SecurityScorecard

SecurityScorecard 2018 Healthcare Report

A Pulse on the Healthcare Industry's Cybersecurity Risks

securityscorecard.com [800] 682 1707

Overview

Since we issued our last report in 2016 on the cyberhealth of the healthcare industry, healthcare as a whole has dropped six places in our rankings. Healthcare organizations overall have struggled to keep up with growing cybersecurity demands and have increasingly fallen victim to sophisticated attackers.

At the same time, Electronic protected health information (ePHI) data remains an appealing target because it often contains social security, financial, health insurance, driver's license data, as well as immutable types of information that can be used to steal identities and commit fraud. In addition, hackers are exploiting configuration issues and other lapses in security best practices to destroy healthcare records or hold them for ransom.[1]

In this year's report, SecurityScorecard looked at more than 1200 healthcare companies from July 2017 through the end of the year and analyzed terabytes of information to assess risk across ten risk factors.

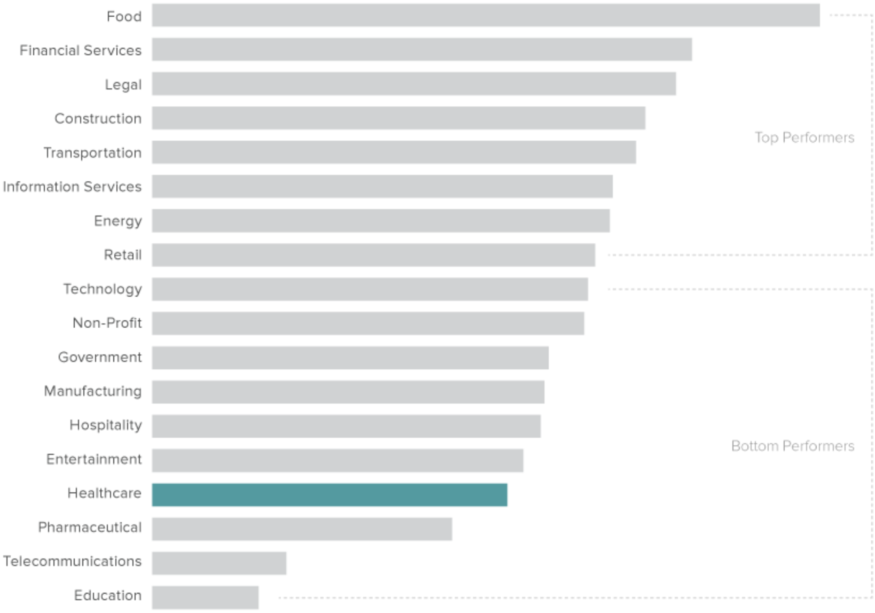
[1] http://www.healthcareitnews.com/news/hackers-are-ransoming-26000-unsecured-mongodb-databases-security-researchers-find

Key Insights:

- The healthcare industry ranks ranks fifteenth in terms of cybersecurity health when compared to 17 other major U.S. industries.
- The healthcare industry is one of the lowest performing industries in terms of endpoint security.
- Social engineering attacks continue to be a common attack vector.
- The most common cybersecurity issues in the healthcare industry relate to poor patching cadence.
- Healthcare organizations, even top performers, struggled with patching cadence and network security.

How the Healthcare Industry Measures up – or Doesn't?

The healthcare industry ranks fifteenth when compared to 17 other major U.S. industries. This poor ranking shows the challenges that many organizations in the healthcare industry face especially when compared to other industries, including legal and financial services, that typically collect high value personally identifiable information.

