SecurityScorecard

2016 Financial Industry Cybersecurity Report

SecurityScorecard
R&D Department

August 2016

Cybercrime has jumped to the second most reported economic crime in PWC's Global Economic Crime Survey and financial institutions are prime targets. As cybercriminals find new ways to attack, breach, and exploit organizations, threat patterns such as phishing, spear-phishing, and social engineering evolve and become more sophisticated. Financial organizations need solutions that assess vulnerabilities and their vendor's vulnerabilities in real-time.

In the spring of 2016, SecurityScorecard analyzed 7,111 financial institutions in the SecurityScorecard platform to find existing vulnerabilities within investment banks, asset management firms, and major commercial banks to determine the strongest and weakest security standards based on security hygiene and security reaction time compared to their peers.

We also cross-referenced compliance industry framework adherence and analyzed recent data breaches and resulting ramifications of Scottrade, CharlesSchwab, and The Central Bank of Bangladesh.

Overview

Cybersecurity departments for major financial organizations face compounding challenges. Threats from cybercrime have increased and legacy IT systems are increasingly becoming a risk factor, especially in the financial industry. Many financial organizations rely on legacy IT systems that are expensive to maintain, prone to more unpatched vulnerabilities and the general challenges of software integration and architecture upgrading compound when mergers and acquisitions are in place.

A SecurityScorecard rating is a comprehensive indicator of relative security health, or security posture. Because only one vulnerable point in a security system is enough for a hacker or an attack to succeed, we take a multidimensional approach to security ratings. Our rating platform looks at 10 primary security categories. Within each category, thousands of unique data points are scored and weighted to determine an overall category grade. Each category grade is then used to calculate an organization's overall rating.

Key Industry Findings & Insights

- The U.S. Commercial bank with the lowest security posture is one of the top 10 largest financial service organizations in the U.S (by revenue).
- Only one of the top 10 largest banks, Bank of America, received an overall 'A' grade.
- 75% out of the top 20 U.S. commercial banks (by revenue) are infected with malware and a number of malware families were discovered within these banks, including Ponyloader, and Vertexnet.[1]
- 95% out of the top 20 U.S. commercial banks (by revenue) have a Network Security grade of "C" or below.
- Nearly 1 out of 5 financial institutions use an email service provider with severe security vulnerabilities.
- The best performing Investment Banks in IT Security include Goldman Sachs, Exchange Bank, BNP Paribas Fortis and Banco Popolare.

See Appendix at the end of this report for key term explanations and definitions

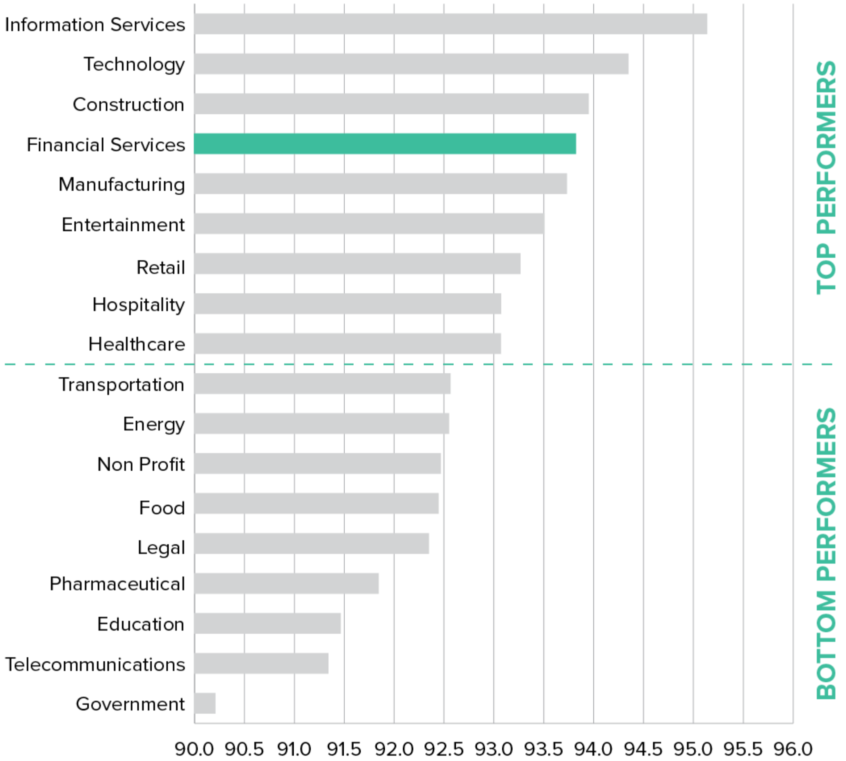
[1] As of 07/05/2016

Financial Services Security Compared to Other Major Industries

According to Homeland Security Research's U.S Financial Services: Cybersecurity Systems & Services Market report, the U.S. financial institution's cybersecurity market is the largest and fastest growing in the private sector, predicted to grow to $68 billion by 2020. Major financial institutions JPMorgan Chase & Co., Bank of America, Citigroup and Wells Fargo spend a collective $1.5 billion on cybersecurity annually.

We found that the U.S. financial industry cybersecurity ranks no. 4 out of 18 of the U.S. economy's primary industries.

