INTERNET RISK SURFACE IN THE HEALTHCARE SECTOR

Benchmarking digital risk factors facing healthcare institutions

A collaborative research project between RiskRecon, the Cyentia Institute, and Health-ISAC

riskrecon
mastercard

119 Cyentia INSTITUTE

HEALTH - ISAC NAVIGATOR™ PROGRAM

CISOs and Security Directors can use this report to benchmark their firm's risk surface against peers as well as communicate successes and challenges to the Board.

Third-party risk managers will discover key factors and firmographics helpful to prioritizing risk from different types of healthcare firms in their network.

Internal Security Professionals can use these findings to identify common risk dimensions affecting Internet-facing infrastructure they manage and defend on a daily basis.

Introduction & Key Findings

According to statistics from the U.S. Dept. of Health and Human Services (HHS), 861 breaches of protected health information have been reported over the last 24 months under the disclosure requirements set forth in 45 C.F.R. § 164.408. These numbers don't exactly offer a good prognosis of cybersecurity among healthcare providers. In this report, we diagnose factors contributing to this state of affairs and share important findings to aid those managing cyber risk in the Healthcare sector.

1. Healthcare boasts one of the highest average rates of severe security findings. Those rates also vary hugely across institutions, meaning the worst exposure rates in Healthcare are worse than the worst exposure rates in any other sector.

2. But not all types of healthcare organizations share the same struggles. For example, the rate of severe security findings in the smallest providers is 3x higher than that of the largest providers.

3. Subsectors within Healthcare show different trends as well. Hospitals have a much larger Internet surface area, but maintain relatively low rates of security findings. Nursing care facilities show the opposite—small footprint with big exposures.

4. Wondering about the broader Healthcare supply chain? You should. Our analysis of equipment manufacturers, pharmaceutical producers, insurance providers, IT services, etc. may surprise you.

5. Many other challenges and risk factors exist. For instance, the industry average rate of severe security exposures in critical cloud-based assets is 10x that of assets hosted on-premises.

RiskRecon and the Cyentia Institute published the Internet Risk Surface and Cloud Risk Surface reports in mid-2019. These studies analyzed data from RiskRecon spanning over five million Internet-facing hosts from ~20,000 organizations as well as major hosting providers around the world. The primary goal was to explore dimensions of interconnectivity, interdependence, and risk exposure that define the era of digital transformation. This report leverages the same dataset and methodology as those publications but focuses exclusively on the Healthcare sector.

Dimensions of the Healthcare Sector Risk Surface

As Digital Transformation ushers in a plethora of changes, critical areas of risk exposure are also changing and expanding. We view the risk surface as anywhere an organization's ability to operate, reputation, assets, legal obligations, or regulatory compliance is at risk. The aspects of a firm's risk exposure that are associated with or observable from the internet are considered its internet risk surface. In Figure 1, we compare five key dimensions of the internet risk surface across different industries and highlight where the Healthcare sector ranks among them:

- **Hosts:** Number of internet-facing assets associated with an organization.
- **Providers:** Number of external hosting providers.
- **Geography:** Measure of the geographic distribution of a firm's hosts.
- **Asset Value:** Rating of the data sensitivity and business criticality of hosts based on multiple observed indicators. High-value systems including those that collect PHI, GDPR, and CCPA regulated information.
- **Findings:** Security-relevant issues that expose hosts to various threats, following the CVSS rating scale.

The values recorded in Figure 1 for these dimensions represent what's "typical" (as measured by the mean or median) among organizations within each industry. While there is a large amount of variation within each industry, what you see here is the general pattern. The blue highlights trace the ranking of Healthcare along each dimension.

