SecurityScorecard

# 2017 U.S. State and Federal Government Cybersecurity Report


**SecurityScorecard**
**Security Research Team**
August 24th, 2017

It's clear that cybersecurity incidents are not going anywhere and that government will continue to remain a target. But with technology propelling forward and hackers as motivated as ever, government agencies are struggling to put up effective cybersecurity defenses- and hackers are taking advantage.

In August 2017, SecurityScorecard leveraged its proprietary platform to analyze and grade the current security postures of 552 local, state, and federal government organizations, each with more than 100 public-facing IP addresses, to determine the strongest and weakest security standards based on security hygiene and security reaction time compared to their peers.

## Key Industry Findings & Insights

1. Across all industries surveyed by SecurityScorecard, including transportation, retail, healthcare and more, government organizations received one of the lowest security scores.

2. When compared to other industries government organizations struggled more with four categories of security measurements: Endpoint Security, IP Reputation, and Patching Cadence.

3. Government organizations struggled with Patching Cadence, regardless of their IP size.

4. The U.S. Secret Service notably appeared in the list of the 10 best overall scores. Other top performers include the National Highway Traffic Safety Administration, Internal Revenue Service, and the Federal Reserve.

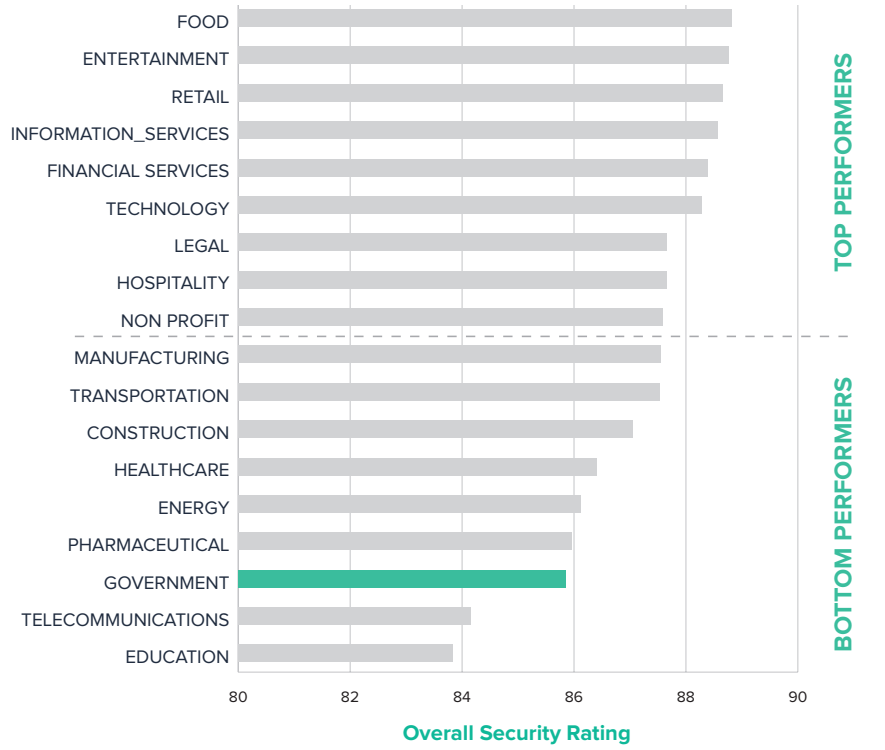
## Overview

By using the information collected through its proprietary data engine–ThreatMarket–and through other non-intrusive collection activities, SecurityScorecard surfaces data on the potential security risks in 10 categories:

1. Web Applications
2. Network Security
3. Leaked Credentials
4. Hacker Chatter
5. Social Engineering
6. Exposed Administrative Portals (Cubit Score)
7. DNS Health
8. Patching Cadence
9. Endpoint Security
10. Malware Presence (IP Reputation).

This data is then analyzed and appropriately weighted by considering factors such as the severity of the issues, the risk level as defined by industry standards, the overall performance of similar companies, and so on- resulting in an overall score that reflects the cybersecurity health of an organization.

**FIGURE 1** Overall Industry Ranking



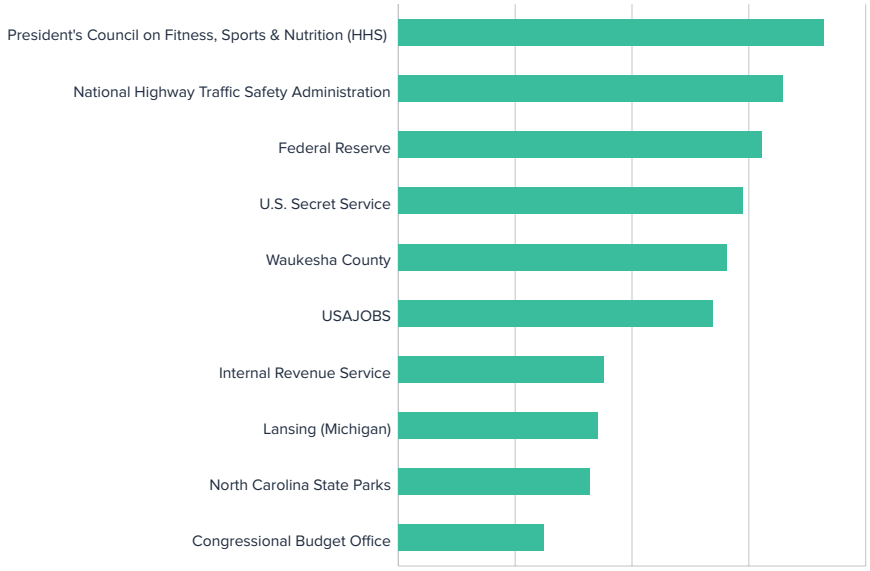

Compared to last year, government has moved from the lowest performing industry, past telecommunications and education. However, this relative improvement still leaves government agencies as as the third lowest performing industry when compared to the cybersecurity of 17 other major industries.

This report identifies key network infrastructure weaknesses and vulnerabilities within government organizations broken down 1) by security factor and 2) by organization's IP footprint size.

# Top Performers

(Combined All 100+ IP Footprints)

**FIGURE 2** Top 10 Overall Strongest Performers




Consistencies in security performance were established across the top government performers, which included small, medium, and large government organizations. Areas of strength across high performers include high scores in: Application Security, Network Security, Hacker Chatter, IP Reputation, Endpoint Security,  Password Exposure, Cubit Score, and Social Engineering.

