2017 Cybersecurity Outlook for Financial Services Organizations

Synoptek®

Table of Contents

The Cybersecurity Challenge

In an industry as highly regulated as financial services, one might think that maintaining regulatory compliance would go a long way toward assuring sufficient protection. This is not the case. While various regulatory acts focus on protecting specific data assets they do not cover the broader scope of network and operational considerations required to achieve high degrees of security.

What Cyber Security Challenges are Facing the Financial Services Industry?

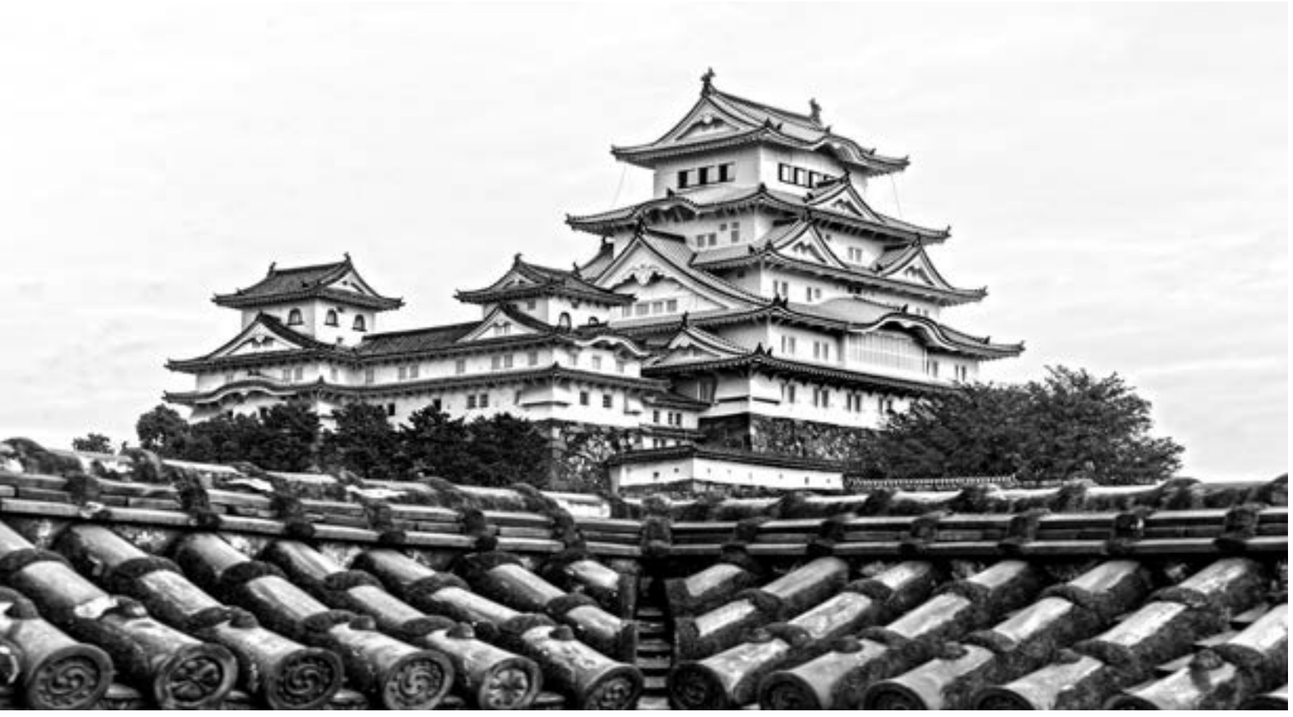
Network Engineers often note that the most vulnerable segment of any network is that segment which occurs between the keyboard and the back of the chair, namely the user. When you think about it, there's great common sense to this. Users are not digital. Their responses can occur anywhere along a continuum of possibilities.

They are unpredictable and easily fooled by well-disguised exploits, such as "phishing" exploits. In a phishing exploit, users receive an email from what appears to be a credible sources. The email contains a link that looks like it goes to that credible sources reliable website, however it does not. In its simplest form, letter substitution, as an example the letter "o" may be substituted by the numeral "0" to create a different domain altogether, as in "northernbank.com" being changed to "n0rthernbank.com."