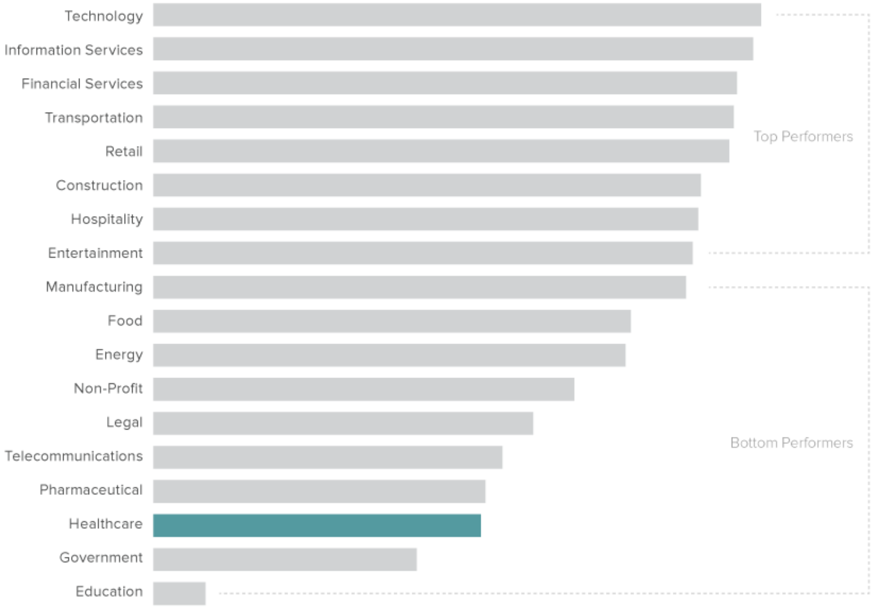


Healthcare records contain some of the most detailed personal information available, and healthcare organizations are not doing enough to protect this information. According to a January 2018 Futurum article, the current dark web rate paid for a health record ranges from $3 to $100 per record, depending on the depth of information.[2] Combine this with the fact that a breach can result in thousands of compromised patient records[3], hackers stand to make a substantial amount of money by selling this information to criminal syndicates across the globe. In addition, organizations that lack adequate cybersecurity capabilities face hefty fines from regulatory bodies, reputational damage, lawsuits, as well as lost revenue.

[2] Kramer, S. (2018, January 12). HITRUST Certification: Increase in HIPAA Breaches Means Brands Need More from Vendors. Retrieved from https://futurumresearch.com/hitrust-certification-increase-hipaa-breaches-means-brands-need-vendors/
[3] Protenus' Breach Barometer 2017 year-in-review available at https://www.protenus.com/press/press-release/56m-patient-records-breached-in-2017-as-healthcare-struggles-to-proactively-protect-health-data

The Healthcare Industry Ranks Near the Bottom in Terms of Endpoint Security

Securing endpoints can be a major challenge for healthcare organizations. Large healthcare organizations typically have thousands of endpoints while, due to a lack of resources, small and medium sized entities struggle to properly monitor and maintain their endpoints. The growth in IoT devices, smartphones, and tablets can add to this problem and make it very difficult for centralized IT departments to properly secure devices on their network. To compound the problem, these devices often store patient data and are the gateway to databases and other systems that contain ePHI.



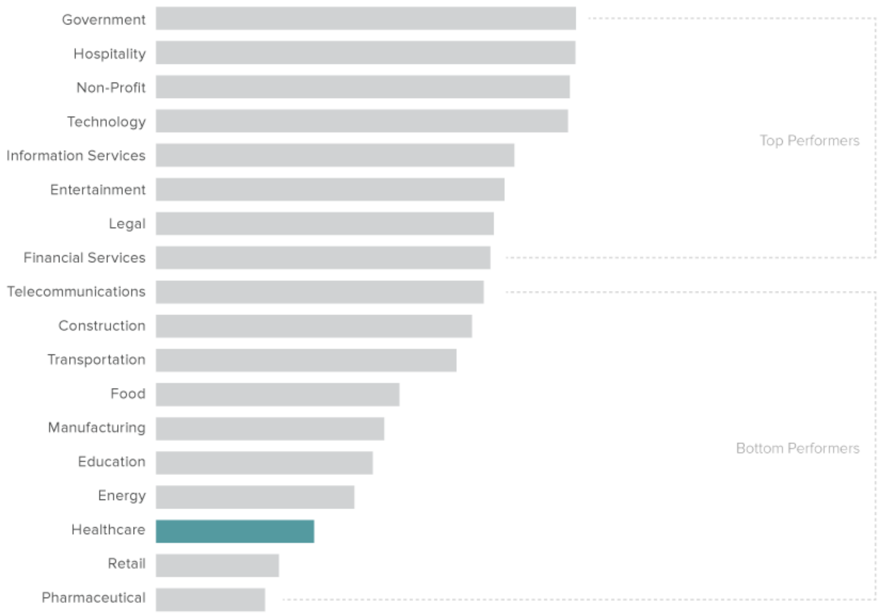
For the healthcare vertical, like most industries, protecting endpoints starts with securing employee devices such as laptops, cell phones, tablets, and other mobile devices that connect to a corporate wireless connection. However, because the healthcare industry is a favorite target for hackers, it's easy to imagine a scenario (such a scenario has also been demonstrated[5]) where exploiting a vulnerability in a wirelessly connected device could allow a hacker to gain access to ePHI or even worse, put a life in danger.

