SecurityScorecard

2019 Healthcare Report

securityscorecard.com [800] 682 1707

SecurityScorecard

Overview

The healthcare industry still needs improvement in its cybersecurity posture.

Meanwhile, malicious actors increasingly target electronic protected health information (ePHI) because the data it contains provides enough information to steal a person's full identity. Healthcare databases store a plethora of information including social security numbers, financial, health insurance, and driver's license data. Online toolkits make targeting this information easier, increasing the number of malicious actors. In December 2018, Dark Reading described how attackers can remotely launch attacks that render firmware and hardware inoperable.[1]

In this year's report, SecurityScorecard looked at 26,204 companies from September 2, 2018 to January 28, 2019 and analyzed terabytes of information to assess risk across ten risk factors.

"It's no secret in healthcare, significant risk exists in the supply chain and it's increasing as systems supporting clinical and administrative processes are migrating out of our data centers and into the hands of service providers more and more. SecurityScorecard gives us a lens into how seriously our service providers take the security of their platforms. We're using it as an input into selecting the right service providers, getting the contracts and service levels right, monitoring adherence to those contracts, and to drive honest conversations about security – which are most important."

Taylor Lehmann
Chief Information Security Officer
Wellforce and Tufts Medical Center

Key Insights

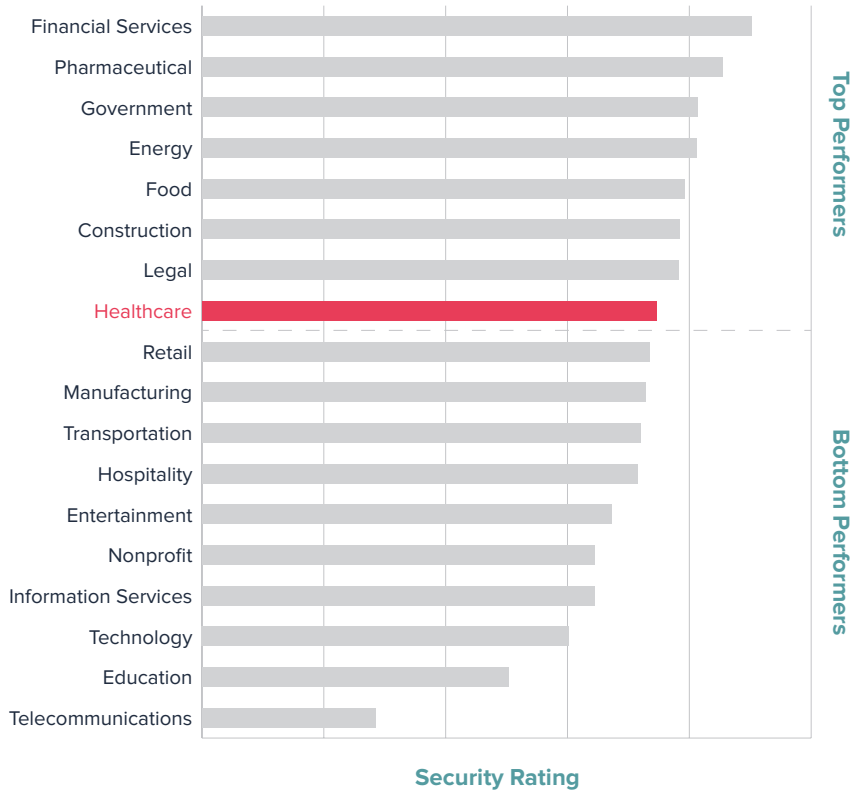
- The healthcare industry ranks eighth out of eighteen other major U.S. industries.
- Ranks eighth out of eighteen for application security when compared to other major U.S. industries.
- Ranks thirteenth out of eighteen in DNS health when compared to other major U.S. industries.
- Ranks twelfth out of eighteen for endpoint security when compared to other major U.S industries.
- Ranks fifth out of eighteen for network security when compared to other major U.S industries.
- Ranks tenth out of eighteen for patching cadence when compared to other major U.S industries.

1 https://www.darkreading.com/application-security/how-to-remotely-brick-a-server/d/d-id/1333531

SecurityScorecard

Healthcare Industry Data Needs a Security Infusion

The healthcare industry ranks eighth when compared to eighteen other major U.S. industries.



Despite being highly regulated, the healthcare industry needs improvement. When compared to other highly regulated industries, such as finance, healthcare looks weak in terms of cybersecurity. Whether from a data protection or compliance perspective, the lack of effective controls continues to be a challenge for the healthcare industry.