Clicking this link unleashes any one of a variety of attacks, such malware that corrupts data or steals valid credentials. In the case of the recent hacks on the Democratic National Committee it has been reported that "spearphishing" attacks were used, in which the recipient of the false email was specifically and individually targeted.

According to PwC Global, phishing was the #1 vector of cyberattacks in 2016, with 43% of financial service employees in a recent survey citing phishing attacks.

One of the growing dangers arising out of phishing and other activities is the threat of "ransomware" in which a company's data is held hostage or stolen. The company is then offered the opportunity to retrieve their data by paying a substantial ransom. Of course there's no reason to believe the attacker will return the data, or not strike again. The main perpetrators for phishing attacks against Financial Services organizations are organized crime syndicates and state-affiliated actors.



The Cybersecurity Challenge

Exploiting the Small to Invade the Large

Larger financial institutions are required by the Consumer Financial Protection Bureau (CFPB) to assure that the smaller third-party associates they work with maintain the same full compliance as they do. This is in response to the many attackers who have learned that the best way to penetrate the large financial network is often through smaller systems with which they connect. Under these rules, in addition to maintaining compliance with regulatory acts such as the Gramm-Leach-Bliley Act (GLBA) or themselves, the large financial institution is responsible for their third-party partners maintaining identical compliance.

From the perspective of the third-party vendor partner, the choices are to become compliant or to risk losing their large financial services clients. This is also challenging in that most large financial institutions are ill-equipped to assist their third-party partners in achieving and maintaining compliance. When their partners fail audit, they fail audit. Many of these large financial institutions have turned to external service providers such as Synoptek to help their partners perform the necessary upgrades and process changes.

A highly visible example of attackers reaching an extremely large network through a smaller, less protected one involves SWIFT, the Society for Worldwide Interbank Financial Telecommunications, whose network processes an average of 25 million financial transactions each day. While this makes SWIFT a highly desirable target for cyber criminals, the organization has spent accordingly to provide a high degree of protection for its data and its network. According to the New York Times, "Swift is billed as a supersecure system that banks use to authorize payments from one account to another." In fact, they report one financial analyst as commenting that SWIFT is "The Rolls-Royce of payment networks." Not so much for some of the banks that use their service. Reuters reports that "A Bangladeshi central bank official's computer was used by unidentified hackers to make payments via SWIFT, and carry out one of the biggest-ever cyber heists." A total of US$81 million was stolen.

In this case, the hackers detoured through a smaller bank's network to make use of the larger SWIFT network.

This clearly suggests that financial institutions must include protection against their own third party vendors in their security plans.

Balancing Customer Convenience and Data Security

In their 2016 Cyber Security Intelligence Index, IBM notes, “On the consumer side of the financial services business, it’s important to recognize that some of the very conveniences that banks now routinely offer customers—including automated teller machines, credit cards and mobile banking apps—have introduced a level of accessibility that goes a long way toward making the financial system highly vulnerable to cyber attacks.”

Here are the most common types of attack vectors reported by financial services companies:

42%	Unauthorized Access
31%	Malicious Code
17%	Sustained Probe/Scan
6%	Suspicious Activity
3%	Access or Credentials Abuse

It’s also important to note that 60% of attackers were identified as being insiders with access to the network, with 44.5% having clear malicious intent, and 15.5% causing events through inadvertent action.

According to an April 2016 article in CSO, being high-profile targets puts financial institutions at a distinct disadvantage as they must marry security with keeping business operations efficient, expeditious, and reliable.

Hostile cyber actors have demonstrated keen insight into developing tactics, techniques, and procedures (TTPs) in order to increase the success rate of their operations. The adage, while cliché, remains true: attackers only have to gain entry once; organizations need to be vigilant and robust defensively all the time, a nearly impossible undertaking in this interconnected reality.

Financial data is very appealing to criminals as it can be quickly monetized especially in an array of regional underground criminal marketplaces. These venues offer platforms to sell stolen merchandise to customers that in some cases have been vetted. Given that cyber crime is projected to cost the global economy an astounding $445 billion, the ability to quickly acquire and turnover stolen data can maximize profits substantially. CNBC points out that the projected $445 billion loss is, “more than the market cap of Microsoft ($411 billion), Facebook ($314 billion) or ExxonMobil ($332 billion) — according to an estimate from the World Economic Forum’s 2016 Global Risks Report.”

