In July 2015, hackers stole social security numbers, health data, and other highly sensitive data from 21 million Americans through the Office of Personnel Management in what, at the time, was the largest data breach in U.S. history. As a response, U.S. government agencies committed to making significant efforts to reinforce and expand existing security measures. SecurityScorecard wanted to find out if these government agencies were successful in their commitment.

In February 2016, SecurityScorecard analyzed and graded the current security postures of 600 local, state, and federal government organizations, each with more than 1,000 public-facing IP addresses, to determine the strongest and weakest security standards based on security hygiene and security reaction time compared to their peers. The data used was derived from SecurityScorecard’s proprietary benchmarking platform ThreatMarket™ and aggregated from more than 30 million daily security-risk signals and sensors.

SecurityScorecard also analyzed the specific scores of NASA, FBI, and the IRS, three major government organizations that fell victim to data breaches in early 2016.

1. Across all industries surveyed by SecurityScorecard, including transportation, retail, healthcare and more, government organizations received the lowest security scores. It tracked 35 major data breaches among all government organizations between April 2015 to April 2016.

2. Low-performing government organizations struggled the most with three categories of security measurements: Malware Infections, Network Security and Software Patching Cadence.

3. Within state organizations with a SecurityScorecard grade below a ‘B’, 90 percent scored an ‘F’ in Software patching cadence and 80 percent scored an ‘F’ in network security.

4. Among local organizations, 60 percent of low performers received an ‘F’ in Network security, 50 percent received an ‘F’ in Software Patching Cadence and 30 percent received an ‘F’ in IP Reputation(Malware).

5. NASA scored the worst among all 600 government organizations. Other bottom-performers include the US Department of State and the IT systems of Connecticut, Pennsylvania, and Washington.
A SecurityScorecard grade 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, SecurityScorecard takes a multidimensional approach to rating security. SecurityScorecard’s benchmarking platform grades 10 security categories comprised thousands of unique data points to determine a category score and then combines them into an individual score based on company score in the same industry.

When compared to the cybersecurity performance of 17 other major industries, government organizations ranked at the bottom of all major performers, coming in below information services, financial services, transportation and healthcare. This report identifies key network infrastructure weaknesses and vulnerabilities within government organizations on a local, state and federal level.
Key Terms

**Application Security**
SecurityScorecard uses non intrusive security testing techniques to scour for vulnerabilities in applications that leave an organization open to exploitation. Middle identification technology identifies web servers and services used to host applications and versions of those services. 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. Cubit also rates an organization’s vulnerability to the frequently targeted Heartbleed.

**Malware**
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 command and control servers. Researchers can then intercept the communication, which can be traced back to an IP address from which it’s emanating, indicating an infected network.

“We used a 1,000 IP address-threshold for two reasons,” said Dr. Luis Vargas, Data Scientist, SecurityScorecard. “We wanted a sizable collection to limit the effects of outliers, for example, honeypots running on a small subset of IPs on a shared range. Having at least 1,000 IPs means that a few outliers wouldn’t strongly bias scores if those IPs had lots of bad signals emanating from them.”
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.

Password Exposure
Passwords that are exposed as part of data leaks, keylogger 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.

Patching Cadence
Security Scorecard 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, SecurityScorecard notes and tracks the vulnerability.

"Patching cadence can be an indicator of security posture maturity by providing insight into how long weaknesses are visible and ultimately, how long they take to fix," said Dr. Vargas.

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 spam, and employees posting negative reviews of the business to social platforms.
Top & Bottom Performers (Combined Local, State and Federal)

Malware and Network Security showed potential challenges to security performance among top performers.

Consistencies in security performance were established across the top government performers, which included federal, state and local organizations. Areas of strength across high performers includes high scores in: Application Security, DNS Health, Hacker Chatter, Endpoint Security, Patching Cadence, Password Exposure, Cubit Score and Social Engineering.

Malware and Network Security showed potential challenges to security performance among top performers.
Federal Organizations

Among federal organizations with the weakest postures, their greatest vulnerabilities were within Network Security, Patching Cadence and Malware. For Network Security, 70 percent of low performers scored an ‘F’; on Patching Cadence, 20 percent received an ‘F’, and 10 percent received an ‘F’ in Malware.