It only takes one outdated device to put an entire organization at risk. In many instances, poor performing organization have hundreds of endpoint security issues. This risk also extends to the broader ecosystem. Healthcare organizations who leverage third party providers also need to vigilantly monitor the security posture of these vendor and partners to limit exposure and ensure compliance.

[5] Marin, E., Singelée, D., Garcia, F. D., Chothia, T., Willems, R., & Preneel, B. (2016). On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. Proceedings of the 32nd Annual Conference on Computer Security Applications - ACSAC 16. doi:10.1145/2991079.2991094

Social Engineering: A Continuing Attack Vector for the Healthcare Industry

The healthcare industry ranks third from the bottom in terms of social engineering. Hackers often leverage social media and other pubic sources to identify human targets that can be easily exploited. Spoofing and phishing attacks are some of the most common types of attack vectors that leverage social engineering tactics. These types of attacks rely on tricking unsuspecting employees into revealing information via malicious websites, email, or over the phone. In addition, hackers leverage social engineering to deploy malware on a network, often by tricking an employee into opening an email containing a malicious payload.



Employees who reveal their company contact information on the web, including company email addresses, are generally considered easier targets for hackers. In addition, companies who have employees who regularly share this type of information in public forums are more likely to have a security policy training issue. This is a signal to hackers that those companies are particularly vulnerable to social engineering attacks.

Patching Accounts for the Most Prevalent Cybersecurity Issues in the Healthcare Industry

Here is a look at the top 5 most common cybersecurity issues in the healthcare industry:

1. Typosquatting
2. Slow patching cadence
3. Vulnerable host
4. Weak ciper
5. End-of-life date

Three out of these top five issues are related to patching cadence. Patching cadence refers to how quickly an organization updates its software once the vendor releases patches.

The Healthcare Industry's "C" Patching Cadence Grade Indicates a Need for Better Patch Management

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.

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.

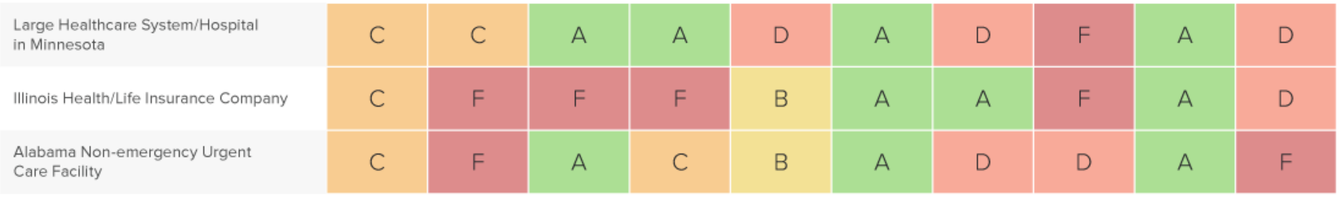
The sheer number of ongoing software patches often paralyzes organizations, keeping them from implementing the most critical repairs and updates. This opens breached companies to negligence claims and lawsuits. With so many vulnerabilities and security concerns, risk assessments that catalogue critical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

SecurityScorecard

A Look at the Top Cybersecurity Performers in the Healthcare Industry

The top performers in terms of cybersecurity health were as follows:

Entity	Total Score	Application Score	Cubit Score	DNS Health	Endpoint Security	Hacker Chatter	IP Reuptation	Network Security	Password Exposure	Patching Cadence
Florida Senior Primary Care Center	A	A	A	B	A	A	A	A	A	A
New York Human Body Visualization Platform	A	B	A	C	A	A	A	A	A	A
Minnesota Teleradiology Practice and Telemedicine Company	A	A	A	A	A	A	A	C	A	B
Michigan Homehealth and Hospice Facilty	A	B	B	D	A	A	A	A	A	A
California Post-Accute Care, Hospice and Assisted Living Facility	A	A	A	B	A	A	A	B	A	B
Tennessee Health Insurance Provider	A	A	A	B	B	A	A	A	A	A
Texas Prosthetics Company	A	A	C	C	A	A	A	C	A	A
Kentucky Rehabilitation Services	A	D	A	D	A	A	A	A	A	A
Large Healthcare System in California.	A	A	A	A	A	A	A	D	A	B
California Dental Provider	B	A	A	B	A	A	A	C	A	C
Califoria Small Community Hospital	B	A	A	B	D	A	A	B	A	B
Large Healthcare System in Tennessee	B	A	A	B	A	A	A	C	A	C
NJ Medical Urgent Care Center	B	B	B	A	B	A	A	C	A	B
Kansas Mental Health Center	B	A	A	C	B	A	A	C	A	C
New York Large Healthcare System	B	A	A	A	C	A	C	A	A	A
NY Large Healthcare System	B	A	A	D	A	A	A	D	A	C
California Electronic Health Records Company	B	D	A	A	A	A	A	F	A	B
Alabama Large Pediatric Hospital	B	D	A	C	C	A	A	B	A	D
Hospital in West Virginia	B	A	A	C	D	A	A	D	A	B
New Mexico Large Healthcare System	B	C	A	C	A	A	A	F	A	D
Florida Developmental Disabilities Medical Treatment Facility	B	F	A	D	A	A	A	C	A	F
New York Pharmaceutical Company	C	A	A	B	A	A	D	D	A	D
Company That Markets and Distributes Over-The-Counter Healthcare and Cleaning Products in New York	C	A	A	A	B	A	D	F	A	F
California R & D Company For Animal Health	C	C	A	B	A	A	D	F	A	F



Large Healthcare System/Hospital in Minnesota	C	C	A	A	D	A	D	F	A	D
Illinois Health/Life Insurance Company	C	F	F	F	B	A	A	F	A	D
Alabama Non-emergency Urgent Care Facility	C	F	A	C	B	A	D	D	A	F

From the above, it's easily seen that even top performers struggle with patching cadence. Network security is another area of weakness for top performers. Examples of network security hacks include exploiting vulnerabilities such as open ports, insecure or misconfigured SSL certificates, or database vulnerabilities.

Before going deeper into the findings, you may want to review what SecurityScorecard scores on; See our security rating overview page and scoring methodology paper for this information.

HIPAA's Utility as a Reference for Top Cybersecurity Performers

When addressing vulnerabilities and high-risk network security concerns on their externally facing systems, healthcare companies may make reference to the guidance provided by HIPAA.

For example, on the frequency of risk mitigation efforts, HIPAA states:

> *"Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to [electronically protected healthcare information] ePHI and detect security incidents, periodically evaluate the effectiveness of security measures put in place, and regularly reevaluate potential risks to ePHI."*

Organizations have to be diligent in their cybersecurity efforts to secure Protected Health Information (PHI) and ensure ongoing compliance with the HIPAA regulations and HITECH act. Most importantly, organizations must avoid ending up on the OCR breach portal, where in addition to hefty fines, they may also face reputational impacts.

To improve in the two critical areas of network security and patching cadence, healthcare companies should:

- Frequently patch systems as recommended by system and application vendors
- Ensure only required ports are open on systems
- Frequently scan to identify system vulnerabilities
- Prioritize addressing system vulnerabilities according to risk severity
- Ensure SSL certificates are current and enabled properly
- Review and remedy other issues reported by SecurityScorecard

Visibility into the Problem is the First Step

The healthcare industry faces a unique set of circumstances that puts organizations, providers, and patients at risk. While there is no silver bullet, maintaining best practices and proper IT hygiene can prevent most breaches from occurring. Unfortunately, many healthcare organizations have not been able to develop the cybersecurity capabilities nor the muscle memory to defend ePHI and other data from hackers. While the road to building a more secure healthcare industry is long, healthcare security leaders can leverage solutions designed to help organizations like theirs quickly and efficiently monitor the health of their own IT infrastructure as well as that of their entire ecosystem. Gaining visibility into the problem is truly the best first step.

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.com
@security_score

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