FIGURE 1 Security Rating By Industry

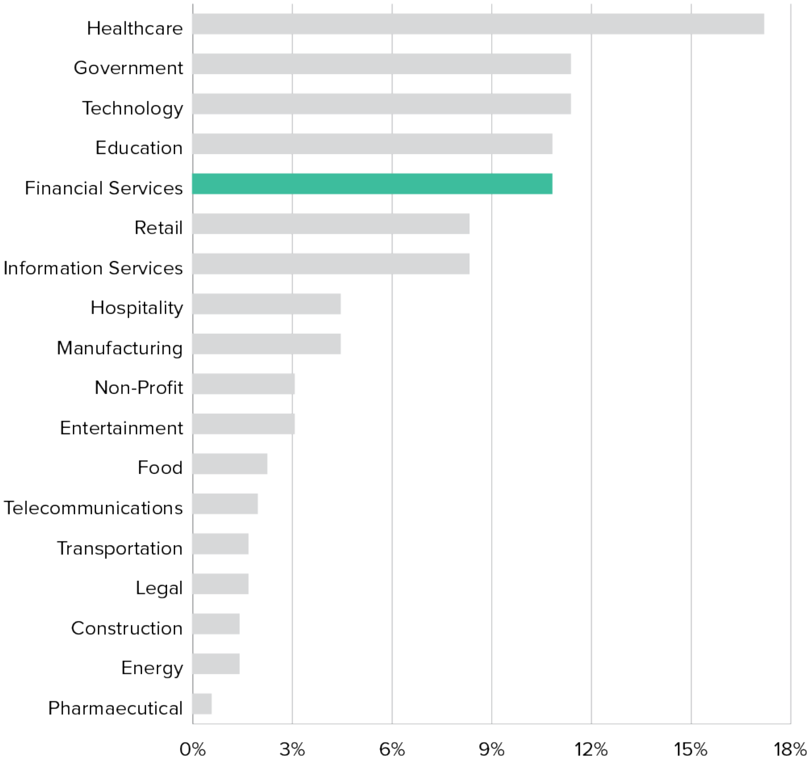


Although the financial industry ranks among the top performing industries for cybersecurity, its Cubit Score, DNS Health score, IP Reputation score and Network Security score are below the overall average for other industries. Based on our previous research, we found that companies with low IP Reputation scores are over three times more likely to experience a data breach compared to companies with a high IP reputation score.

Financial Records Targeted for Cybercrime

SecurityScorecard analyzed 361 international companies breached between June 2015 and April 2016. More than 10 percent were financial services organizations.