FIGURE 1: COMPARISON OF RISK SURFACE DIMENSIONS AMONG SECTORS WITH HEALTHCARE HIGHLIGHTED

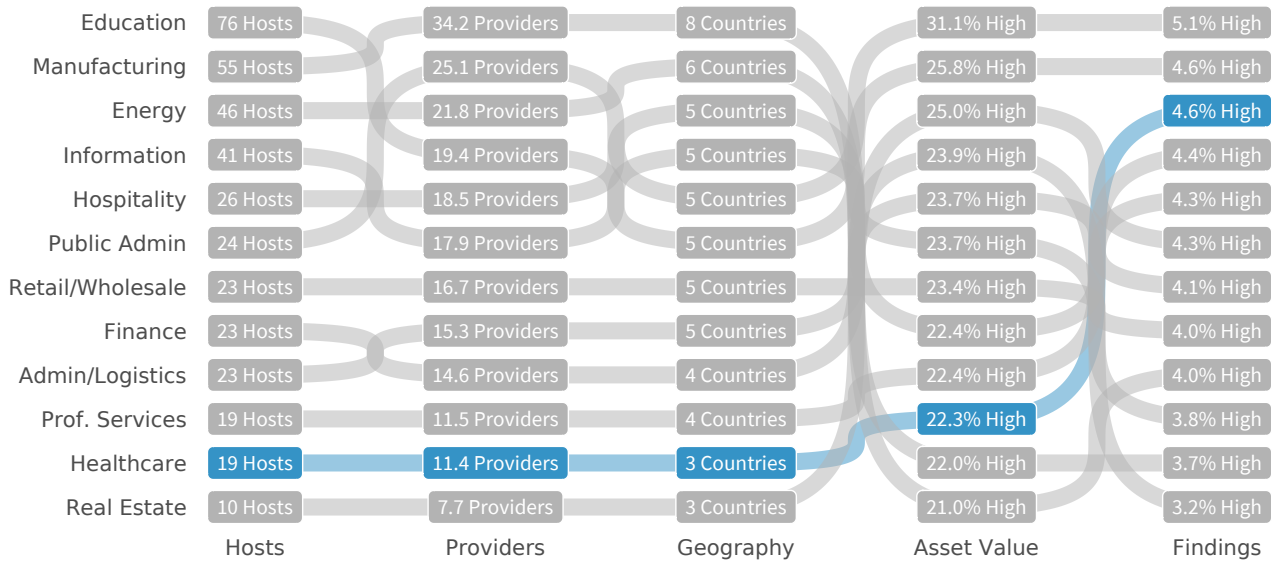


Figure 1 makes it clear that Healthcare consistently ranks low in four of five risk surface dimensions. The prototypical healthcare firm has fewer hosts scattered across fewer service providers and global locations than other sectors, and a lower proportion of those assets exhibit high-value functions. That trend reverses for the findings dimension, where Healthcare's rate of severe security findings ranks among the highest of all sectors.

Healthcare's high exposure rate indicates that managing a comparatively small Internet footprint is a big challenge for many organizations in that sector. This becomes even more apparent when examining the distribution of hosts with severe findings in Figure 2. Blue dots mark the average exposure rate for the entire sector (which corresponds to values in Figure 1), while the grey bars indicate the amount of variation among individual organizations within each sector. This reveals that the worst exposure rates in Healthcare are even worse than the worst rates in any other sector.

FIGURE 2: DISTRIBUTION OF HOSTS WITH HIGH OR CRITICAL FINDINGS IN EACH SECTOR

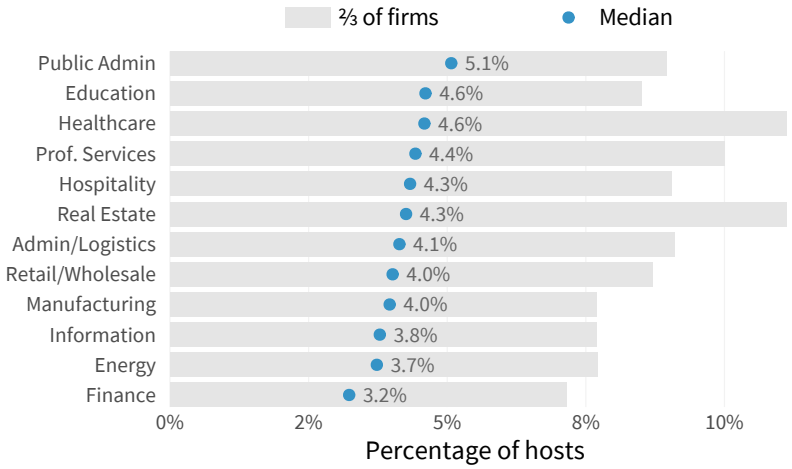


Figure 2 shows Healthcare boasts one of the highest average rates of severe security findings (see blue dots). It also exhibits huge variation (see gray bars), meaning the worst exposure rates in Healthcare are even worse than the worst rates in any other sector.

We also thought it would be worthwhile to briefly inspect how the size of healthcare institutions affects security posture. Bigger providers understandably have a larger risk surface stemming from more employees, more hosts, more services, and more third parties operating across more service areas. It could be argued that gives smaller institutions a security advantage because they don't contend with that scale and complexity. The data from Figure 3, however, does not support that argument.