On average, for top performers the two areas where there were slight fluctuations in scores were DNS Health and Patching.

## Small Organizations

(IP Footprint = 100 to 1000)

While one might think that a smaller IP footprint means these government entities have a smaller attack surface, in most cases, it also means that there are less people monitoring the attack surface. Where large enterprises might have dedicated staff to address cybersecurity issues, smaller government organizations may have just one resource devoted to all of IT or even outsource their IT and cybersecurity function.

Smaller budgets and resource shortages may explain why small government organizations with the weakest security postures have vulnerabilities in the areas of Network Security and Patching Cadence. (For Network Security, 70 percent of low performers scored an 'F,' and for Patching Cadence, 75 percent received an 'F.') But not all small agencies struggled.

**FIGURE 3** Top 10 Small Organizations

| Entity | Total Score | Application Sec | Cubit Score | DNS Health | Endpoint Security | Hacker Chatter | IP Reputation | Network Security | Password Exposure | Patching Cadence | Social Engineering |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Federal Agency | A | A | A | A | A | A | A | A | A | A | A |
| County in Wisconsin | A | A | A | A | A | A | A | A | A | A | A |
| Federal Website | A | A | A | A | A | A | A | A | A | A | A |
| Federal Agency | A | A | A | B | A | A | A | A | A | A | A |
| City in Georgia | A | A | A | A | A | A | A | A | A | B | A |
| Federal Agency | A | A | A | A | A | A | A | A | A | B | A |
| City in Arizona | A | B | A | A | A | A | A | A | A | A | A |
| State Government | A | A | A | B | A | A | A | A | A | A | A |
| Police Department in Maryland | A | A | A | B | A | A | A | A | A | B | A |
| Federal Agency | A | A | A | A | A | A | A | A | A | B | A |

Among small organizations with a high security posture, nearly every security factor scored an 'A' for these organizations. With that said, even some top-performers saw small fluctuations in Patching Cadence scores, with a handful receiving 'Bs,' indicating the slightly fluid nature of their security posture.

## Medium Organizations

(IP Footprint = 1000 to 10000)

Often with the same budget and staff limitations of small organizations, medium-sized government organizations can face many of the same issues and concerns as small organizations. Low performers in this group may struggle with Network Security and Patching Cadence just like their smaller counterparts, but they also may have weaknesses in the category of IP Reputation.

**FIGURE 4** Top 10 Medium Organizations

| Entity | Total Score | Application Sec | Cubit Score | DNS Health | Endpoint Security | Hacker Chatter | IP Reputation | Network Security | Password Exposure | Patching Cadence | Social Engineering |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Federal Agency | A | B | A | A | A | A | A | A | A | C | A |
| Federal Agency | A | A | A | A | A | C | A | B | A | A | A |
| Federal Agency | A | A | A | B | A | A | A | A | A | B | A |
| County in Nevada | A | A | A | B | A | A | A | A | A | B | A |
| County in Washington | A | C | B | A | B | A | A | A | A | B | A |
| Federal Agency | A | A | A | B | A | A | A | C | A | B | A |
| Federal Agency | A | A | A | B | A | A | A | B | A | B | A |
| City in Iowa | A | A | A | C | A | A | A | C | A | A | A |
| City in Florida | B | A | A | D | A | A | A | B | A | B | A |
| Federal Agency | B | A | A | A | A | A | A | C | A | C | A |

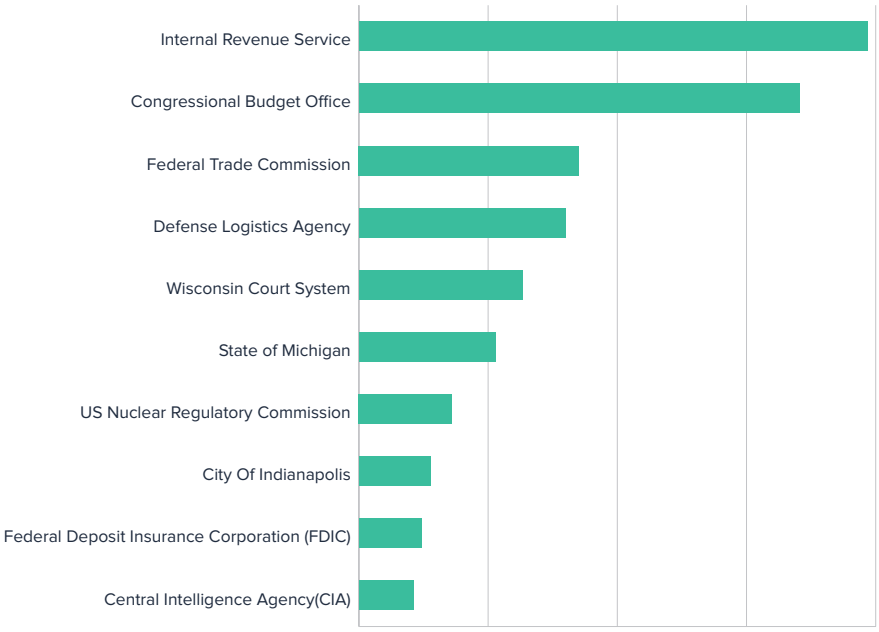
Those who overcame the hurdle of managing a medium-sized IP footprint and established themselves as top-performing medium organizations scored particularly well in Leaked Credentials, Cubit Score, and Social Engineering. However even these organizations sometimes struggled with DNS Health, Patching Cadence, and Network Security.

## Large Organizations

(IP Footprint = 10000+)

With a greater attack surface than the small and medium organizations, low-performing, large organizations inherently face a slew of issues. There are certainly some top performers - including the CIA, IRS, FDIC, and FTC- that score consistently well across the board with nearly all 'A's in all categories.

**FIGURE 5** Top 10 Large Organizations




However, many large government organizations have not developed sufficient cybersecurity capabilities yet. Historically, it's exactly these sorts of large government agencies that put significant investments into technology, dating back to the start of the internet. So if they've invested in technology and made efforts to harden their defenses in recent years, why are these large government organizations still coming up short? The problem is those old technology investments are still sitting there. A museum-worthy collection of technology investments through the '80s, 90s, and mid 2000s full of vulnerabilities sit alongside new emerging (and often misconfigured) technology, creating a horrible hodgepodge of cybersecurity risks.