FIGURE 2 Percentage of Major Data Breaches by Industry, April 2015 - June 2016

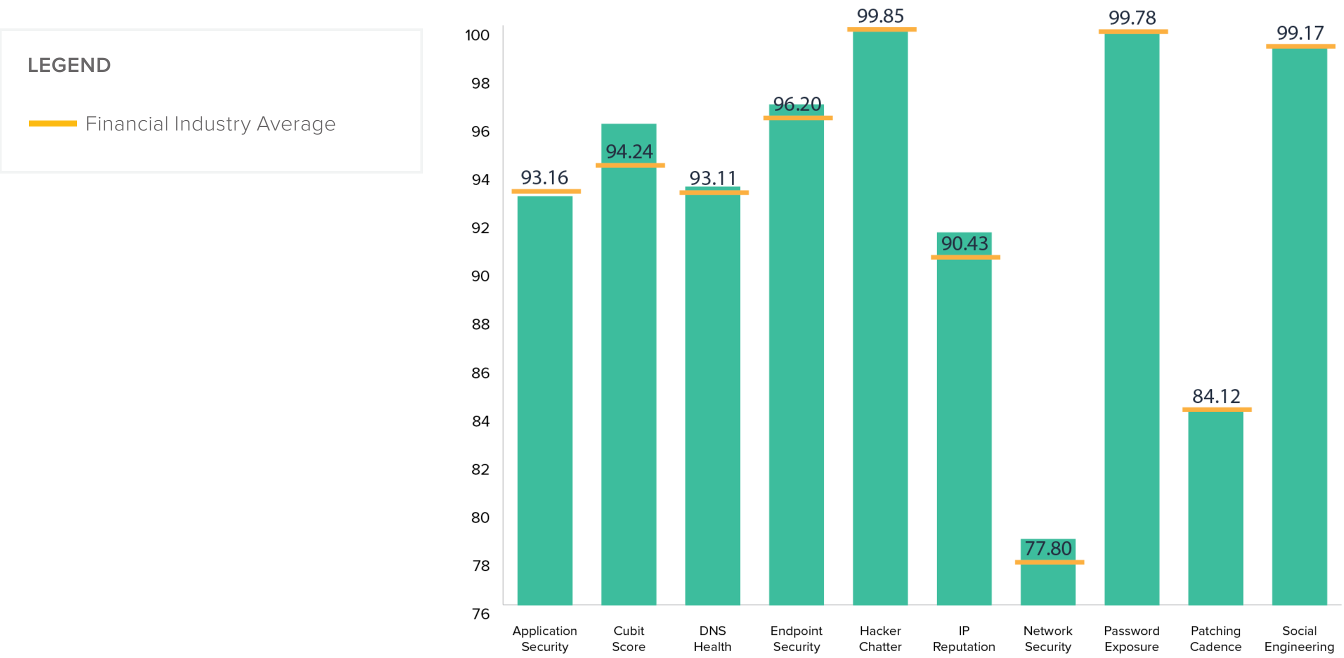


% of Total Companies Experienced Data Breaches during June 2015 to April 2016

Major Vulnerabilities Consistent Across Financial Industry

Of the 7,111 financial services companies assessed by SecurityScorecard, 1,356 show at least one CVE (Common Vulnerabilities and Exposures) unpatched. 72 percent of these companies are vulnerable to CVE 2014-3566 [POODLE], 38 percent are vulnerable to CVE 2016-0800 [DROWN], and 23 percent are vulnerable to CVE 2015-0204 [FREAK]. These common CVEs represent issues with SSL configuration.

FIGURE 3 Financial Industry Security Performance Compared to All Industries



Growth Strategies May Put Major U.S. Commercial Banks at Risk

Legacy systems continue to provide challenges to cybersecurity. As banks continue to grow through acquisition, legacy systems from the acquired organization—and the vulnerabilities that come with them—can remain in place for years.

The FDIC has noted that regulation such as 'Too Big to Fail' has encouraged a flurry of M&A activity among the larger banks looking to grow or maintain their status and, as such, protection under the law. During M&A transactions, legacy IT infrastructure and staff are absorbed into the buying organization resulting in chaos and confusion. These older systems might not be updated and secured for an extended period of time resulting in extensive vulnerabilities despite over half of the synergies available in a merger being IT-related, according to McKinsey. The FDIC requires an audit when a bank's status, size or system is changed. It was noted that the IT systems of larger banks have not responded well to these M&A activities as indicated in the table below.

Financial institutions should take an IT department's perspective into account more heavily on any M&A targets, looking at, in addition to other factors, ease of integration, infrastructure compatibility, scope of merging architecture, and the target's security posture.

SecurityScorecard Results for Top 20 U.S Banks Based on Revenue

The table below shows the 10 critical security category grades for the top 20 U.S Commercial Banks by Revenue. **These findings show that the bank with the weakest security posture is one of the top 10 largest financial service organizations in the U.S (by revenue).**

FIGURE 4 Security Posture of the 20 Largest US Commercial Banks in order of Total Score

Bank	Application Security	DNS Helath	Hacker Chatter	IP Reputation	Network Security	Endpoint Security	Patching Cadence	Password Exposure	Cubit Score	Social Engineering	Total Score
Bank 1	A	A	A	C	D	A	A	A	A	B	A
Bank 2	A	A	A	B	F	F	A	A	A	B	A
Bank 3	A	B	A	C	C	A	B	A	A	C	A
Bank 4	B	B	A	B	D	A	A	A	A	A	A
Bank 5	F	A	A	A	A	A	A	A	A	B	A
Bank 6	B	B	A	A	C	A	A	A	A	A	A
Bank 7	A	A	A	C	F	A	D	A	A	A	B
Bank 8	A	A	A	D	D	B	F	A	A	A	B
Bank 9	B	B	A	F	D	A	B	C	A	A	B
Bank 10	F	A	A	B	D	B	F	B	A	A	B
Bank 11	A	A	B	D	D	A	F	A	A	A	B
Bank 12	A	A	A	F	F	B	B	A	A	A	B
Bank 13	A	A	D	B	F	D	B	A	A	B	B
Bank 14	D	B	A	A	D	A	D	C	A	B	B
Bank 15	F	B	A	F	D	C	C	A	A	A	B
Bank 16	A	B	A	B	D	A	F	A	A	A	B
Bank 17	D	A	A	B	F	C	F	A	A	D	B
Bank 18	A	A	A	D	F	D	F	A	A	A	B
Bank 19	A	B	A	D	F	A	F	A	A	C	B
Bank 20	F	A	A	F	F	A	C	C	A	C	C

Among the top 20 U.S. commercial banks, 19 have a Network Security grade of 'C' or below.

- **Specific Issues:**
  - 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

These network security issues are all vulnerable attack vectors leaving commercial banks open to man-in-the-middle attacks (MITM) and brute-forcing credentials. In the case of expired SSL certificates, users are often likely to click through security warnings that inform them of these expired certificates, making them more susceptible to phishing sites. Due to the large infrastructure banks tend to have, auditing networks are a tedious process, but in order to reduce the total surface area of potential attack, banks need to keep their networks audited, secured, and updated.

> “We detected malware in nearly half of the largest 20 US Commercial banks over the previous 30 days*”

Among the top 20 U.S. commercial banks, 17 of them have an IP Reputation grade of 'B' or below.

- **Specific Issues:**
  - 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
  - We detected malware events 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.

All top 20 U.S. commercial banks received an 'A' in Cubit Score™.