FIGURE 3: HOSTS WITH HIGH OR CRITICAL FINDINGS IN HEALTHCARE PROVIDERS BY EMPLOYEE COUNT

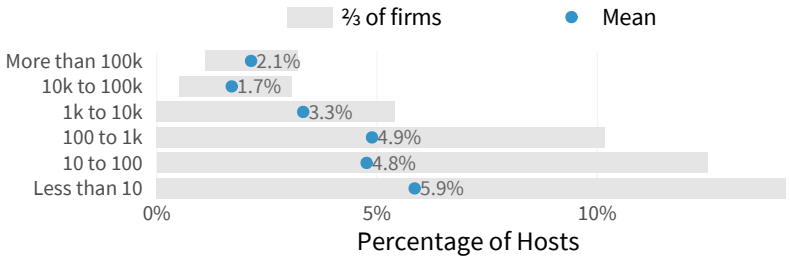


Figure 3 reveals that severe security findings decrease as employees increase. This likely reflects growing resources, maturity, and governance.

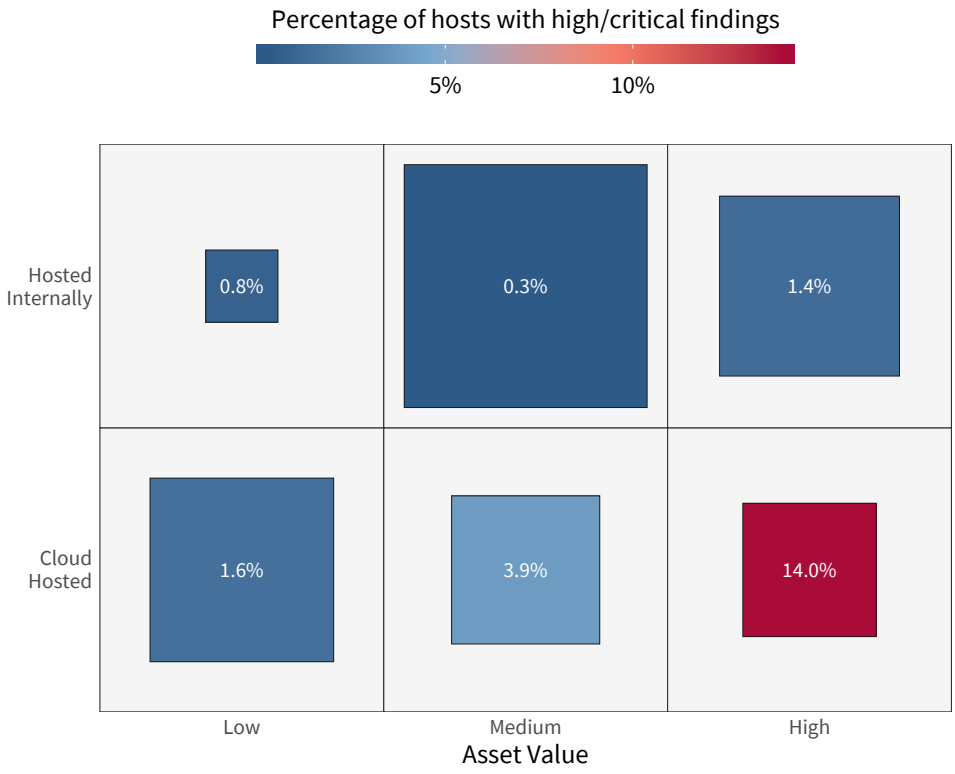
Regardless of size, the fact that healthcare institutions face an uphill battle against security hygiene is no surprise to anyone responsible for that critical mission. But we hope these findings add some helpful context regarding the extent of that battle and where's it raging most intensely. If there's a silver lining here, it's that the risk surface isn't (typically) as distributed as in some other sectors. That suggests gaining the visibility needed to pinpoint and rectify exposures in that surface is feasible.

> The silver lining is that gaining the visibility needed to pinpoint and rectify exposures in the Healthcare risk surface is feasible.

Security Exposures in Healthcare Cloud Deployments

We now know healthcare firms struggle to minimize security findings but are those struggles the same across all infrastructure? Figure 4 answers that question by featuring four of the five key risk surface dimensions: the proportion of hosts (square size), asset value (columns), hosting location (rows), and the rate of severe security findings (color scale and value label). This view facilitates a range of comparisons, including the relative proportion of assets hosted internally vs. in the cloud, how asset value distributes across hosting locales, and where high-severity issues accumulate.