With the myriad of personal information a single healthcare record contains, a cybercriminal can steal an identity-- that identity can then be leveraged for insurance fraud, third party account takeovers, opening new lines of credit, and so on. In June 2018, Health IT Outcomes reported that while a credit card record with personal information is worth a maximum of $30 on the dark web, medical records consistently sell for $70-$90 each.[2] (The price is higher for medical likely due to the numerous additional data points that the records provide which reduces the research overhead needed from an attacker to achieve a successful impersonation.) Meanwhile, fines for accidentally violating the Health Insurance Portability and Accountability Act (HIPAA), even with reasonable due diligence, can be anywhere from $100-$50,000 per violation.[3]

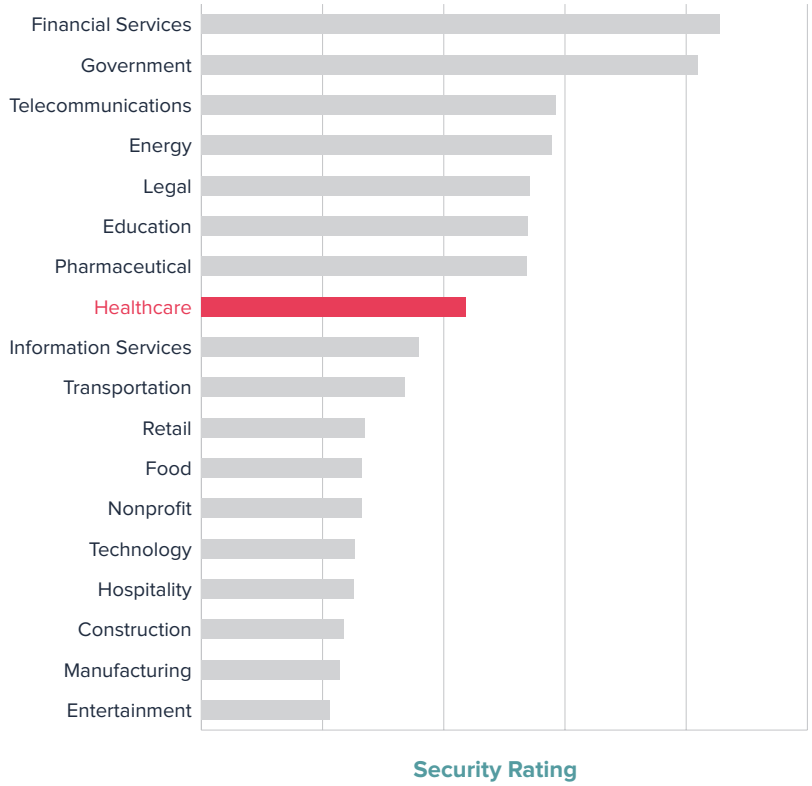
2 https://www.healthitoutcomes.com/doc/why-hackers-value-ephi-more-than-credit-cards-0001

3 https://www.hipaajournal.com/hipaa-violation-fines/

SecurityScorecard

Internet of Things and Connectivity Causes Complexity in Managing Cybersecurity Health

The healthcare industry ranks eighth out of eighteen for application security.



Healthcare providers use more mobile applications than ever before, and projections indicate that the use will only increase. The 2018 WhiteHat Application Security Statistics Report found that 60% of applications had at least one serious and exploitable vulnerability during 2017 and nearly 70% of every application is built upon reusable software.[4] In short, applications come with vulnerabilities that previous applications and software had. Moreover, in 2018, researchers at the IEEE 9th International Conference on Dependable Systems, Services, and Technologies explained, "According to the preliminary forecasts about 50 billion devices will be connected to the internet and the IoT market will reach about $1.7 trillion by 2020."[5] Since IoT devices oftentimes rely on inherently insecure embedded applications, the rise of networked medical devices places patient data at an even greater risk. The healthcare industry's reliance on embedded applications within IoT medical devices creates a vulnerable ecosystem whereby attackers can leverage multiple exploitable vectors to obtain access to confidential data.