Top Performing U.S. Investment Banks and Asset Management Firms

FIGURE 5 Top 10 Asset Management Firms with the Strongest Security Posture

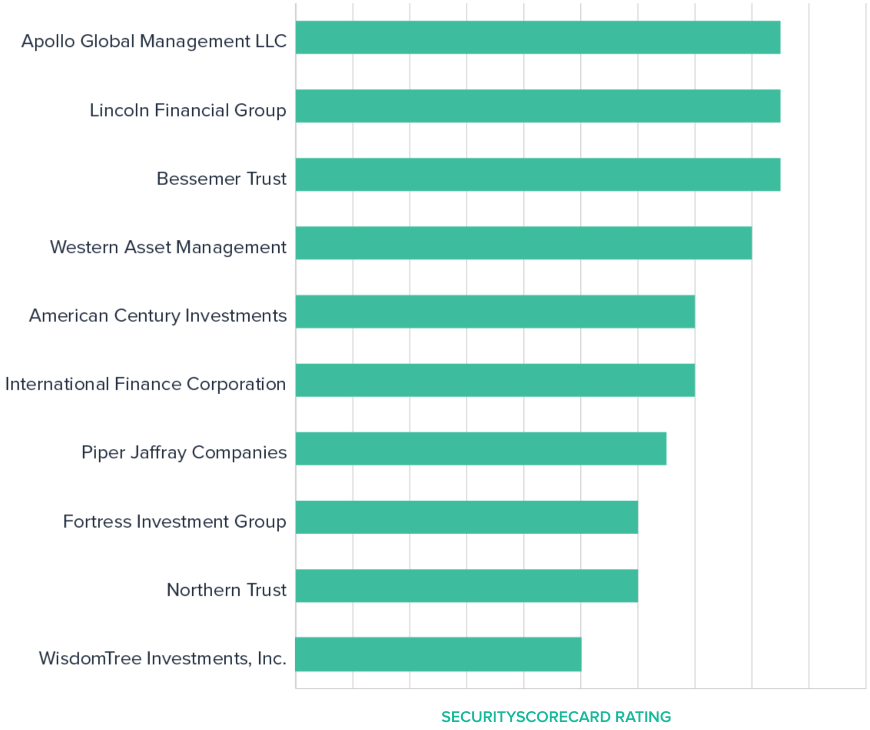
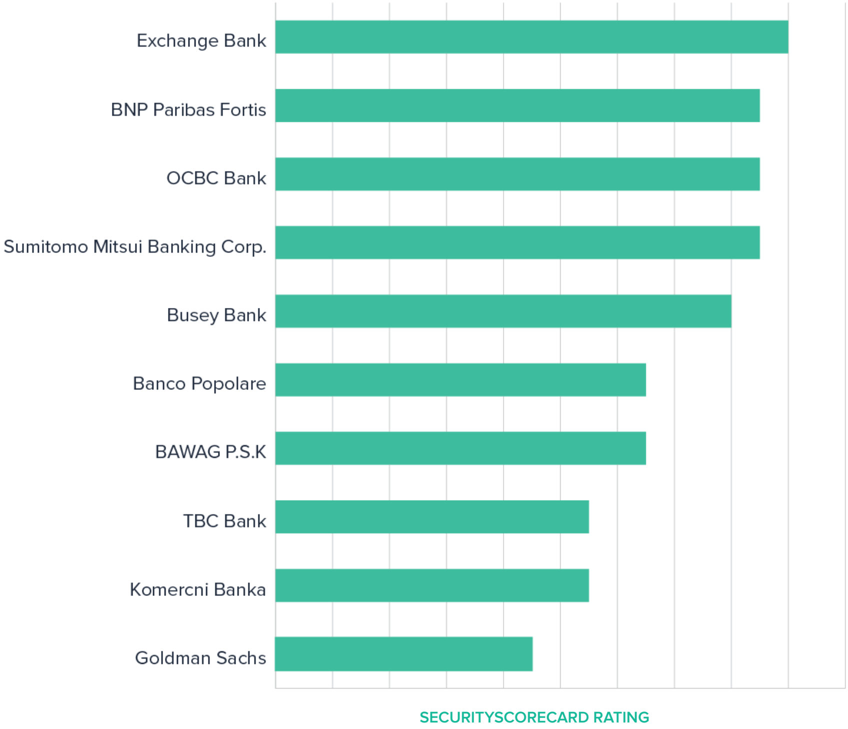


FIGURE 6 Top 10 Investment Banks with the Strongest Security Posture



The top performers for both investment banks and asset management firms excelled in the Social Engineering factor, one of the more volatile risk vectors for companies.

The top performing asset management firms struggled in the Network Security factor, receiving a mix of A, B, and D grades across the top 10. As mentioned earlier in our analysis of the top 20 commercial banks, a low Network Security score is associated with open ports, weak SSL certificate security, and insecure ciphers that may leave networks vulnerable to MITM attacks and brute-force attacks.

Even top performing investment banks scored low in Patching Cadence. While half received an 'A', three firms received a 'D', suggesting a lack of priority on patching CVEs. As noted in the Verizon Data Breach report, not only are CVEs being exploited sooner post-publication, older CVEs are also commonly exploited by hackers. Any unpatched CVE poses a security risk, one that increases as more time passes between publication and patch implementation.

> “Any unpatched CVE poses a security risk that increases as time passes”

Bottom Performing U.S. Investment Banks & Asset Management Firms

The top four most common vulnerabilities found in 399 investment banks and asset management firms are:

- **CVE-2014-3566:** Support of weak CBC ciphers in SSLv3.
  Known as Padding Oracle on Downgraded Legacy Exports (POODLE) is shared by 52 percent of U.S. investment banks and asset managements.