The annual 2016 Verizon Data Breach Investigations Report (DBIR) differentiates their industry-target analysis between number of incidents and number of actual breaches with confirmed data loss. In terms of incidents, the financial services industry ranked third behind “Public” and Entertainment. However, they were clearly the industry with the greatest number of actual breaches, nearly tripling the nearest other industry, Accommodation. The IBM Cyber Security Intelligence index adds that, while companies across all industries averaged 52,885,311 security events in 2016, the financial services industry averaged 82,898,784, more than 36% more.

2016 Cybersecurity Scorecard

The SecurityScorecard 2016 Financial Industry Cybersecurity Report provides some startling insights into the condition of cyber security in the financial sector showing, for example, that the bank with the weakest security posture of all surveyed is one of the top 10 largest financial service organizations in the US measured by revenue.

SecurityScorecard identifies potential vulnerabilities in network security by identifying open ports and examining whether or not an organization uses best practices such as staying up-to-date with current protocols, or securing network endpoints to ensure external access to internal systems are minimized.

Among the top 20 U.S. commercial banks, 19 have a Network Security grade of ‘C’ or below. Specific Issues include:

- 18 out of 20 commercial banks support one or more weak or insecure TLS cipher suites
- 15 out of 20 commercial banks have a SSL certificate that is expired
- 9 out of 20 commercial banks have open FTP ports found
- 5 out of 20 commercial banks have open SMB ports found

To evaluate if malware is active in a system, SecurityScorecard reverse engineers the source code of an infection and determines how the malware communicates back to its control. Researchers can then intercept the communication, which can be traced back to an IP address from which it’s emanating, indicating an infected network.

Among the top 20 U.S. commercial banks, 17 of them have an IP Reputation grade of ‘B’ or below. Specific Issues include:

- Generic Malware was found in 15 out of 20 commercial banks
- Ponyloader was found in 14 out of 20 commercial banks
- Vertexnet was found in 9 out of 20 commercial banks
- Keybase was found in 8 out of 20 commercial banks
- Malware events were detected in all 20 commercial banks over the past 365 days.
- Over 422 malware events over the past year were detected in just one of the commercial banks.
- A total of 788 malware events were detected in all 20 commercial banks over the past 365 days.

Risk Mitigation and Cybersecurity Considerations for 2017

The SecurityScorecard 2016 Financial Industry Cybersecurity Report concludes, “Our data shows that the financial industry still needs to improve basic security hygiene such as keeping a consistent patching cadence, support proper SSL security, and improving their overall network and application security. Not only do these issues not adhere to security standards, they present a real increase in potential breach risk when hackers become aware of their vulnerabilities.”

However, tracking reports such as the Verizon DBIR and the SecurityScorecard Cybersecurity Report across several years shows that the variety of exploits changes with each year, as does the target attack community. Financial Services institutions simply cannot focus on information security tactically. Instead, financial services institutions must incorporate network security and information privacy into their overarching risk mitigation strategies.

Discussing “Technology Trends” in their “Top financial service issues of 2017”, the Financial Services institute at PwC notes, “It’s no secret that financial services has become a digital business. But the speed and extent of the transition is downright jarring.”

Artificial intelligence now drives the way leading firms provide everything from customer service to investment advice. Blockchain, with its ability to store information on distributed ledgers without a central clearinghouse, could upend a variety of businesses. Digital labor, or robotic process automation, is helping firms automate things they couldn’t do before, without having to hire an army of developers. And all of this depends on robust cybersecurity, to hold off threats that are coming from multiple directions.

New Strategies to Mitigate Digital Risk

The financial services industry is responding with specific new strategies to mitigate their digital risks. Findings:

- 51% of respondents in their Global State of Information Security® (GSIS) Survey reported that they use managed security services for solutions like authentication and real-time monitoring and analytics.
- 54% plan to spend more to improve network and mobile security
- 61% now require employees to complete on-going cybersecurity training

Risk Mitigation and Cybersecurity Considerations for 2017

Here are the top five risk mitigation and cybersecurity considerations financial services companies will want to heed in 2017:

1. Integrate cybersecurity, anti-fraud, and anti-money laundering efforts. You’ll improve your ability to ward off threats by combining analytics from pooled data, strengthening your risk management environment, and implementing controls more effectively.