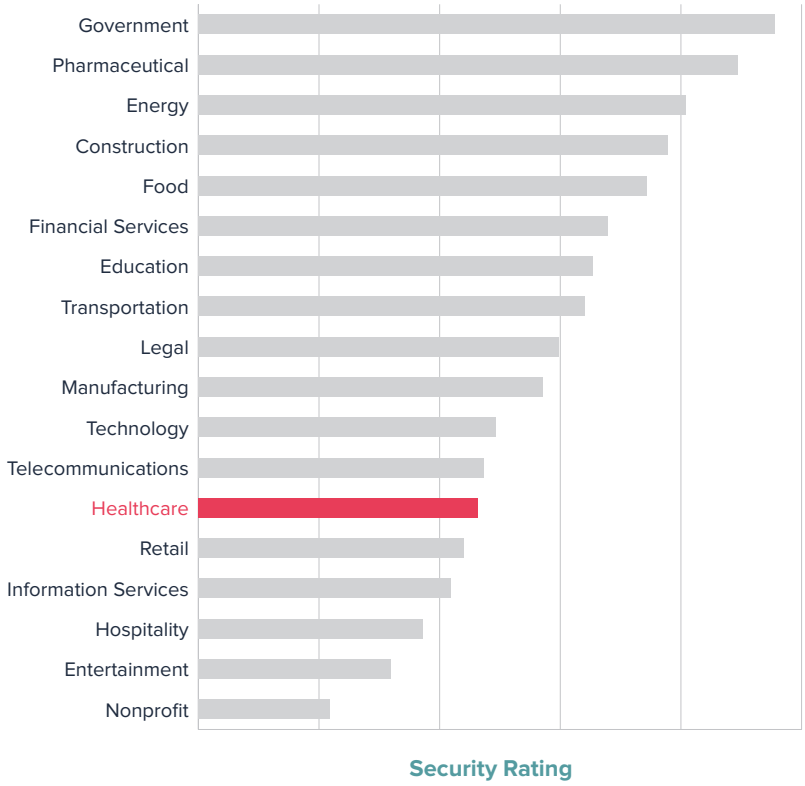
4 https://www.whitehatsec.com/blog/2018-whitehat-app-sec-statistics-report/

5 https://ieeexplore.ieee.org/document/8409099

SecurityScorecard

DNS Security a Weakness for Healthcare

The healthcare industry ranked thirteenth when comparing its DNS security to other industries.



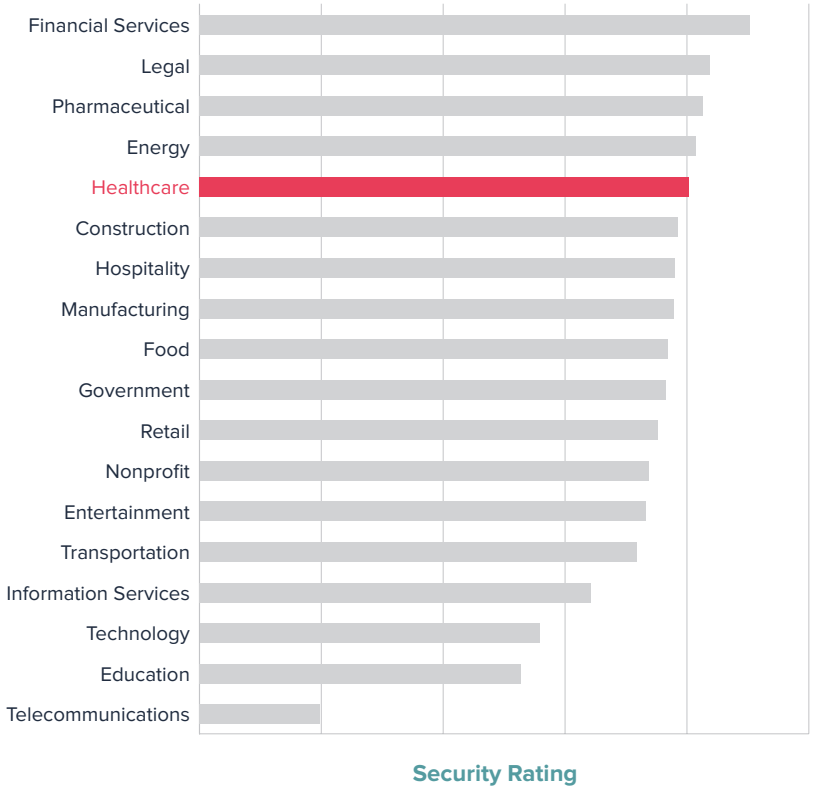
In January 2019, the HIPAA Journal announced that the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Agency (CISA) issued an emergency warning about DNS hijacking attacks.[6] A DNS server allows computers to connect to IP addresses without the user having to type in the numbers associated with the website. The cyber criminals changed the DNS records, re-routing web and email traffic. This allowed them to collect sensitive information being shared over the internet. The healthcare industry's low score for DNS health makes it a prime target for attacks to occur with greater frequency.