- **CVE-2016-0204:** Support of weak export-grade ciphers which can allow for a downgrade attack.
  Known as Factoring RSA Export Keys (FREAK) is shared by 29 percent of investment banks and asset management firms.

- **CVE-2016-0800:** Support of SSLv2, an obsolete protocol whose encryption can be compromised.
  Known as Decrypting RSA Using Obsolete Weakened Encryption (DROWN) is shared by 27 percent of investment banks and asset management firms.

- **End-of-life:** 57 percent of investment financial organizations that were breached were actively using end-of-life products at the time of the breach.

FIGURE 7 Top 10 Investment Banks with the Weakest Security Posture

Bank	Application Security	DNS Health	IP Reputation	Network Security	Endpoint Security	Hacker Chatter	Password Exposure	Cubit Score	Patching Cadence	Social Engineering	Total Grade	Total Score
Bank 1	F	A	F	F	A	A	F	A	B	F	C	75
Bank 2	A	D	D	F	F	A	D	A	F	F	C	78
Bank 3	B	C	A	D	A	A	F	A	D	F	B	80
Bank 4	B	C	F	D	A	A	F	A	C	A	B	81
Bank 5	D	B	C	F	A	A	A	A	F	B	B	82
Bank 6	A	C	D	F	A	A	A	A	F	D	B	82
Bank 7	A	B	C	D	B	B	A	A	F	F	B	83
Bank 8	D	A	D	C	A	A	C	A	D	A	B	84
Bank 9	A	B	F	D	F	A	D	A	A	A	B	86
Bank 10	B	C	D	C	A	A	A	A	D	A	B	87

FIGURE 8 Top 10 Asset Management Firms with the Weakest Security Posture

Bank	Application Security	DNS Health	IP Reputation	Network Security	Endpoint Security	Hacker Chatter	Password Exposure	Cubit Score	Patching Cadence	Social Engineering	Total Grade	Total Score
Bank 1	F	A	D	F	B	A	F	A	B	A	B	81
Bank 2	D	B	C	D	F	A	D	A	D	A	B	82
Bank 3	C	B	B	C	B	A	F	A	F	A	B	85
Bank 4	B	C	F	D	F	A	A	A	C	D	B	83
Bank 5	F	C	B	F	A	A	A	A	C	A	B	85
Bank 6	A	B	A	F	B	A	A	A	F	F	B	85
Bank 7	B	A	B	F	C	A	C	A	D	A	B	86
Bank 8	A	C	A	F	F	A	C	A	C	B	B	87
Bank 9	A	A	A	C	A	A	F	A	A	F	B	87
Bank 10	C	C	C	B	C	A	A	A	C	A	B	88

> “Half of the bottom performing Asset Management firms received an ‘F’ in Network Security”

Network Security and Patching Cadence are also areas low performers struggle with, whether they are asset management firms or investment banks. Half of the lowest performing Asset Management Firms received an ‘F’ in Network Security, and only one received an ‘A’ in Patching Cadence. Investment Banks fared similarly - 40% of the bottom performers received an ‘F’ in Network Security and, again, only one received an ‘A’ in Patching Cadence. However, it is worth noting that all the bottom performers have high marks of ‘A’ across the board on the Cubit Score factor.

The struggle with patching cadence, which is a measure of how often organizations are applying patches to fix vulnerabilities is an issue of patch management. Existing standards require the organization to test patches before pushing them out to the organization’s network. A high proportion of organizations can have some CVEs outstanding or in test, leaving their networks vulnerable.

Maintaining ongoing patch management is necessary for a successful vulnerability management program because unpatched systems are a leading source of vulnerabilities leveraged by cybercriminals. Patching issues arise when legacy systems are no longer supported by application providers, when mainstream operating systems reach end-of-service, and when organizations fail to keep up with the upgrade cadence set by manufacturers. Cybercriminals will constantly test a network's external perimeters seeking detectable weaknesses. When a weakness is found, it can be exploited through simple but persistent infiltration techniques. Audit requirements demand that organizations test patches on larger systems prior to implementation, adding to the tester's workload despite the requirement that patches be implemented in a timely manner.

> “Cybercriminals will constantly test a network seeking weaknesses”

Firewalls and other security devices on the perimeter of networks are regularly found to be unpatched due to a lack of registration, which causes the device's security capabilities to expire. This could be a result of the IT refresh cycle shrinking from three years to 18 months. As manufacturers develop faster and more reliable servers and other computer hardware, companies are pressured to replace older hardware in order to reap the benefits. However, manufacturers are releasing these updates more frequently, which increases the risk for human error or for IT managers to skip an update and wait for the next one.