## Key Findings by Security Factor

In addition to the insights about overall score depending on IP footprint size detailed above, the SecurityScorecard team extracted information specific to each of the ten security factors monitored by the SecurityScorecard platform.

It is important to note that these factors are not presented in order of criticality. Hackers use many different techniques and methods of attack that exploit multiple vulnerabilities across an organization's entire infrastructure. They may also use multiple vulnerabilities to gain access to a network or steal sensitive data. For example, an Information Leak can be used to exploit a flaw in an organization's Network Security, giving a hacker a way inside an organization.

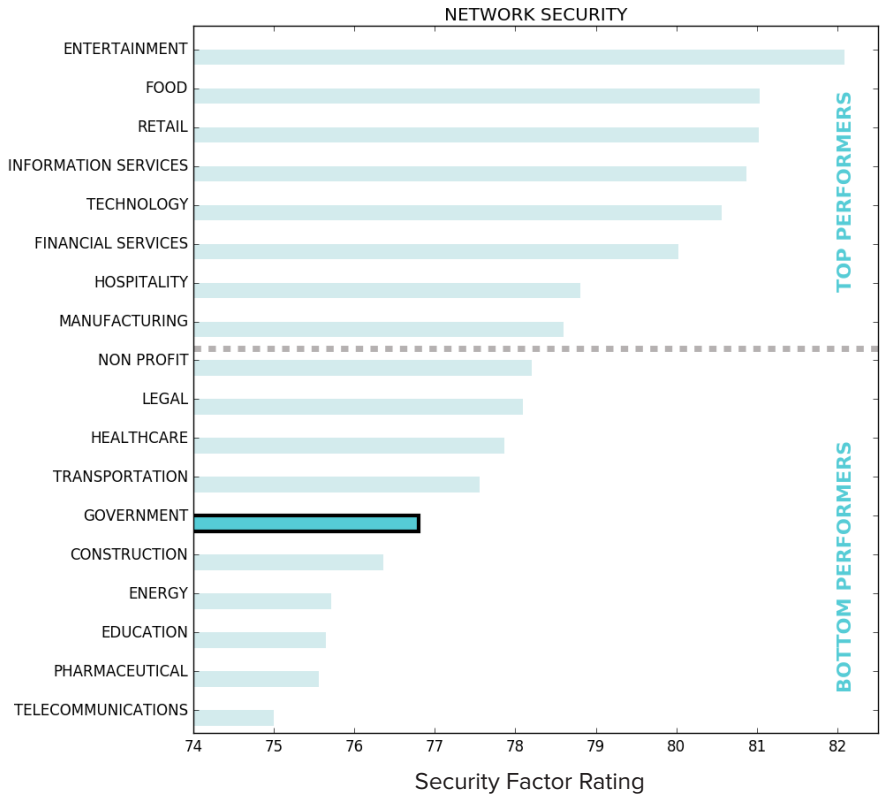
## Network Security

Network Security is one of the most crucial aspects of security and often the major focus of efforts by security professionals- and one of the weakest factors for government organizations of all sizes.

The core principle of network security is to close off and secure external access to all internal systems, with an exception for critical systems that need to stay exposed to the Internet. Over the years, network security has evolved rapidly with firewalls, intrusion detection systems (IDSs), packet filtering routers, and advanced network threat detection systems becoming available, giving organizations the flexibility and tools necessary to keep their network safe. Stronger scores in this category can indicate use of these tools to safeguard against new threats and methods of attack.

SecurityScorecard identifies potential vulnerabilities in network security by identifying open ports–such as FTP (Port 21), telnet (Port 23), SMB (Port 445), and RDP/VNC (Port 3389 and Port 5900)–connected to an organization's network exposed to the Internet 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.

**FIGURE 6** Industry Ranking by Network Security

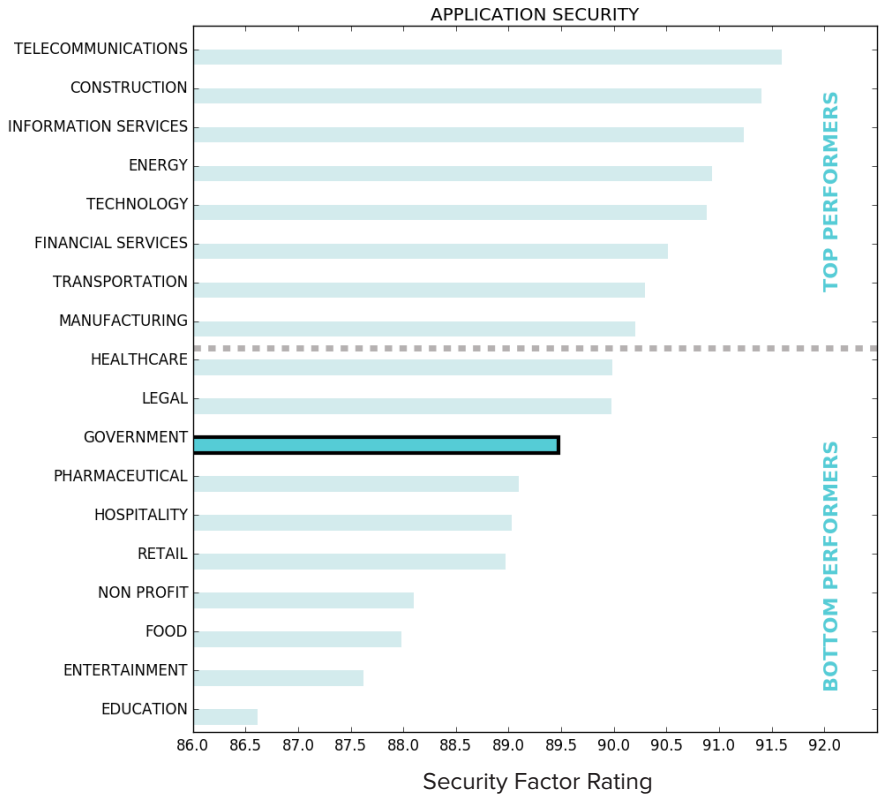



By analyzing these open ports, SecurityScorecard determined that government organizations fall in the bottom performers in the category of Network Security. These low scores typically indicate that the organization has an open port making them susceptible to attack- for example, the WannaCry attack that propagated through port 445. An insecure network is one of the easiest ways for a hacker to obtain access to sensitive data. Examples of network security hacks include exploiting vulnerabilities such as open access points, insecure or misconfigured SSL certificates, or database vulnerabilities and security holes that can stem from the lack of proper security measures. Once a hacker is inside the organization's network, digital assets can be compromised or stolen outright, throwing operations into chaos.

