameworks are increasing, making comprehensive security visibility and reporting even more essential.
- **Maintaining brand reputation and trust.** Cyber threats such as ransomware, spear phishing and data breaches, coupled with the attendant public breach disclosure and negative press, can erode public trust and reputation. For smaller financial organizations that serve a regional market, lost trust can have a meaningful impact on revenue and customer retention. For larger financial institutions, one lost major customer (such as a treasury customer) can cost millions in lost revenue.
- **Enhancing new services and customer experiences.** Financial institutions must innovate and adopt new processes to compete with technology savvy fintech

> Fintech
>
> A combination of the words "finance" and "technology" used to describe tech-based financial services.[5]

firms that embody automated and more efficient operations. Your once-loyal business customers and retail consumers are now more willing to use new financial tools and smaller firms in order to reduce costs or to bring expanded capabilities such as capital markets access. Mobile financial services and analytics make it easy to disperse data and valuable information across an organization, increasing the risk and chance of data exfiltration. While third-party partners can augment your capabilities, they require security vetting and strong operational management.

- **Addressing the security skills shortage:** Although the largest handful of banks and insurance firms have deep security expertise, mid-sized organizations in banking, insurance, hedge funds and wealth management are typically faced with a staff and skills shortage. Staying ahead of cyber attackers requires a significant investment in resources and strategic investment; many financial organizations augment their skills with managed security services providers.

New technologies and approaches bring opportunities to the financial services industry. Interconnectedness and critical infrastructure concerns heighten awareness of your business risk in light of the persistence of today's cyber attackers.

Conclusion

The financial services industry is an important part of global GDP, accounting for seven percent of output in the U.S. and 10 percent in the U.K.[6] Longstanding financial services organizations in the future face continuous pressure to innovate or be overtaken by nimble upstarts who use technology to increase efficiency, personalization and analytics to win away customers. As the financial industry leverages customer data and an "always on" mobile ecosystem, you must continue to protect PII and data privacy. Cyber attackers continue to target the financial services industry due to its valuable data, which can be stolen electronically and sold to the highest bidder. Cyber attackers also target the data for non-monetary purposes like political hacktivism. You must be vigilant to balance preventing and detecting cyber threats to maintain your hard-won trusted relationships and brand reputation.

SecureWorks Solutions

As a world leader in security solutions, SecureWorks provides an early warning system for evolving cyber threats, enabling you to prevent, detect, rapidly respond to and predict cyber attacks on your financial services operations. We undergo periodic examinations by the member agencies of the Federal Financial Institutions Examinations Council (FFIEC), as well as annual Statement on Auditing Standards (SSAE 16) Type II audits. SecureWorks delivers intelligence-driven solutions and expertise across banking, investment management and insurance in 59 countries.

Security and Risk Consulting

Our Security and Risk Consulting team provides strategic advice and analysis to help you enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency. Our highly skilled security consultants help you test and improve your security defenses and security processes, and design and develop new security programs. SecureWorks offers robust visibility into emerging threats to financial institutions of all sizes.

Managed Security Solutions

SecureWorks offers a wide range of managed IT security solutions for financial services organizations. The Counter Threat Platform™ is at the core of our intelligence-driven approach to security solutions. The CTP analyzes billions of network events 24x7 to discover potential threats, deliver mitigation approaches and generate valuable context and threat insights. This visibility, in addition to our own proprietary CTP research, lets us develop and implement countermeasures specific to the financial services industry. We help you detect advanced persistent threats (APTs) and mitigate any damage that they may have caused. Our security analysts serve as an extension of your team to monitor and detect threats across your environment. For financial services firms large and small, we provide management and monitoring that can identify true threats and eliminate false positives that can distract your time and attention.

Threat Intelligence

The SecureWorks Counter Threat Unit™ research team collects relevant information wherever it can be found, and then analyzes it and synthesizes it into meaningful guidance on which you can act. Our threat intelligence helps you identify threat actors who may be specifically targeting your financial services organization or executives, and provides the insights to help you defend and even preempt both financially motivated attackers and political hacktivists. SecureWorks is also a member of Financial Services — Information Sharing and Analysis Center (FS-ISAC) and contributes to threat information sharing across the worldwide financial services industry in order to increase sector-wide visibility of cybersecurity threats.

Incident Response and Management

Our incident management practices provide rapid containment and eradication of threats, minimizing the duration and impact of a security breach that threatens your sensitive customer data, patented trading algorithms and proprietary financial services processes.

Leveraging our cyber threat intelligence and global visibility can help you prepare for, respond to and recover from even the most complex and large-scale security incidents. SecureWorks has the people, processes and technology to help you detect threats sooner to minimize damage and identify root causes to avoid being recompromised.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com

End Notes

[1]Tiburon Strategic Advisors, "Financial Services Industry Profitability," September 17, 2014, http://www.tiburonadvisors.com/RRAP/FSI_Profitability/Client/FSI_Profitability_KF.doc , accessed September 14, 2016.

[2]http://www.bankdirector.com/files/5214/5804/9793/2016_Risk_Practices_Survey.pdf

[3]Identity Theft Research Center, January 25, 2016, http://www.idtheftcenter.org/Data-Breaches/2015databreaches.html , accessed September 15, 2016.

[4]Bank Director's 2016 Risk Practice Survey.

http://www.bankdirector.com/files/5214/5804/9793/2016_Risk_Practices_Survey.pdf, accessed September 19, 2016.

[5]Advisoryhq.com. http://www.advisoryhq.com/articles/what-is-fintech-definition-and-review/ , May 23, 2016, accessed September 20, 2016.

[6]BankInnovation.net. "How We Define & Categorize Fintech," http://bankinnovation.net/2016/04/how-we-define-categorize-fintech/, April 12, 2016, accessed September 18, 2016. (no author)