6 https://www.hipaajournal.com/dhs-issues-emergency-warning-about-dns-hijacking-attacks/

SecurityScorecard

The Status of Network Security in Healthcare Industry

The healthcare industry ranked fifth out of eighteen for Network Security when compared to other industries.



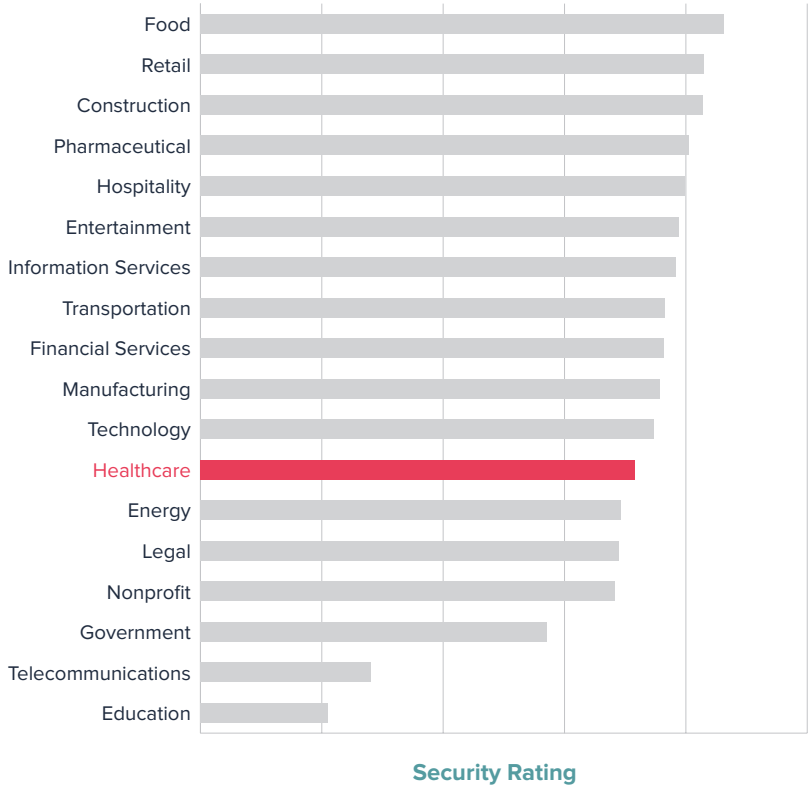
Currently, the healthcare industry scores relatively well at network security. Focusing on firewalls and network segregation to maintain HIPAA compliance helped the industry's score. However, a January 2019 article in Health Data Management notes that only 20% of healthcare providers have a comprehensive security program.[7] The article further notes that most cybersecurity programs are pieced together focusing on requirements in standards and regulations, many of which focus on network security, which means that the strong heartbeat of security remains at risk from another control weakness. When the network security ratings are put into context with endpoint security ratings - it can be inferred that the majority of healthcare industry is reliant on the antiquated "eggshell security model," where a strong, hardened perimeter defends a soft, vulnerable internal network.[8]

7 https://www.healthdatamanagement.com/opinion/why-healthcare-has-unhealthy-detection-protection-problem

8 https://www.legaltechnology.com/latest-news/comment-why-old-school-eggshell-security-no-longer-hacks-it/

SecurityScorecard

Healthcare Has Mediocre Performance in Endpoint Security



HIMSS, a healthcare nonprofit organization focusing on health IT, noted in its 2018 Cybersecurity Survey that 27.5% of respondents felt that "too many endpoints" was one of the biggest barriers to remediating and mitigating cybersecurity incidents.[9] Looking back to its 2015 report, HIMSS noted that the results were nearly the same. In 2015, 32% of respondents felt that having too many endpoints was their biggest barrier.

In short, organizations in the healthcare industry remain consistently overwhelmed by the large number of endpoints, stagnating their cyber security.