## Application Security

As web applications proliferate, so do hackers' attention to them. The problem is exacerbated by the fact that web applications are often built with speed, as opposed to security, as a priority. Attacks that exploit web application vulnerabilities may result in the hacker modifying the personal information found on cookies in a user's computer for identity theft, hijacking a web session, manipulating hidden fields, defacing a web page, or placing malicious code to cause erratic program behavior, among others. These unfortunate results are often achieved through the use of a Cross-Site Scripting (XSS) or an SQL injection attack.

**FIGURE 7** Industry Ranking by Application Security




Overall, government organizations score near the middle for application security- with organizations hovering on either side of average performance. A strong score in this area indicates that these government organizations are likely using web application firewalls, which often protect against DDoS attacks and the OWASP Top 10. However, it's important to note that in the case of many government agencies these

web application firewalls are just band-aids protecting poorly developed applications. Weaker scores in this category indicate that old website, php applications, and the like with multiple Common Vulnerabilities and Exposures (CVEs) are being used and are open to the OWASP Top 10 Most Critical Web Application Security Risks.

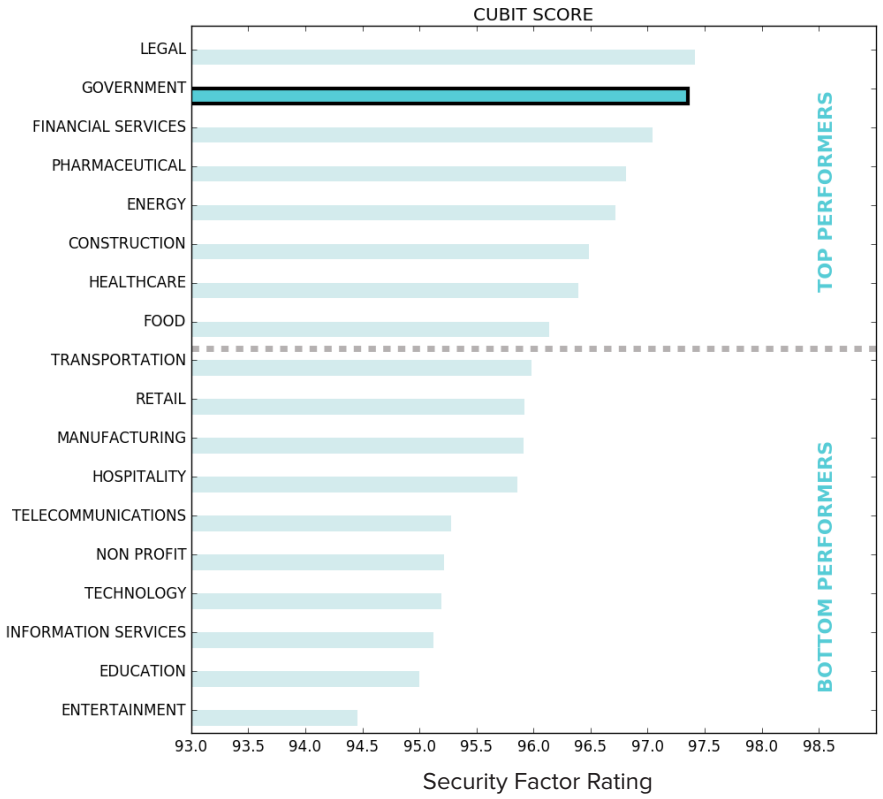
One example of this was in the tail-end of Summer 2016: the FBI released a 'Flash Alert,' warning election offices and officials in the U.S. to improve security and to be on the lookout for potential intrusions. The announcement came after a recent attack on the Illinois and Arizona electronic voter registration systems, where the FBI found that an SQL injection attack brought down Illinois' voter registration site for 10 days causing over 200K voter records to be compromised.

The SQL injection vulnerability has been in the top 10 list of most common vulnerabilities since 2003, peaking in 2011-12, where the U.S. Department of Homeland Security, Mitre, and SANS Institute named it the most dangerous vulnerability. As organizations continue to make use of web applications, they're putting themselves at risk of succumbing to a commonly exploited vulnerability.

## Cubit Score

The Cubit module reveals which administrative portals or subdomains are publicly viewable, which provides a potential access point to an organization's internal network. By knowing that there is an exposed administrative portal, a hacker may look for leaked credentials in the deep web and use it to leverage the identity of an authorized user. Once logged in, the hacker may obtain unauthorized access of default accounts, take over unused pages on a website, unpatched flaws, or unprotected files and directories to gain access to or knowledge of the system.