Federal agencies may be susceptible to more risk due to the sheer size of their infrastructure, but in many cases, may be prepared to fare better against cybersecurity threats due to larger budgets and teams of security personnel.
Even top-performers saw fluctuations in their security postures for Malware and Network Security scores.

Even top-performers saw fluctuations in their security postures for Malware and Network Security scores, with several receiving scores of ‘D’ and ‘F,’ indicating the fluid nature of their security posture.

Among federal organizations with a high security posture, top strengths included Application Security, Password Exposure, Cubit Score and Social Engineering. Strength in these areas indicate that an organization has website security monitoring and security awareness training in place to ensure employees are not using government credentials with external third-party software or exposing sensitive data. This requires clear communications and written policies that ensure the organization and every employee is up-to-date on the ever-increasing exploits to which they could be exposed.
Among low-performing state organizations, 90 percent scored an ‘F’ in Patching Cadence and 80 percent scored an ‘F’ in Network Security.

Top-performing state organizations scored consistently well in Endpoint Security, Password Exposure, Cubit Score and Social Engineering.
Fluctuations occurred even in top-performing states, in IP Reputation, Network Security and Patching Cadence scores. Because SecurityScorecard’s monitoring is constant, it can expose vulnerabilities over the lifetime of a security system. In addition, government agencies, federal, state and local, often retain legacy systems longer than business and other private organizations, increasing their exposure to threat in these areas.

Local Organizations

Low-performing local organizations struggled the most with Network Security, with 60 percent receiving an ‘F;’ Patching Cadence, where 50 percent received an ‘F;’ and IP Reputation, where 30 percent received an ‘F.’
Top-performing local organizations scored consistently well in Application Security, Hacker Chatter, Password Exposure, Cubit Score and Social Engineering, with the most pronounced fluctuating scores in Patching Cadence.
In order to understand the breadth and true risk involved within these government organizations, SecurityScorecard uncovered the major data breaches of the last twelve months and took a detailed look at the last 3 major breaches, namely NASA, FBI, and IRS, who had breaches in early 2016.

**Major Government Data Breaches from April 2015 to April 2016**

1. state.co.us
2. georgia.gov
3. irs.gov
4. ca.gov
5. opm.gov
6. army.mil
7. nationalguard.com
8. va.gov
9. state.gov
10. illinois.gov
11. mn.gov
12. colorado.gov
13. az.gov
14. amherstohio.org
15. state.md.us
16. whs.mil
17. vermont.gov
18. state.tx.us
19. laems.net
20. flgov.com
21. nyc.gov
22. brunswickme.org
23. floridahealth.gov
24. slco.org
25. myflfamilies.com
26. dentoncounty.com
27. tchhsa.org
28. gsa.gov
29. itsmarta.com
30. ncdhhs.gov
31. fws.gov
32. nasa.gov
33. dhs.gov
34. fbi.gov
35. lacounty.gov
NASA's scores ranged from mid-level ‘C’ to mid-level ‘D’ scores since October 2015, nearing the top of the ‘C’ range in the month of February 2016. However, their scores dropped by 10% before the data breach in mid-February was reported and dropped further, dipping into the ‘D’ range, after the breach. Since then, there have been slight improvements to their cybersecurity but they still have the lowest score among government organizations since the first week of March.

NASA’s primary threat indicators include a large number of detected malware signatures over the past 30 days, tracked P2P activity, various SSL certificate issues, and insecure open ports, varying from IMAP to Telnet to DB ports among others. Their Email SPF seems to be misconfigured, which can lead to email spoofing. Secondary threat indicators include defacement mentions on hacker sites, at-risk credentials, usage of an end-of-service product, and vulnerability to high severity CVEs. This has led to NASA scoring an ‘F’ in the following factors: IP Reputation, Network Security, Patching Cadence, and a ‘C’ in DNS Health and Password Exposure.

Over the past six months, the FBI’s SecurityScorecard grade varied within the ‘B’ range, peaking in late January. However, the FBI’s score dramatically dropped two weeks prior to a breach reported in the second week of February. The score dropped to a ‘C’ and dropped further post-
breach. Since the breach, the FBI’s score has been on the rise, but is still fluctuating within the mediocre ‘C’ range.