9 https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf

SecurityScorecard

Patching Accounts for a Substantial Quantity of the Cybersecurity Issues in the Healthcare Industry

According to the 2019 Avast PC Trends Report, 55% of all programs worldwide are out of date and 48% of applications installed on PCs are out of date.[10] Outdated programs, applications, and operating systems leave an organization vulnerable to cyberattacks. Security updates protect the organization by closing gaps called "commonly known vulnerabilities." Cybercriminals track these vulnerabilities and look to exploit them. Organizations not patching their systems, networks, and software leave them open to a data breach.

Often, companies choose to delay patch deployments because updating software requires coordinating system downtimes and the allocation of IT resources. Fears of "bricking" a system due to untested code often prevent organizations from implementing patches immediately, with some worrying that updates lead to lower productivity. Unfortunately, hackers study the release of patched vulnerabilities and take advantage of gaps in security update times. Delaying critical patch deployments creates opportunities that can lead to data breaches.

10 https://blog.avast.com/pc-report-2019-shows-users-fail-to-update-avast

The healthcare industry isn't unique in struggling with patching cadence. As referenced in the SecurityScorecard Big 500 index, many major corporations have difficulty maintaining proper patching – with more than 117,653,451 unique patching cadence issues being detected in the SecurityScorecard Big 500 group over a six month period.

Explaining Slow Patching Cadences

Slow patching cadences indicate several factors affecting IT departments. Sometimes companies lack engineering resources to implement a solution, while other times they lack resources to respond to problems patches cause. In still more concerning cases, some companies do not know vulnerabilities and patches exist. Since many standards and regulations require ongoing monitoring, slow patching cadence risks the organization's data and its compliance stance.

The sheer number of ongoing software patches often paralyzes organizations, keeping them from implementing the most critical repairs and updates. This opens breached companies to negligence claims and lawsuits. With so many vulnerabilities and security concerns, risk assessments that catalogue critical assets and focus on continuous monitoring for critical vulnerabilities act as the road map to cybersecurity success.

SecurityScorecard

A Word on The State of Cybersecurity in the Healthcare Industry from our VP of Compliance:

Fouad Khalil
VP of Compliance

The healthcare industry continues to struggle with securing data environments and ecosystems, leading to data breaches and HIPAA violations, as well as other regulatory and industry standards compliance issues. While the number of breaches remained static, the number of confirmed data disclosures as a result of the breaches nearly doubled in 2018 when compared to 2017, placing electronic Protected Health Information (ePHI) in even more danger. Data breaches arising from business associates, defined as third-party business partners or vendors, were the most severe, accounting for 42% of all exposed/stolen records in 2018.

The risk of ePHI exposure and unauthorized access is an increasing trend year after year. Reviewing all published breaches by the Health and Human Services (HHS) Office for Civil Rights (OCR) since 2009, a shocking total of 195 million healthcare records were affected, equating to 59.8% of the US population.

The OCR, as the main enforcer of the Health Insurance Portability and Accountability Act (HIPAA) Rules, has the authority to issue financial penalties for violations. In 2018, OCR issued ten financial penalties to resolve HIPAA violations that were discovered during the investigation of healthcare data breaches and complaints. However, under the HiTECH Act, State Attorneys General can also enforce state resident rights in the event of HIPAA noncompliance and issue fines for HIPAA violations.

Considering all the above, a point-in-time compliance stance is no longer sustainable. Healthcare organizations must adopt continuous assurance practices to maintain compliance and adequately protect data. Additionally, covered entities must implement best practices for business associate agreements to avoid civil and criminal HIPAA enforcement penalties. Continuously monitoring business associate security and privacy programs is as critical as monitoring your own.

Poor cybersecurity practices cannot be taken lightly. In December 2018, twelve states filed a class action suit dating back to the May 2015 cyberattack on the electronic health record application WebHealth that resulted in unauthorized access of over 3.9 million records containing ePHI.

SecurityScorecard

Moreover, HIPAA may no longer be the only regulation with which the healthcare industry must comply. California's new privacy law is considered the beginning of America's move toward creating its own version of the European Union (EU) General Data Protection Regulation (GDPR). Thus, privacy must become an integral part of conducting business across all industries. Since HIPAA law focuses on ensuring privacy and protection of ePHI, it can be used as a model for protecting data to help comply with all new privacy laws. Ensuring continuous compliance and the implementation of a mature privacy program helps keep your data safe, regulators off your back, and your company name off the news.

To learn more about how healthcare organization have improved their cyberhealth please click here.

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.io

SecurityScorecard HQ
111 West 33rd Street
11th Floor
New York City, NY 10001

securityscorecard.com [800] 682 1707