**FIGURE 8** Industry Ranking by Cubit Score



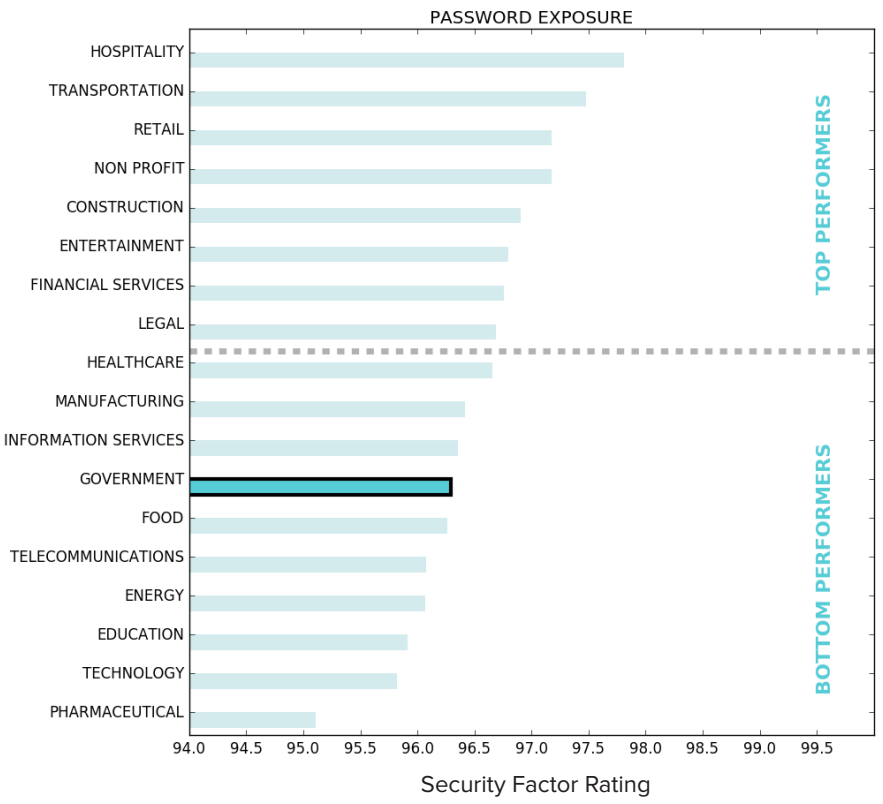

Government organizations rank second compared to other industries in this category, falling behind only the legal industry. These strong scores typically indicate that portals are not available to the public without some kind of secure Virtual Private Network (VPN) or whitelist and can also indicate the use of some kind of two-factor authentication.

## Leaked Credentials

The fastest way into most organizations is through stolen information, an increasingly-used tactic that all hackers take advantage of as part of infiltration. Each year, hundreds of millions of credentials are stolen, leaked, and shared freely within the hacker community. Hackers can buy the information and bide their time until they use it in conjunction with another attack to potentially inflict even more damage on an organization.

SecurityScorecard identifies all sensitive information that is exposed as part of a data breach or leak, keylogger dumps, pastebin dumps, database dumps, and via other information repositories. SecurityScorecard maps the information back to the companies who own the data or associated email accounts that are connected to the leaked information. By doing so, SecurityScorecard is able to assess the likelihood that an organization will succumb to a security incident due to the leaked information.

**FIGURE 9** Industry Ranking by Leaked Credentials



Government organizations fell into the low performers bucket for this security factor. It's no surprise given that government credentials have been seen in massive breaches such as the Yahoo, LinkedIn, Dropbox, or Ashley Madison mega-breaches flooding the dark market with over one billion records.

Low performance in this category can indicate: 1) that employees are using corporate emails for non-work purposes and 2) that passwords are being reused.

Password reuse is one of the oldest problems in information security. When coupled with the amount of leaked passwords floating around the dark market, providing insight into password patterns, hackers have now turned compromised credentials into a systematic way to routinely break into corporate accounts.

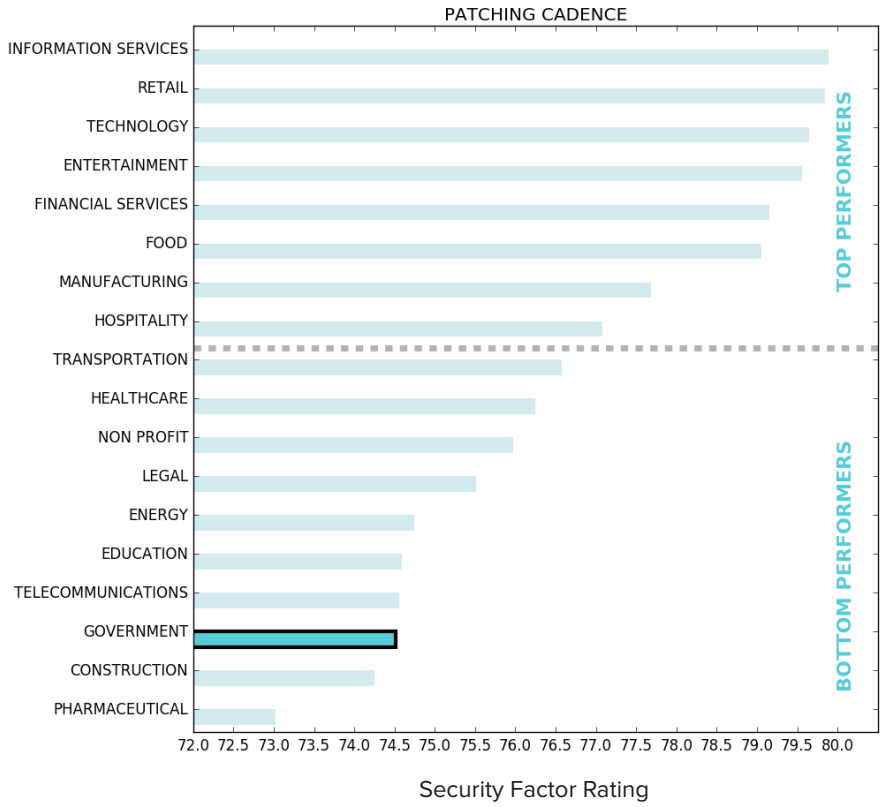
However, sensitive information is also made publicly available without the need of a hackers' expertise or due to a previous leak. Because of insecure security practices or poor content management, sensitive information may even be publicly viewable via common search or data repositories such as Google or Github.

## Patching Cadence

Software patches are inevitable, but diligently patching operating systems, services, applications, software, and hardware in a timely manner is necessary to keep hackers at bay. Often, when a vulnerability is disclosed, usually in conjunction with a patch, cybercriminals will look for organizations where that vulnerability exists, targeting companies with a slow or readily predictable patching cadence. If a hacker knows that a company has a slow patching cadence, then the hacker can wait for a newly disclosed vulnerability, build a payload, and exploit the vulnerability in less time than it takes for that organization to apply a patch. Depending on the vulnerability exploited, hackers can lure users to malicious websites, access sensitive information, take control of browsers or software, or hold an organization's entire network infrastructure for ransom by encrypting all of an organization's data.

SecurityScorecard 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, SecurityScorecard tracks the vulnerability. Furthermore, by noting the first and last time a vulnerability was observed, the platform is able to provide insight into how fast an organization is patching.

