SecurityScorecard

2018 Government Cybersecurity Report

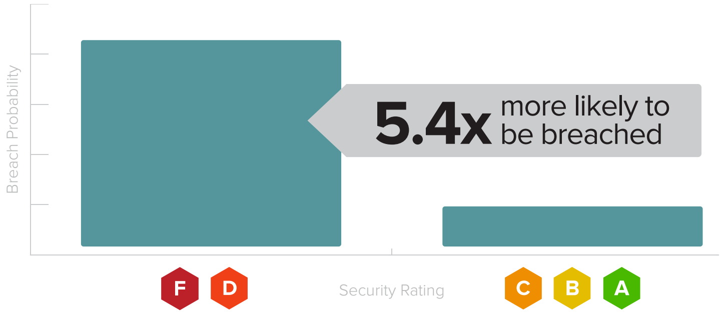
securityscorecard.com [800] 682 1707

Critical Infrastructure Vulnerabilities Shake Public Confidence

Throughout 2018, significant security weaknesses in federal, state, county, and municipal government agencies have left mission critical services, such as court systems, municipal utilities, bill payment services, traffic control systems, power grid systems, and voting registration infrastructures susceptible to cyberattacks.

The recent disclosures of successful attacks against governments and related critical infrastructures in mainstream news media have solidified the public perception of the importance of cybersecurity risk management. Attackers motivated by profit have been using ransomware as their tool of choice to target enterprises in both the public and private sectors. Attackers motivated by foreign state-sponsored goals often seek to exfiltrate data – such as when the federal government's Office of Personnel Management was breached and all security clearance records relating to security clearances were exfiltrated. In 2017, the game changed again with the release of the 'EquationGroup' hacking toolkit. (This toolkit contained a collection of zero-day exploits developed by the NSA which was stolen and leaked by adversaries.) This landscape was made even more complex when enterprises began rapidly implementing IoT technologies on top of existing infrastructure in an attempt to bring legacy analog hardware online for remote management.

Companies with a D or F are 5.4 times more likely to be breached.



The ultimate result of all these factors is a tangled web of legacy web applications, legacy network software, exposed network services, slow patching implementations, and a new vector of access and attack through IoT devices – leaving government agencies defending their infrastructures and applications with a difficult task.

Methodology

In early 2018, SecurityScorecard leveraged our proprietary platform to analyze and grade the current security postures of 655 local, state, and federal government organizations. Each scored entity contained over 100 public-facing IP addresses. More information about our scoring methodology can be found here.

A Look at the Cybersecurity Posture of U.S. Swing States

	Overall Rating	Endpoint Security	IP Reputation	Network Security	Patching Cadence
Florida	C	F	C	F	F
County in Florida	C	B	F	C	F
Ohio	C	F	D	F	D
County in Ohio	D	B	F	F	F
City in Michigan	D	B	F	F	F
Nevada	D	F	C	F	F
New Hampshire	D	A	F	F	F

Budget allocations for information security resources were supposed to have been provisioned over the last several years. By taking a snapshot of the current grades of swing states, we were able to observe whether these states have taken steps to implement basic enterprise cybersecurity controls.

The prominent visibility of swing state governments during election cycles will bring increased attention to their websites and internet resources. With that increased attention comes the inevitable increase of malicious users seeking to identify exploitable conditions to leverage in new creative ways.

Low grades in endpoint security, IP reputation, network security, and patching cadence are highly predictive indicators that an organization may have a higher probability of experiencing an imminent information security incident than on organization with high grades in these areas. All large enterprises will likely experience an information security incident – the differentiator in how much impact those incidents have is the speed of response to the incident, the remediation of the problem, and the implementation of mitigating controls to prevent repeat events.