Financial Industry Not Compliant With SIG, SIG Light, PCI and ISO Security Standards

SecurityScorecard analyzed 7,111 financial services for adherence to compliance standards in May 2016. The standards analyzed for include:

- ISO 27000 Series
- Standard Information Gathering Questionnaire (SIG)
- Standard Information Gathering Questionnaire subset (SIG Lite)
- Payment Card Industry Data Security Standard (PCI DSS)

Financial institutions that fail to adopt standards such as ISO and SIG can find themselves facing significant fines if breached due to a lack of a formal Information Security Management System (ISMS). Each regulatory board has its own way of determining fines, which can include fines for noncompliance per regulator, fines per record lost for each standard such as FFIEC, PCI or HIPAA, the costs of a forensic audit, remediation costs, audits by regulators that are conducted with a higher level of scrutiny, and lawsuits from data owners such as employees, customers, partners, and class action lawsuits. Regulatory standards are more stringent than the organization's own ISMS, but in the highly regulated financial industry, such standards are the norm.

FIGURE 9 The most common non-compliant ISO, SIG, and SIGLITE responses from finance companies

LEGEND

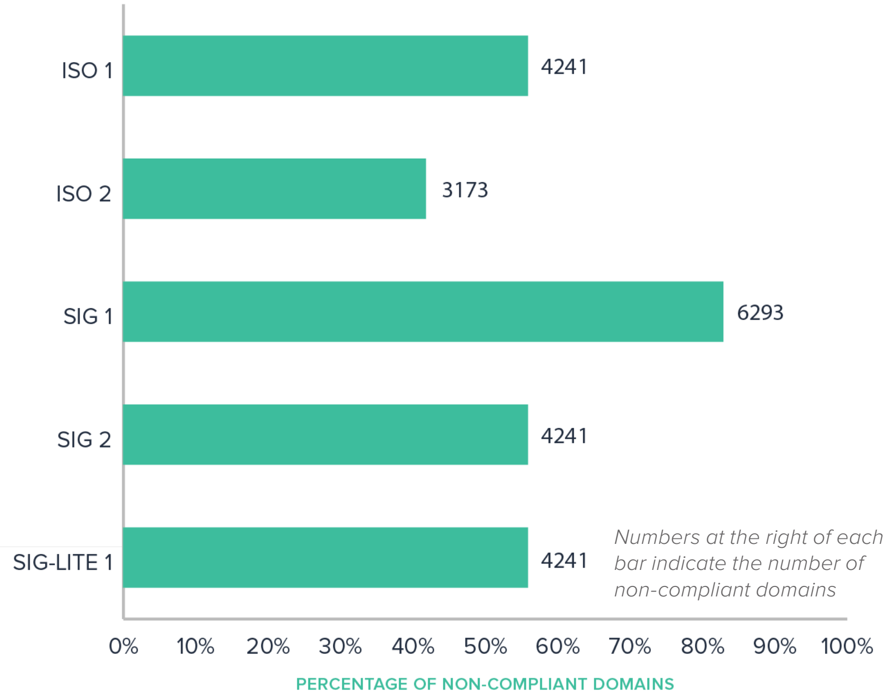
ISO 1 Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements

ISO 2 Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

SIG 1 May not have an information security policy based on detected open ports, SPF issues and/or DNS misconfiguration

SIG 2 Is there an approval process for the ports allowed through the network devices?

SIG-LITE 1 Issue types associated with having external network connection (Internet, Intranet, Extranet, etc.)



Numbers at the right of each bar indicate the number of non-compliant domains

Common issues linked to the compliance questions such as SIG 1 and SIG-LITE 1 that impacted the financial industry were the detection of open ports, which can increase the attack surface of an organization and is an indicator of improper network maintenance and DNS and SPF misconfiguration, which puts organizations at risk for spoofing.

Overall, these questions correspond to issue types report by the the Network Security, IP Reputation, and DNS Health factor scores, which is not surprising as Network Security and IP Reputation are the factors that the finance industry are struggling with the most. Our platform found a number of open ports, misconfigured email SPF, which can be exploited by attackers to send emails from spoofed addresses, malware events, and improper DNS configuration on a large majority of the financial industry domains as seen in the graph above.

FIGURE 10 The most common non-compliant PCI responses by finance companies[2]

LEGEND

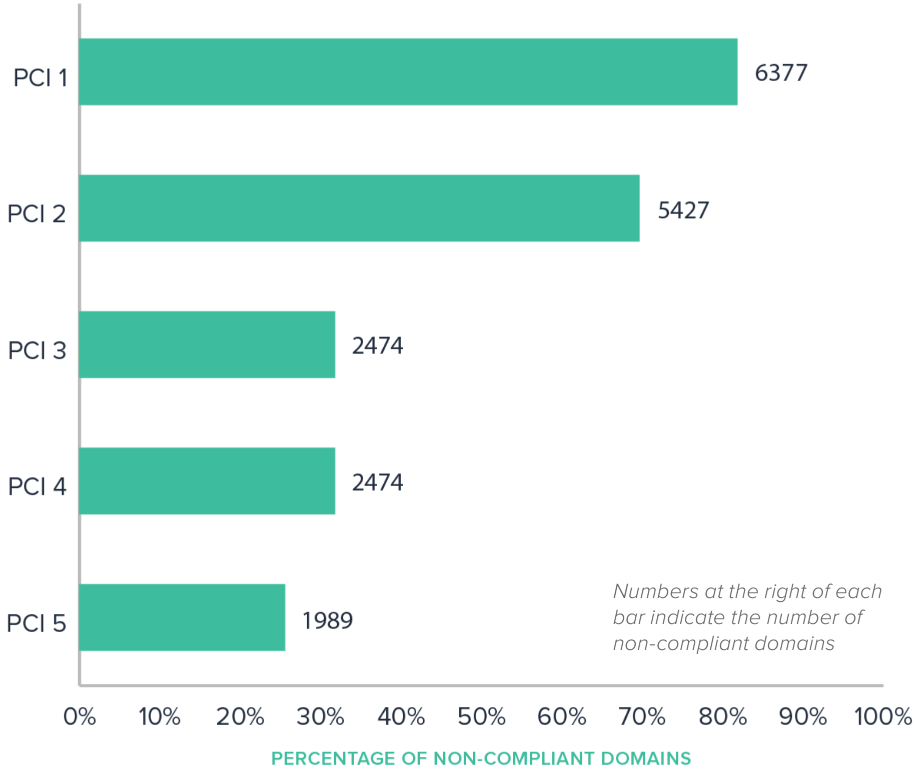
PCI 1 Issue types associated with authentication for use of the technology [general information security]