**FIGURE 10** Industry Ranking by Patching Cadence



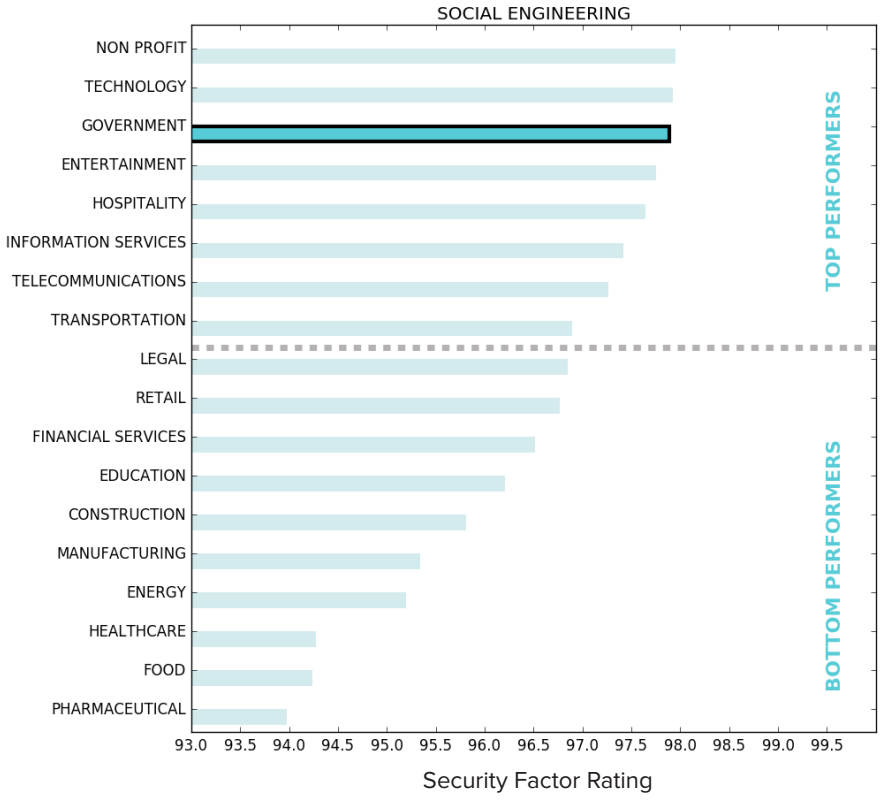

Government organizations are near the bottom of the pack with Patching Cadence, meaning these organizations likely have vulnerabilities from lack of patching, slow patching times, and use of vulnerable products and services. While some might think 'slow' is just the norm for government agencies, patches are likely not applied as quickly as they should be because government agencies are working with old legacy systems that aren't patch-friendly.

## Social Engineering

Social engineering is a method of exploitation that predates the computer. In essence, it is a technique that convinces a person or group to give you something by gaining and exploiting their trust. With the low level of security knowledge the average employee has, due to a lack of security awareness training, they might not even know that the information that they are handing out, or that the actions they are taking, are relevant from an information security standpoint. To successfully facilitate a social engineering attack, a hacker must leverage external resources such as marketing lists, social media profiles, and overall employee satisfaction to build profiles (known as Doxxing) to then carry out the attack. Social Engineering attacks are much more behavioral in nature than technical, which makes them difficult to defend against.

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.

**FIGURE 11** Industry Ranking by Social Engineering



Its relatively high social engineering score in the graph above indicates that government emails are less likely to show up on breached databases, spam lists, and so on when compared to other industries. It's a good indicator that government employees are likely trained sufficiently enough to not use corporate email addresses and credentials to sign up for marketing lists, social networks, and so on.

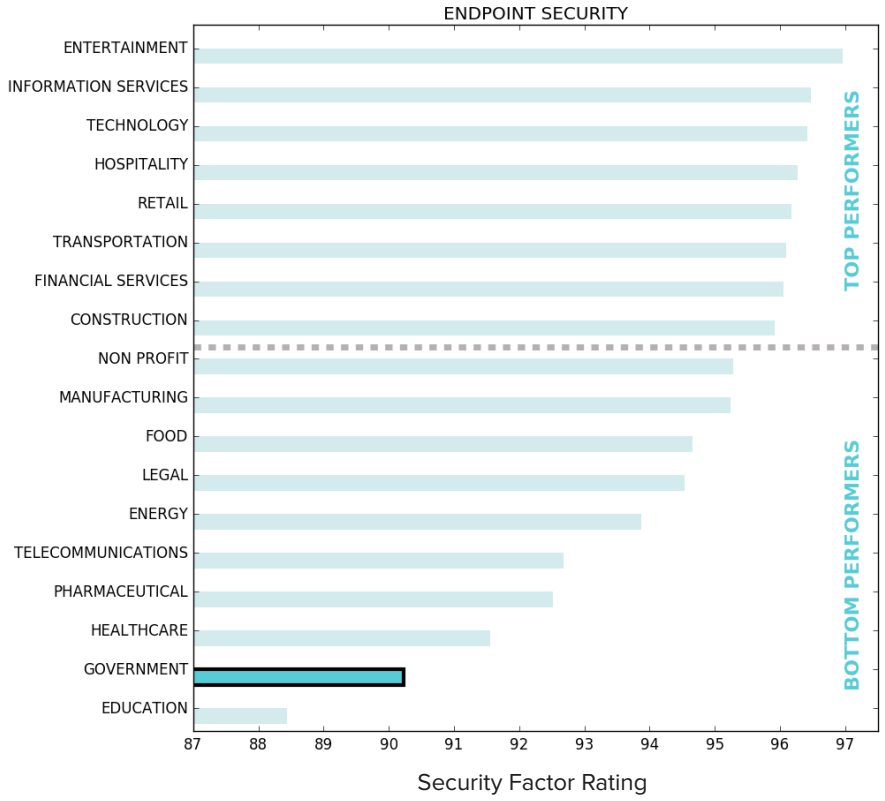
## Endpoint Security

Endpoint security refers to the protection involved regarding an organization's laptops, desktops, mobile devices, and all employee devices that access that company's network. As organizations allow employees to bring their own devices (BYOD) to work, endpoint security has grown in complexity. That complexity has turned into a benefit for hackers who are looking for a weak spot in an organization's network.

In the underground internet, hackers use exploit kits, which are software (also known as crimeware) that provide criminals and hackers with tools that exploit various vulnerabilities across different kinds of softwares, products, and services. This allows hackers who have little or no programming experience to merely pay for the exploit kit, release it into the wild, and wait for money to come in from successful hacks.

SecurityScorecard is able to detect when endpoints at an organization are using old, insecure browsers and operating systems by tracking identification points that are extracted from metadata related to operating systems, web browsers, and related active plugins. The information gathered identifies outdated versions of these data points which can lead to client-side exploitation attacks through a methodology similar to the way an exploit kit would.