Currently, the FBI has an ‘F’ in both IP Reputation and Network Security and a ‘C’ in Application Security and Endpoint Security. Primary threat indicators and vulnerabilities include open ports, various malware signatures found within the last 30 days, faulty SSL certificate security, out-of-date browser usage and many others. Secondary threat indicators include vulnerabilities to CVEs within the last thirty days and mentions in underground hacker forums which indicate towards potential future hacks or sensitive data being shared.

The IRS score fluctuated between a low ‘A’ and low ‘B’ scored from October 2015 on, peaking in late January. However, there was a dramatic rating drop in early February, where the IRS dropped 11 percent, their biggest fluctuation within a 6 month period. At the time the data breach was reported, in mid-February, the score dropped further, falling to a ‘C.’ Since then, the IRS’s score has steadily increased, indicating that efforts to improve their security have been effective.

Currently, the IRS has an ‘F’ in Network security, their worst-performing factor. The IRS has SSL certificate issues, which include expired certificates and the use of weak and/or insecure ciphers. Open ports on the IRS have also been identified, which may allows hackers to have unfettered access. There have also been leaked company emails matched to social networking sites and insecure security questions have been identified.
An effective remediation solution can include many variants and depends on the specific needs of the organization. Below are some suggested remediation tactics.

**To improve Patching Cadence:**

- Monitor Common Vulnerabilities and Exposures (CVE) lists and vulnerability repositories for code that could exploit an infrastructure.
- Get alerts to new exploits and vulnerabilities as they are released by subscribing to the BugTraq mailing list.
- Maintain a regular update schedule for all software and hardware used by the enterprise to ensure that patches are implemented as soon as they are released.
- Ensure each version of the software has been patched or updated to protect against known vulnerabilities.

**To improve IP Reputation:**

- Investigate devices connected to the identified IP addresses and check for evidence of malware infection.
- Institute persistent malware protection mechanisms by using current antivirus software.
- Use Intrusion Detection Software (IDS) or a Web Application Firewall (WAF) to monitor incoming and outgoing traffic for suspicious behavior.
- Block and blacklist any suspicious traffic and follow up by investigating malware incidents.
- Subscribe to Open-Source Intelligence (OSINT) malware feeds available to your organization.

**To improve Network Security:**

- Review the business necessity of open ports listed. Close any unnecessary ports and ensure remaining open ports are patched, require authentication, and are configured for security best practices.
- Ensure that all versions of services running on Internet-facing services are updated to latest versions.
• Implement an IP whitelist for access to open ports that restricts unauthorized access attempts from connecting through the Internet.

• Configure servers to support strong symmetric ciphers and use sufficiently large public key sizes.

• Avoid RC4 encryption. Multiple documented vulnerabilities have rendered it insecure.

• Confirm SSL certificates are current.

Conclusion

To ensure network and infrastructure security at every level and meet the government’s own National Institute of Standards and Technology (NIST) standards, government agencies must have a holistic view of their security postures and be able to assess both strengths and weaknesses in their systems over the course of time.

SecurityScorecard data indicates that while some government agencies across local, state, and federal organizations are improving their cybersecurity postures, there are still many risks and vulnerabilities yet to be addressed, especially at the larger federal level.

Government agencies should consider using outside resources to assist in examining vulnerabilities and developing plans for short and long-term remediation.
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
About SecurityScorecard

SecurityScorecard provides the most accurate benchmark of security risk across the entire business ecosystem. The cloud platform helps enterprises gain operational command of the security posture for themselves and across all their partners and vendors. It offers a breadth and depth of critical risk factors not available from any other service provider and in a completely self-service and automated tool. It’s based on the ThreatMarket™ data engine which collects over 30 million daily security risk signals from the entire Internet. SecurityScorecard was founded in 2013 by two former Chief Information Security Officers, Dr. Aleksandr Yampolskiy and Sam Kassoumeh. It is made up of veteran security researchers, cryptographers, data scientists, and software engineers. The company is privately held with headquarters in New York City. Security Scorecard investors include Sequoia Capital, Evolution Equity Partners, Boldstart Ventures, and others.

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