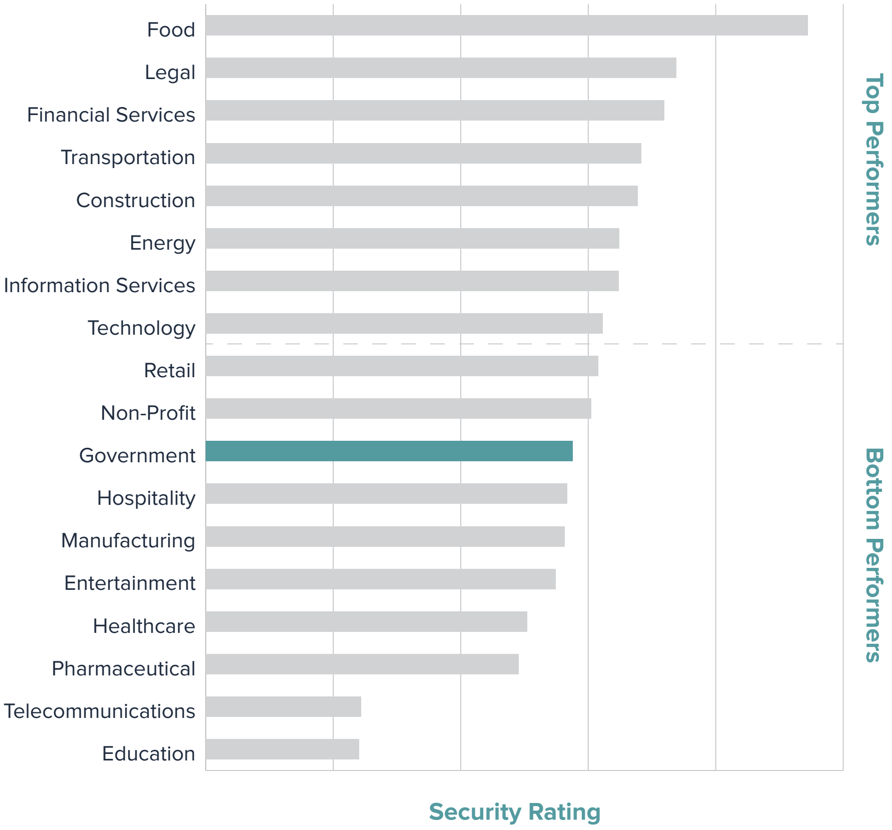
Why Government Agencies Struggle With Cybersecurity Year Round

Government organizations remain a primary target given the reams of personally identifiable information (PII) stored and processed by agencies, not to mention top-secret national security details. All the necessary components of critical infrastructure networks such as courts, traffic, public transportation, elections, and public utilities fall under the auspices of regional governments. Even 'small' governments can be huge, slow-moving bureaucracies with a mix of emerging technologies and a massive, highly vulnerable entrenched legacy infrastructure, all of which present a perfect storm for the modern hacker.

In nearly 60 percent of security incidents, it takes the government years to discover the breach.

On top of concerns about the proliferation of attacks and the irreparable damage they may cause, the cost associated with cyberattacks continues to escalate at a sobering rate. By 2019, the global cost of data breaches is projected to exceed $2 trillion annually, with a single breach costing more than $4 million, on average, according to Juniper Research.

Government vs. Other Major U.S. Industry Sectors



The government sector is strengthening its cyber defense. Compared to last year, the public sector moved up from third to last to nearly the middle of the pack, performing better than hospitality, manufacturing, entertainment, healthcare, and pharma, and ranking 11th among 18 major U.S. industry sectors with an overall "B" grade.

Top performers in 2018 in the government sector include many federal agencies that earned an "A" grade.

While the government's improvement in cybersecurity is a step in the right direction, it's essential to note that government scores again fell below average in several categories (see "Top Three Government Security Factor Weaknesses" below). Cybersecurity due diligence must remain a top priority.

Key Findings by Security Risk Factor in the Government Sector

This report identifies network infrastructure weaknesses within government organizations. In addition to the overall security posture ratings used for the industry comparison above, the SecurityScorecard team extracts and analyzes information specific to a broad range of security risk factors monitored by the platform. A SecurityScorecard rating (numeric score and letter grade) is a comprehensive indicator of relative cyber heath, calculated according to the severity of issues within each risk factor category, the level of risk (defined by industry standards), and the performance of comparable agencies. Within each security risk factor, a breadth of unique data points is scored and weighted. These data are then used to calculate the organization's overall rating.