**FIGURE 12** Industry Ranking by Endpoint Security



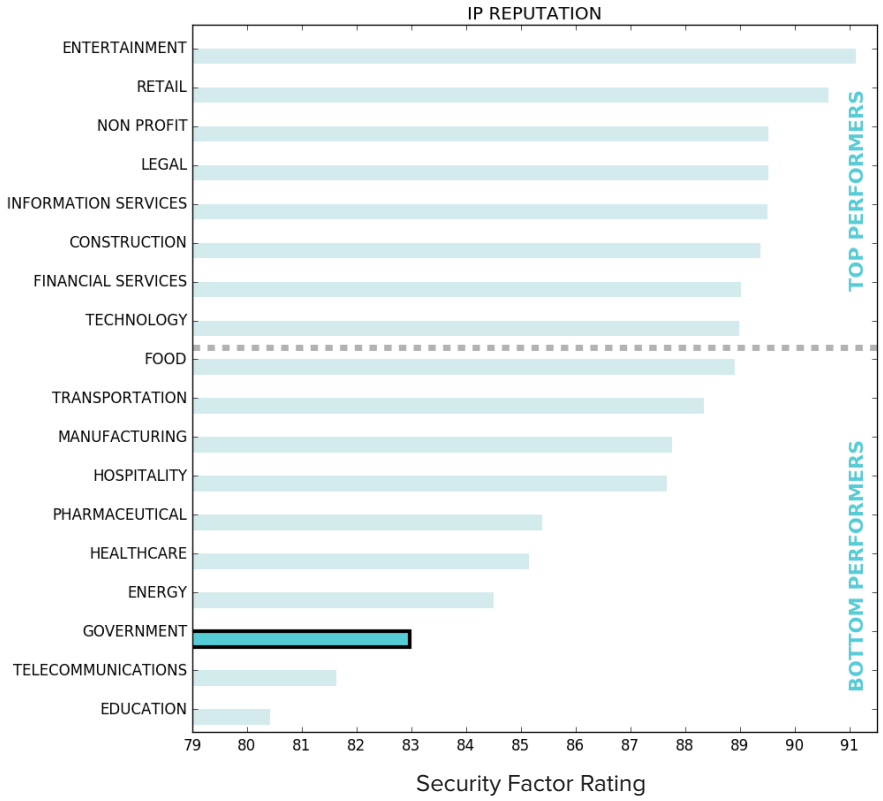

The low score in the category endpoint security when compared to other industries indicates that government agencies may be employing unsafe practices like using out of date browsers and old software. It might seem like a simple problem to fix, but often times these government agencies are using old versions of software, because new versions are not compatible with the antiquated infrastructure in place in these organizations.

## IP Reputation

An IP address gets a good or bad reputation based on malware presence, unsolicited bulk email activity, detected nefarious activity such as scanning or brute-forcing, or whether or not it has appeared on third-party blacklists. Hackers can take control of the device behind an IP address to exfiltrate data, spew spam, spread viruses or malware, to be used as a proxy for further attacks. If your company's IP address is used by hackers, it may be blacklisted, potentially affecting your organization's capability of accessing and communication through the internet.

The SecurityScorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures from all over the world. The incoming infected IP addresses are then processed and attributed to corporate enterprises through our IP attribution algorithm. The quantity and duration of malware infections are used as the determining factor for these calculations, providing a data point for the overall assessment of an organization's IP Reputation. Additional methods of assessment include setting up honeypots, which detect nefarious activity stemming from an IP address, or spam traps which identify the IP addresses responsible for sending bulk spam email.

**FIGURE 13** Industry Ranking by IP Reputation



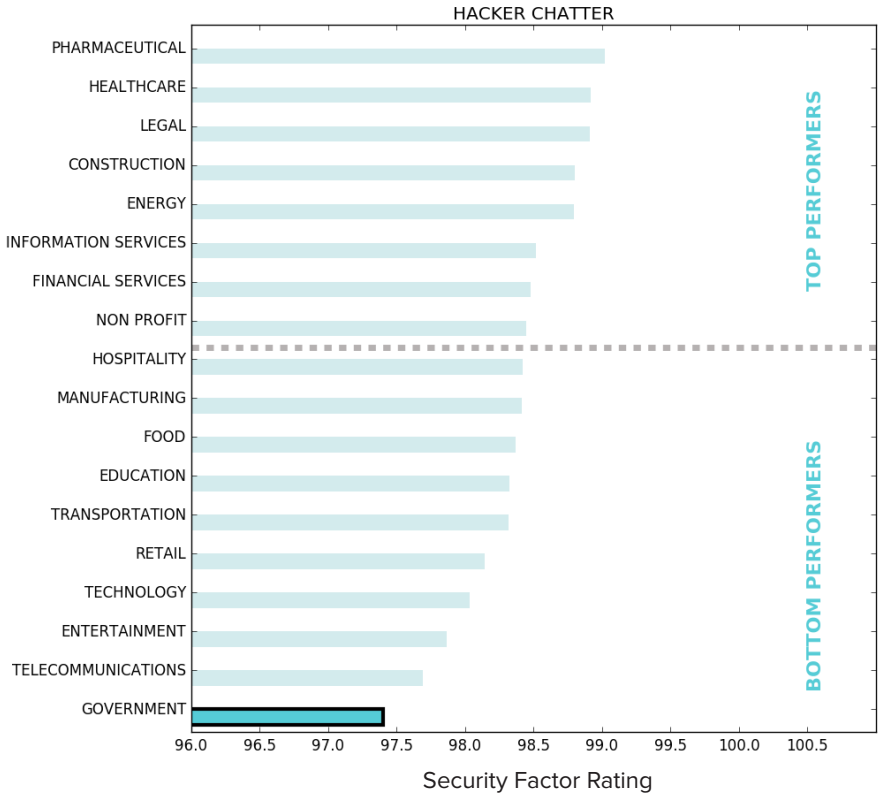

The relatively low score of government when compared to other industries indicates that government IP addresses are hitting these blacklists (sinkholes, honeypots).

## Hacker Chatter

Information about an organization's vulnerability moves rapidly across the hacker community. Comments made at small technical conferences or in obscure blog posts are often reacted to in a matter of hours. Once hackers know where a weakness exists, they can quickly determine how to exploit it. The need to keep an ear to the ground can't be understated when dealing with opportunistic and aggressive hackers.