PCI 2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

PCI 3 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use.

PCI 4 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.

PCI 5 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.



Numbers at the right of each bar indicate the number of non-compliant domains

For questions such as PCI 1 that are wide-reaching, we associated issues linked to email and domain configuration such as SPF, DNS, and DKIM setup. Missing or improperly configured email and domain setup weaken the authenticity of an organization, allowing hackers to use spoofed email addresses in spam or spear-phishing campaigns.

The majority of the issues found within the PCI standard involved many of the same security factors as the other standards as well as Patching Cadence, Application Security, and more Network Security vulnerabilities such as weak cipher support, expired or self-signed SSL certificates, and a detection of a slow patching cadence suggesting these financial institutions are not updating vulnerable programs or software as soon as they should be.

[2] As of 07/13/2016

Financial Industry Susceptible to Breach Through Third-Party Vendor Ecosystem

> “
> Common essential service providers used by financial institutions have received an ‘F’ in Patching Cadence
> ”

SecurityScorecard assessed 7,111 financial services companies and determined the most commonly used third-party vendors, their grades, and their most significant vulnerabilities.

- 18 percent of financial services companies use a popular email service that has received a grade of ‘F’ in Patching Cadence, Network Security, and IP Reputation; and a grade of ‘D’ in Hacker Chatter and Social Engineering
- 16 percent use an enterprise cloud storage provider that has received a grade of ‘F’ in Patching Cadence and a grade of ‘D’ in Network Security and IP Reputation.
- 14 percent use a domain registering and web hosting provider, among other things that has received a grade an ‘F’ in Patching Cadence and ‘D’ in Application Security, Password Exposure and Cubit Score^{TM}

All three third party vendors provide essential services to these banks and replacing them would be an arduous task given the amount of users and dependencies for each third party vendor. Due to the critical nature of these providers, replacing them may take years or impact the institution too negatively for a replacement to be worth the effort.

Instead, banks and other enterprises utilizing these services and others like them should vet their vendor’s security posture and understand what systems and data will be integrated or hosted with these vendors to ensure access is as minimal as possible and that there are processes in place to react quickly should a data breach occur.

Financial Institutions Suffered 22 Major Publicly Disclosed Data Breaches Over the Past Year

1. Central Bank of Russia
2. Citizens Bank
3. Coast Central Credit Union
4. Educators Credit Union
5. E*TRADE Financial Corporation
6. First National Bank of Omaha
7. FXCM
8. Golden 1 Credit Union
9. Hawaii First Federal Credit Union
10. Invest NI
11. Woodbury Financial Services
12. Lloyds Bank
13. Moneytree
14. Nationstar Mortgage
15. Permanent TSB
16. Santander Bank
17. Charles Schwab
18. Scient Federal Credit Union
19. Scottrade
20. TD Bank
21. The Money Shop
22. Bangladesh Bank

Data Breach Analysis

Scottrade disclosed details of their breach in October 2015. Contact information, email addresses, and Social Security numbers, in some cases, were compromised for over 4.6 million customers. A check on their SecurityScorecard grade reveals details on Scottrade's security flaws.

We found multiple SSL and TLS network issues, detected an out of date browser in use, and found that one of their domains lacked an SPF record. These are all vulnerable attack points that a malicious actor can take advantage of to infiltrate a system. However, we should note that over the past six months, Scottrade has improved their security score from a low B to a high B.

Charles Schwab recently suffered through a small data breach in May 2016 when an unauthorized person logged into a number of user accounts, exposing client's names, account numbers, stock positions, and transaction history. Charles Schwab has maintained that the credentials used to log-in were not the result of a vulnerability within Charles Schwab and instead were likely taken from a different source.

This is an issue that is becoming more and more common since the massive 2012 LinkedIn data breach recently surfaced again, where over 100 million user accounts and passwords were leaked. Because of the huge amount of user account and password details being released, malicious actors may be able to use the leaked data and attempt to log into other company databases using an automated system. For this reason, many companies have pre-emptively reset user passwords that may be linked to the data breach. Unfortunately, for companies that haven't done so, they remain vulnerable to similar attacks that led to the Charles Schwab breach.