Based on information gathered with our proprietary data engine—ThreatMarket™—and through other nonintrusive collection activities, SecurityScorecard analyzes risk factors in the following categories:

- Endpoint Security
- Network Security
- Patching Cadence
- DNS Health
- Social Engineering
- Web Application Security

- Leaked Credentials
- Hacker Chatter
- IP Reputation

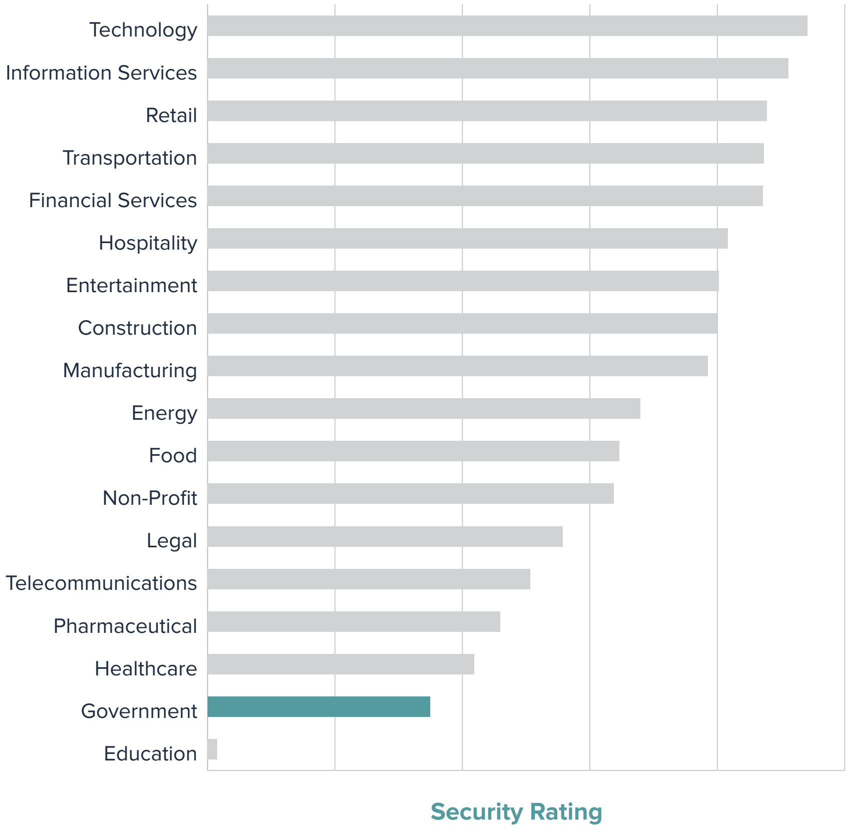
Top Three Government Security Factor Weaknesses

Organizations in all industries face mounting difficulties in tackling particular security issues. Government entities continue to be plagued by and perform especially poorly in Endpoint Security, Network Security, and Patching Cadence.

Endpoint Security

Endpoint Security refers to the protection of all laptops, desktops, and mobile devices that access the organization/agency network. Hackers, including those with limited programming experience, often use exploit kits to penetrate endpoint vulnerabilities.

SecurityScorecard detects endpoints running outdated and insecure browsers, operating systems, and software that warn of potential attack. One employee using an outdated operating system or browser can expose an entire organization to an unacceptable level of risk.