FIGURE 4: COMPARISON OF SECURITY FINDINGS BY ASSET VALUE AND HOSTING MODELS IN HEALTHCARE



Healthcare's severe finding rate for high-value assets in the cloud is 10x that of on-prem! That's the largest on-prem vs. cloud exposure imbalance of any sector.

10x
higher exposure rate in cloud assets

High-value assets collect sensitive information or authenticate user identity. Medium-value assets do not perform those sensitive functions but are network neighbors to those that do. Low-value assets are brochure sites that collect no private data and offer no foothold into the network. Figure 4 indicates healthcare firms host a majority of their Internet-facing systems on-prem but do leverage the cloud for low-value assets. It's apparent that security exposures concentrate more acutely in high-value assets hosted in the cloud.

Given that cloud vs. on-prem exposure disparity, we feel the need to caution against jumping to conclusions. We could interpret these results to proclaim that the cloud isn't ready for healthcare applications and should be avoided. Another interpretation, however, might suggest that it's more about institutional readiness for the cloud than the inherent insecurity of the cloud. Either way, these results should encourage all healthcare organizations migrating to the cloud to assess their capabilities for handling the paradigm shift that is cloud security.

For those wondering how Healthcare's "health chart" compares to other sectors, Figure 5 is just what the doctor ordered. We're not labeling exposure rates in this version because a) spacing issues and b) that's not the point. The goal here is to aid general visual comparisons across sectors. It's clear that no other sector matches Healthcare exactly. Sure, that bright red square for Hospitality suggests both sectors struggle to secure critical assets in the cloud, but the similarities end there. Bottom line—Healthcare faces some unique challenges with respect to managing its risk surface. And while that's probably not news to anyone reading this, it's helpful to see the data illustrate and validate those challenges.

> We could interpret these results to proclaim that the cloud isn't ready for healthcare applications and should be avoided. But it's more about institutional readiness **for** the cloud than the inherent insecurity **of** the cloud.

FIGURE 5: COMPARISON OF SECURITY FINDINGS BY VALUE AND HOSTING MODELS ACROSS SECTORS

Figure 5 puts Figure 4 (previous page) into a broader perspective. In addition to the highest rate of severe findings (see Figure 2), Healthcare exhibits the largest on-prem vs. cloud exposure imbalance of any sector.

It must also be noted that not all cloud environments are the same. Our Cloud Risk Surface report discovered an average 12X difference between cloud providers with the highest and lowest exposure rates. We believe this says more about the users and use cases of various cloud platforms than intrinsic security inequalities. At the same time, we recommend evaluating cloud providers based on features as well as resources they make available to assist customers in securing their environments. Certain clouds are undoubtedly a better match for healthcare use cases while others less so.

Risk Surface of Healthcare Subsectors

Having compared Healthcare to other sectors, we now examine major subsectors within Healthcare according to the following NAICS designations:

- **Ambulatory Health Care:** Offices that provide a range of outpatient services.
- **Hospitals:** Provide inpatient medical, diagnostic, and treatment services.
- **Nursing and Residential Care:** Provide nursing, supervisory, or care to residents.
- **Social Assistance:** Provide a variety of social services directly to clients.

Figure 6 compares these Healthcare subsectors along the same dimensions used in Figure 1. Here we see that hospitals generally maintain a much larger Internet surface area (hosts, providers, countries), but a substantially lower rate of security findings. We take a small measure of comfort in that result, despite hospitals being more routinely impacted than any other Healthcare subsector in our study of multi-party cyber incidents.[1]