The SecurityScorecard Hacker Chatter factor continuously collects communications from multiple streams of underground chatter, including hard-to-access or private hacker forums. Organizations and IPs that are discussed or targeted are identified. Forums, IRC, social networks, and other repositories of hacker community discussions are continuously monitored to locate mentions of business names and websites.

**FIGURE 14** Industry Ranking by Hacker Chatter




In this case, a low score in hacker chatter for government is not surprising and is not necessarily indicative of as big of a security weakness as it may appear. Often times hackers are mentioning government websites, because they are talking about these agencies sanctioning hackers or cracking down on enforcement.

## DNS Health

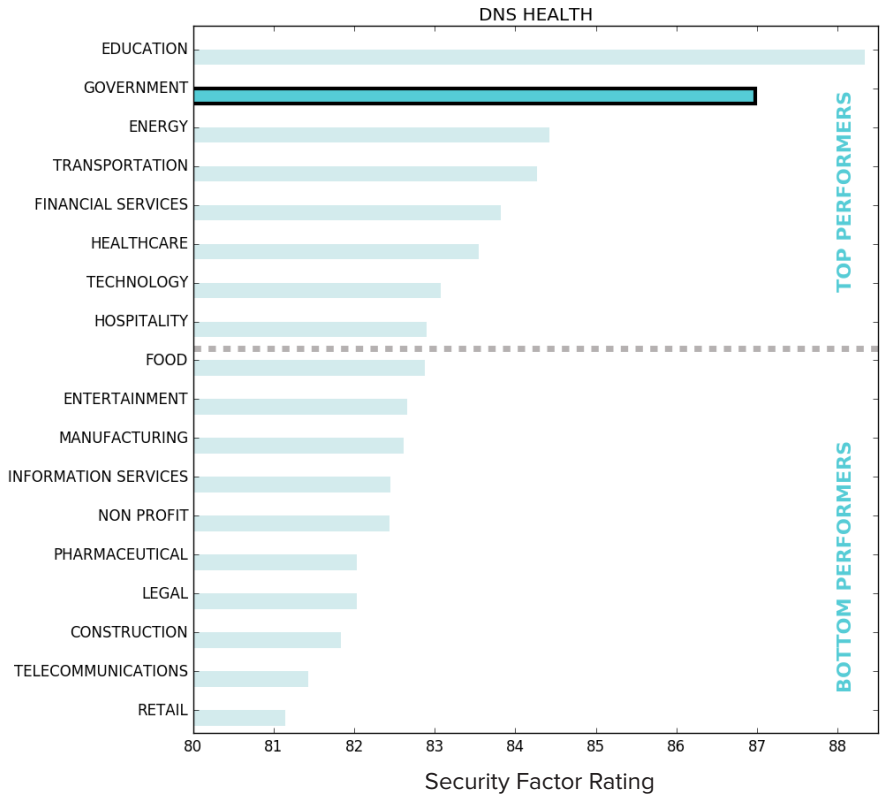
The Domain Name System (DNS) protocol maps domain names to IP addresses, and is widely considered a "global internet phonebook." The DNS configurations of domain names tell the internet which IP addresses to use for web hosting, which email services to use, and what compliance and security configurations to check.

Attackers frequently make use of an organization's DNS records for reconnaissance purposes against that organization and may be looking to complete objectives such as:

- discovering subdomains for internal login portals
- locating additional IP addresses associated with the target
- probing the DNS configuration itself for vulnerabilities such as the 'OpenResolver' setting, which, if exploited, allows the DNS server to be used in a Distributed Reflective Denial of Service Attack (DrDoS), explained below

The SecurityScorecard platform measures multiple DNS configuration settings, such as OpenResolver configurations as well as the presence of recommended configurations such as DNSSEC, SPF, DKIM, and DMARC.

**FIGURE 15** Industry Ranking by DNS Health



The relatively strong score of the government industry indicates that these organizations are using good practices, such as ensuring proper configurations and employing other practices to protect DNS health.

## Conclusion

The increasing severity of cyber attacks and the emergency of new technologies are just two of the many driving forces pushing the U.S. government sector to improve its cybersecurity. With threats ramping up in frequency and sophistication, investing in creating meaningful cybersecurity strategies and cleaner architectures has become paramount for government agencies to achieve the cybersecurity posture.

Get your free Instant SecurityScorecard here.

# References


- https://www.marketresearchmedia.com/?p=206
- https://www.acunetix.com/websitesecurity/cross-site-scripting/
- https://krebsonsecurity.com/2016/02/fraudsters-tap-kohls-cash-for-cold-cash/
- https://oag.ca.gov/system/files/ACID_PRINTERPROOFS.NOTICE%20LETTER_0.pdf
- https://www.scmagazine.com/panther-creek-senior-arrested-for-hacking-school-changing-grades/article/528315/
- https://krebsonsecurity.com/2016/02/fraudsters-tap-kohls-cash-for-cold-cash/
- http://www.csoonline.com/article/2961066/supply-chain-security/ubiquiti-networks-victim-of-39-million-social-engineering-attack.html
- https://gizmodo.com/security-hell-private-medical-data-of-over-1-5-million-1731548110
- http://news.berkeley.edu/2016/02/26/campus-alerting-80000-individuals-to-cyberattack/
- http://www.coindesk.com/major-security-flaw-heartbleed-puts-critical-services-risk/
- http://heartbleed.com/
- http://www.infoworld.com/article/3148145/security/flash-player-remains-target-of-choice-for-exploit-kits.html
- https://www.recordedfuture.com/top-vulnerabilities-2016/
- http://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware
- http://blog.securityscorecard.com/2016/10/28/iot-responsible-massive-ddos-attack/
- https://thehackernews.com/2016/08/election-system-hack.html
- https://threatpost.com/sql-injection-attack-is-tied-to-election-commission-breach/122571/
- https://www.netsparker.com/blog/web-security/sql-injection-vulnerability-history/
- https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
- http://arstechnica.com/security/2016/06/teamviewer-says-theres-no-evidence-of-2fa-bypass-in-mass-account-hack/
- http://fortune.com/2015/04/07/heartbleed-anniversary-vulnerable/
- http://arstechnica.com/security/2015/03/bogus-ssl-certificate-for-windows-live-could-allow-man-in-the-middle-hacks/
- https://fcw.com/articles/2017/01/09/2017-forecast-federal-it.aspx
- https://insights.hpe.com/articles/what-to-expect-2017-it-trends-in-government-and-the-public-sector-1701.html