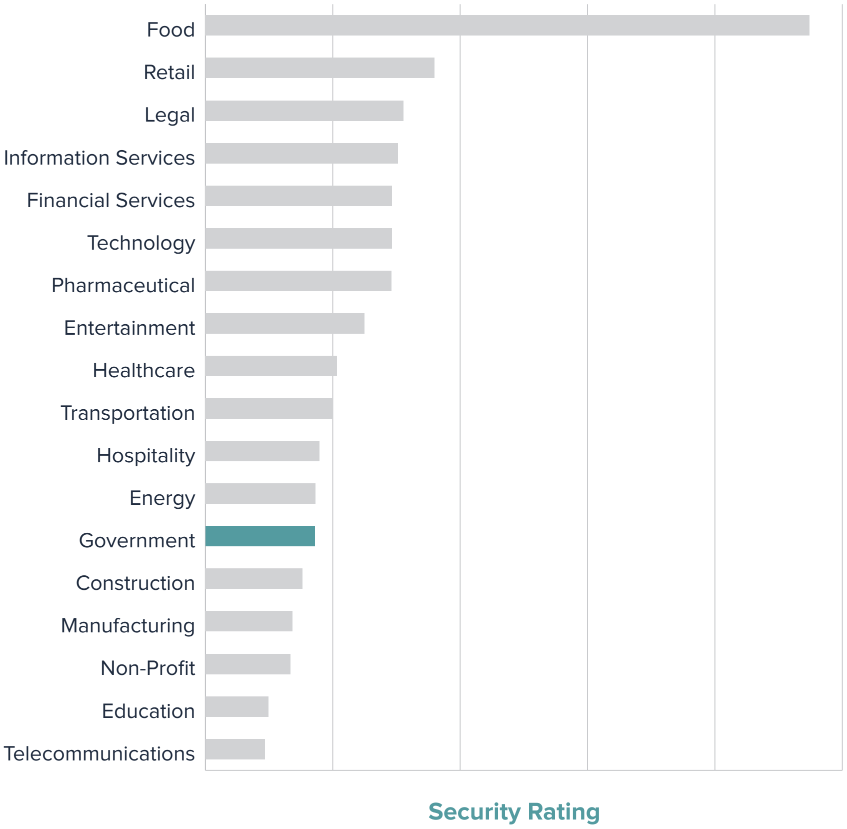
Exploit kit developers use black market sales campaigns to sell licensing and maintenance programs to hackers. They continue to evolve their products to evade detection by security defenders, achieve successful infection rates, and increase illegal profits. They deliver services that can be used by affiliates or distributors to extract extortion payments from victims.

Telstra Cyber Security Report 2017

The government sector remains second from the bottom compared to other industries in this category with a mid-B score, well below the average grade and down marginally from last year's relatively poor score. The persistent low score for this security factor indicates that government employees continue to use multiple outdated browsers and applications, likely because new versions are incompatible with legacy infrastructure that remains in place in many government organizations.

Network Security

Network Security involves securing and preventing, as necessary, external access to internal systems. Strong performance in this category requires deployment of advanced tools and technologies to safeguard against emerging threats and sophisticated attack methodologies. SecurityScorecard detects potential vulnerabilities in Network Security by identifying open ports connected to the organization's network and evaluating the company's track record in complying with current security protocols and minimizing external access to internal systems by securing network endpoints. An insecure network is one of the easiest ways for hackers to gain access to sensitive data. Once a hacker is inside the network, the next steps include lateral movement, eventually resulting in the compromise and theft of mission-critical digital assets.