The Central Bank of Bangladesh was hacked by a sophisticated team of hackers who infiltrated the bank's network, installed credential-stealing malware, and were able to obtain log-in credentials to the Society for Worldwide Interbank Financial Telecommunications network (SWIFT) a messaging network used by financial institutions to transmit information. This allowed the hackers to steal over $80 million dollars.

Details surrounding the hack have been emerging every week and SWIFT maintains that their systems have not been compromised. But as a response, SWIFT will lay out a collaborative five-step plan aimed to bolster security for all parties involved. However, there have been a number of new security incidents involving banks that have the same pattern of attack as the Bangladesh Bank hack and SWIFT has warned that if financial institutions do not improve their security, more attacks will occur.

Conclusion

While financial institutions are often the most up to date and focused on information security, this report shows that there is a lot of room for improvement, especially for larger financial institutions and their third party vendors. Financial institutions have a high risk of data breaches due to the increase in targeting and because successful attacks reap huge benefits. As the 2016 Verizon Data Breach noted, the finance industry ranked #1 for security incidents with confirmed data loss.

Unfortunately, the financial industry has a lot to catching up to do when it comes to cybersecurity risks. Ransomware is evolving quicker than ever, the use of legacy IT systems will continue to hurt financial institutions and new attack methods related to third party vendors and partners pose different risks financial institutions need to account for. The Bangladesh Bank Hack resulted in over $100 million lost to hackers and the ensuing fallout continues to afflict banks and breaches as seen in the Charles Schwab case will increase given the large amount of leaked data that resulted from the resurfaced 2012 major LinkedIn data breach.

> “
>
> The finance industry has suffered the most security incidents with data loss
>
> 2016 Verizon Data Breach Report
>
> ”

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, there is promising news in the financial sector. As noted before, SWIFT is already making efforts to improve cybersecurity and educate banks on how to maintain a secure network. The OCC has increasingly focused on third-party vendors in its standards on security and the SEC chair, Mary Jo White, famously announced that cybercrime is the most pressing threat to global financial systems at the Reuters Financial Regulation Summit in May. The increasing focus on cybercrime and information security will spur financial institutions to take a stronger look at their security posture, their vendor's security and make strides in third party risk management and proper security assessments.

Want To Know Your Company's Score Right Now?

Discover how hackers, partners, and customers see you from the outside

For a free instant security scorecard please visit

instant.securityscorecard.com

Key Terms

Application Security

SecurityScorecard uses security testing techniques to scour for vulnerabilities in applications that leave an organization open to exploitation. Web servers and services used to host applications and versions of those services are identified to ensure they are up to date. By combining a detailed knowledge of software vulnerabilities with service versions, SecurityScorecard can identify insecure technology being used to host applications.

Cubit™ Score

Cubit Score is SecurityScorecard's proprietary threat indicator. It rates organizations based on a targeted collection of security issues specific to that business. Cubit reviews all security signals and identifies the ones most vulnerable to hackers, including examples such as admin subdomains exposed by public-facing DNS records, blacklisted IPs, spam-generating IPs, IPs hosting malicious executables and configurations displaying personal information about system administrators.

Common Vulnerabilities and Exposures (CVE)

An international catalog of publicly known information security vulnerabilities and exposures.

IP Reputation

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.

Password Exposure

Passwords that are exposed as part of data leaks, key logger dumps, database dumps and other types of exposure are identified. SecurityScorecard ties the credentials back to companies that own the exposed email accounts, allowing clients to see where employees have left their organizations exposed.

Network Security

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.

Patching Cadence

SecurityScorecard surveys scans ports and crawls sites to gather information relative to the versions of software and hardware in use by an organization. If there are vulnerabilities, such as an end-of-life software that can no longer be patched, or unpatched CVEs such as POODLE, FREAK, DROWN, or Heartbleed, SecurityScorecard notes and tracks the vulnerability.

Social Engineering

SecurityScorecard identifies multiple factors related to social engineering such as employees using corporate account information in social networks; employees exposing an organization to phishing attacks and span; and employees posting negative reviews of the business to social platforms.

ISO

The International Standards Organization publishes the leading information security standard ISO 27001, used by Financial Organizations as an (ISMS) Information Security Management System. ISO is the basis from which many other standards are based such as NIST and PCI. ISO standards are updated infrequently.

Standardized Information Gathering

The Standardized Information Gathering (SIG), another standard by which IT risk is assessed for internal projects and third-party vendors. SIG standards are updated annually in both a Lite and Full version.

About SecurityScorecard

SecurityScorecard provides the most accurate rating of security risk for any organization worldwide. The proprietary cloud platform helps enterprises gain operational command of the security posture for themselves and across all of their partners and vendors. The platform offers a breadth and depth of critical data points not available from any other service provider and in a completely self-service and automated tool. The platform provides continuous, non-intrusive monitoring for any organization including third and fourth parties. Security posture is assessed and measured non-intrusively across a broad range of risk categories such as Application Security, Malware, Patching Cadence, Network Security, Hacker Chatter, Social Engineering and Passwords Exposed.

To receive an email with your company's current score, please visit instant.securityscorecard.com.

www.securityscorecard.com
1 (800) 682-1707
info@securityscorecard.com
@security_score

SecurityScorecard HQ
22 W 19th St. 9th FL
New York, NY 10011