2. Find the regulatory balance in the guidance. Focus first on building a robust risk-based cybersecurity program. This can help you achieve your broad strategic objectives while also complying with regulatory requirements.

3. Establish an independent, second line of defense. Keep your security governance and oversight capabilities separate from cybersecurity design, implementation, and operations. Also, your second line of defense should engage the board and its risk committee on cyber topics.

4. Anticipate risks from third parties. Recognize the potential for increased risks when outsourcing. Collaborate with third party vendors to make sure they take the right measures to protect your data.

5. Speed innovation by focusing on cybersecurity up front. When designing and developing new digital products and services, you should integrate cybersecurity and privacy in the beginning stages. Failure to maintain full regulatory compliance may result in very heavy fines and penalties, including possible imprisonment for involved individuals. Failure to maintain superior security for your information and the networks it travels upon may prove fatal to your business, or at least to your career. A comprehensive digital risk mitigation strategy is beyond a good idea, it is now a survival strategy.

Who is Synoptek?

Synoptek was founded in Irvine, CA in 2001 and provides strategic IT leadership and IT operational support for customers around the world.

Synoptek has a credited history of providing managed IT services to financial services organizations for almost 20 years with client types ranging from credit unions, banks, insurance companies, investment funds, accountancy companies, and Fintech organizations.

During this time, Synoptek has provided secure access to critical information from devices, improved performance and security of systems while decreasing exposure to risk and compliance violations. Synoptek has experience with managing IT security for large and complex environments from sophisticated cyber threats, including insider attacks, malware mercenaries, and attacks on critical infrastructure.

Synoptek has a diverse team of over 475 IT professionals that protect information environments and detect emerging threats within them 24x7, this gives the team and the customer the opportunity to proactively defend against active cyber-attacks.

Synoptek can extend the capacity of your organization's IT Team to protect applications, computing, and network infrastructure with advanced security solutions that are easy to implement, fully managed, and do not require large upfront investments.

In 2016, Synoptek has been globally recognized for many industry awards, including: #20 on the Top 100 Cloud Services Providers list, #4 on MSPMentor's Top 501 total-service-provider list, and reception of three accolades for customer service from the 2016 ACE Awards.

Synoptek is headquartered in Irvine, CA with offices in San Francisco, CA; Sacramento, CA; San Diego, CA; Las Vegas, NV; Boise, ID; Denver, CO; Marlborough, MA; Pittsford, NY; New Brunswick, Canada and Raleigh, NC.

Managed IT Security Solutions from Synoptek

In response to the increased attacks on the financial services industry, Synoptek has developed several programs including: end-user training and threat education, end-point security, network security, as well as cyber security advisory.

Network Anomaly Detection Program

Synoptek's cyber security analysts look at the core of your network, using world-class technology that uses machine self-learning and probabilistic mathematics. Immediately after installation, the appliance begins modeling normal activity and detects abnormalities occurring in real-time. By looking at this data, Synoptek's security analysts are able to take action on any active security incidents to prevent the infliction of serious damage. Organizations will also receive a weekly Threat Intelligence Report, outlining any risks and recommended remedial action.

End-User Training - the Human Firewall Program

Financial Services organizations must ensure that they're not just investing in technology, but also nurturing a security-conscious environment. To accomplish this, Synoptek can provide monthly cyber security training for all of your employees. Synoptek's human firewall program has three main components: educating the employee, minimizing human error, and getting ahead of new threats. The main objective of a human firewall is to raise the awareness of your staff to such an extent that they become a solid line of defense against attempts to compromise your systems. This training helps your users stay on top of threats - like phishing attacks, malware, and Trojans.

Virtual CISO Consulting Services

Synoptek's Virtual CISO and cybersecurity consulting services helps fill in the security gaps and challenges unique to your organization. Combining industry knowledge and security expertise, a virtual CISO can establish process and an effective security and risk program.

Here's how Synoptek's Virtual CISO service can help your organization:

- Policy development and maintenance
- Business continuity planning and disaster recovery
- Compliance requirements and regulations
- Vendor risk management
- Regular meetings to review and educate a security and risk program

888.796.6783
Synoptek.com