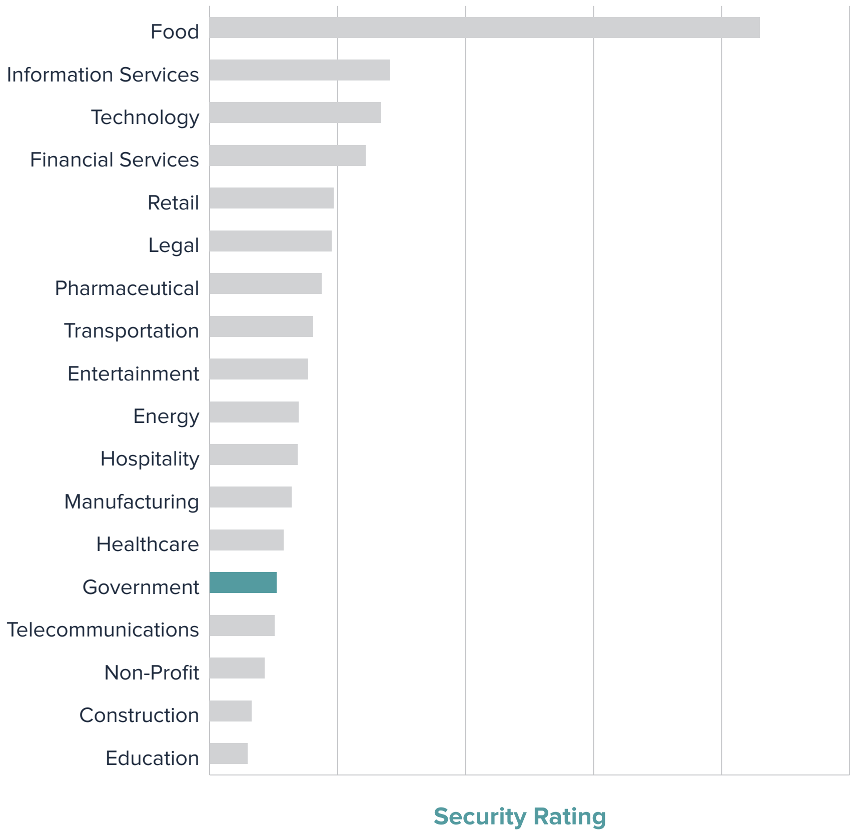


Government organizations remain among the poor performers in this category. With a 2018 mid-C score, down slightly from last year, the public sector falls just below the average score for all major industries in this report. Government agencies (and nearly all industry sectors) still have open access points, misconfigured SSL certificates, and database vulnerabilities that are susceptible to attack.

Patching Cadence

Diligently patching operating systems, services, applications, and software in a timely manner is mandatory to keep hackers at bay. Yet, 80 percent of all cyberattacks exploit security vulnerabilities with existing patches. Patching cadence seems like an obvious area for due diligence, but companies in every sector continue to exhibit poor patching practices and miss this opportunity to safeguard their networks. The threat of inattentive patching is pervasive across industries.

It typically takes organizations months, or in some cases more than a year, to apply available security patches to Common Vulnerabilities and Exposures (CVEs). It's critical to maintain a patching schedule for critical assets and monitor the emergence of new CVEs. When a vulnerability is disclosed, usually in conjunction with a patch, cybercriminals look for and attack organizations with that weakness and target companies with a slow cadence. The longer it takes an organization to implement security patches after vulnerabilities are disclosed, the bigger the window of opportunity for hackers to successfully execute attacks. In the Equifax breach, hackers exploited an end-of-service (outdated) version of Apache Struts web application software no longer supported (via patches) by the manufacturer for vulnerabilities or functionality improvements. Hackers are aware that patches will not be released for end-of-life, end-of-service assets.



SecurityScorecard scans ports and crawls sites to gather data relative to versions of software and browsers in use. The platform tracks how fast organizations patch or remediate vulnerabilities. Government organizations remain below average and in the bottom third of industries for this category, earning a slightly better score (mid-C) than last year but one that mandates improvement.

Government agencies are patching slowly and/or using vulnerable legacy systems and software that cannot be patched. Even some top performers fall short in this category. One federal agency, for example, earned a "C" in patching cadence despite achieving an "A" in overall cybersecurity performance.

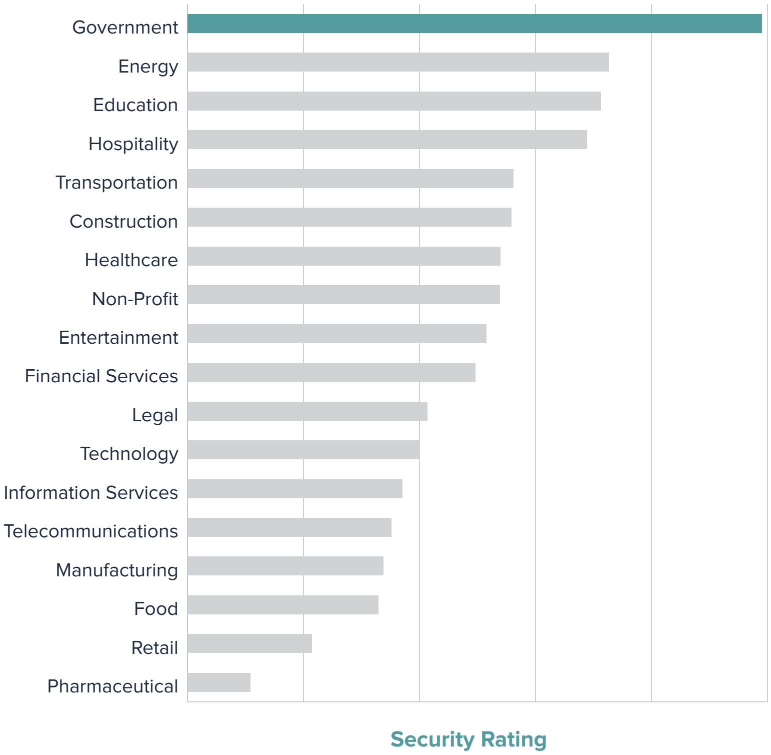
Top Three Government Security Factor Strengths

Compared to other industry sectors, government entities performed well in 2018 in DNS Health, Social Engineering, and Application Security.

DNS Health

The Domain Name System (DNS) protocol maps domain names to IP addresses, providing a “global internet phonebook.” DNS configurations of domain names tell the internet which IP addresses to use for web hosting, which email services to engage, and what compliance and security configurations to check. Attackers target vulnerable DNS records and configurations for DDoS attacks and other nefarious activities.

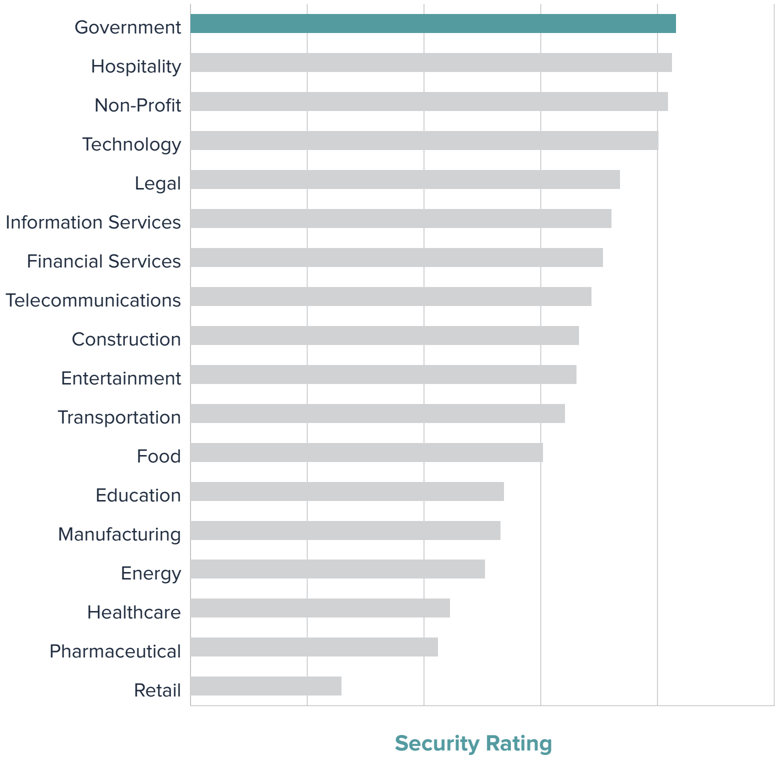
SecurityScorecard looks at DNS configurations from multiple perspectives including compliance, best practices, third-party vendor detection, and security.



Government agencies jumped up a rung in this category in 2018, surpassing education and energy to take the top spot among all industry sectors with a high-B score, which is marginally higher than the average score across industries surveyed in this report. The government continues to nurture employee security awareness and maintain good DNS health practices to protect agency information systems.

Social Engineering

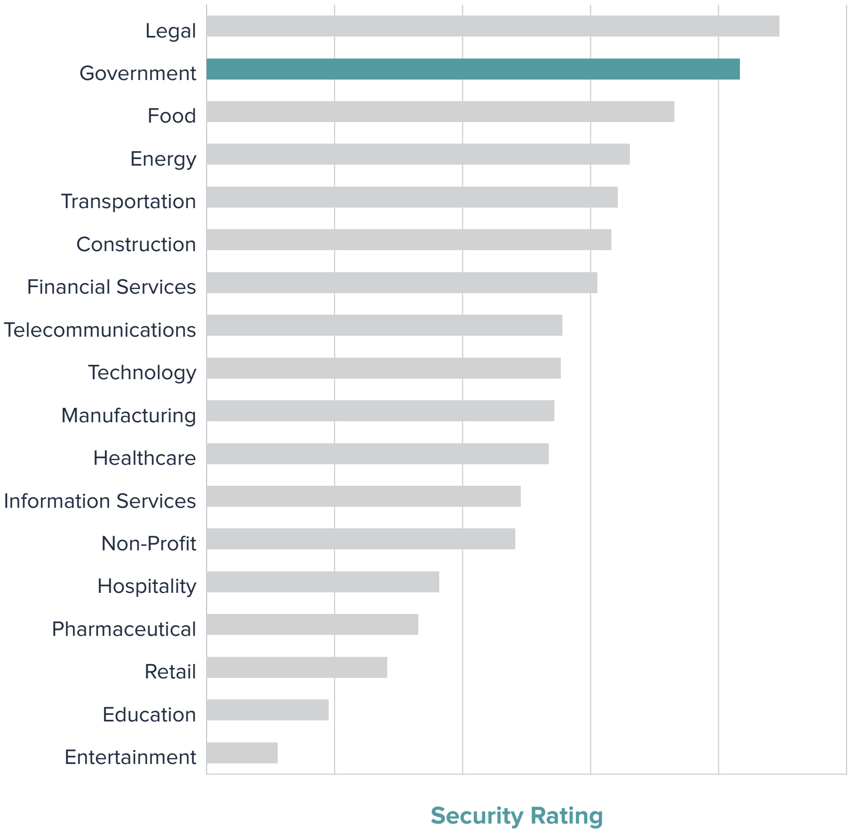
Social engineering, encompassing the tactics of convincing people to provide information by gaining and exploiting their trust, is a prominent threat in the cybersecurity landscape. SecurityScorecard identifies multiple factors related to social engineering, including phishing attacks and spam, use of corporate email addresses in social networks and e-commerce platforms, and other employee activity on social media platforms. Attackers will often profile email addresses obtained from data breaches and match them to existing social network profiles to target accounts and execute spear phishing attacks. For example, if an employee creates a Facebook or LinkedIn account with a government email address, it increases the risk of a phishing attack through one of those networks.



Government agencies jumped two levels in this category in 2018, performing better than hospitality and last year's industry leaders—the technology and non-profit sectors—and grabbing the top spot with a near-perfect score in the high nineties. While many industries score well in this category, the public sector's notable performance is due in part to the fact that government emails are less likely to show up in breached databases and spam lists. Also, agency employees, perhaps with greater cybersecurity awareness than those in other industries, generally know not to use work email addresses and credentials for marketing lists, social networks, etc.

Application Security

As web applications continue to proliferate, attackers increasingly exploit vulnerabilities that often stem from DevOps prioritization of speed and agility over security. Web applications are often vulnerable entry points that can be infiltrated to gain access to sensitive information.



Last year, government organizations fell in the middle of the pack in this category. In 2018, the public sector leaped nine spots to land in second place behind the legal industry with an “A” grade, marginally above the industry average. Government agencies have updated or replaced some legacy applications with commonly exploited vulnerabilities and are rigorously deploying web application firewalls to protect against DDoS attacks and the OWASP Top 10 Most Critical Web Application Security Risks.

Conclusion

Government agencies must continue to vigilantly reduce exposure, improve threat detection, accelerate incident response times, and proactively mitigate threats before they cause damage. The time is now, in advance of the discovery of attacks against the national critical infrastructure. It is important that those tasked with these responsibilities leverage available resources to address the unique requirements of government network infrastructure security and integrity.

The implementation of a continuous, external risk management platform such as SecurityScorecard can assist in the discovery of risk conditions on an ongoing basis. Continuous data-driven monitoring of agency, vendor, and contractor security posture; access to predictive breach insights; and proactive remediation of vulnerabilities can help contribute to higher security scores and a more resilient cybersecurity defense designed to stay one step ahead of hackers.

Ensuring that proper security protocols are in place and improving security posture now will lay the groundwork to avoid problems in the future. In the case of interconnected government systems that automate tasks for society – ensuring the security of these assets is a direct contribution to ensuring the security of national infrastructure.

SecurityScorecard

About SecurityScorecard

SecurityScorecard helps enterprises gain operational command of their security posture and the security posture of their third-parties through continuous, non-intrusive monitoring. The company's approach to security focuses on identifying vulnerabilities from an outside perspective, the same way a hacker would. SecurityScorecard's proprietary SaaS platform offers an unmatched breadth and depth of critical data points including a broad range of risk categories such as Application Security, Malware, Patching Cadence, Network Security, Hacker Chatter, Social Engineering, and Leaked Information.

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
214 West 29th St
5th Floor
New York City, NY 10001