FIGURE 6: COMPARISON OF RISK SURFACE DIMENSIONS AMONG HEALTHCARE SUBSECTORS

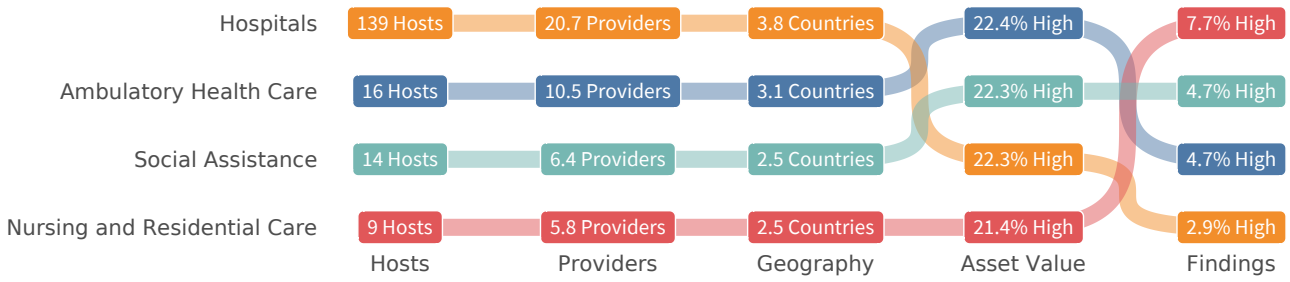


Figure 6 compares Healthcare subsectors along key risk dimensions. Note the shifts in ranking among columns. Nursing care facilities, for example, show the smallest Internet footprint but the highest levels of exposure.

The data is not at all comforting with respect to the Nursing and Residential Care subsector. It has the smallest Internet footprint yet the highest levels of exposure. Outpatient (Ambulatory) and Social services mostly fall in between hospitals and nursing facilities. Overall, these results reinforce the lesson that dimensions of the Internet risk surface vary substantially, even among organizations in the same industry. Thus, such distinctions need to be considered when assessing and managing third-party risk associated with different types of healthcare providers.

> We take a small measure of comfort in hospitals having the lowest rate of severe security findings, despite them being impacted more than any other subsector in our study of multi-party cyber incidents.

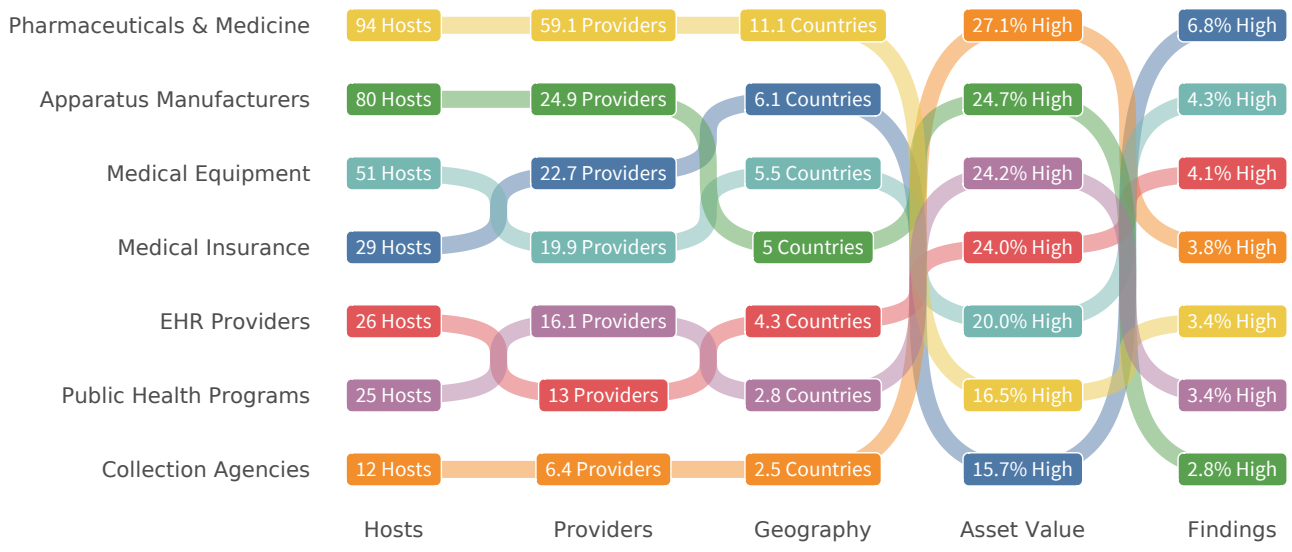
[1] See Ripples Across the Risk Surface report: https://www.riskrecon.com/ripples-across-the-risk-surface

Risk Surface of the Healthcare Supply Chain

While the types of organizations covered in the previous section officially fall under the Healthcare designation according to NAICS, it's important to realize that the broader healthcare ecosystem spans numerous industries. Hospitals, for instance, have extensive supply chains that include equipment manufacturers, pharmaceutical producers, insurance providers, IT services, government agencies, and many more. Such entities often have deep connections into the healthcare provider's facilities, operations, and information systems. This, of course, has significant ramifications for third-party risk management.

A sampling of these non-Healthcare industries is given in Figure 7, and it tells a pretty interesting story for those who follow the threads. "Big Pharma" has the biggest footprint in terms of hosts, 3rd party service providers, and countries of operation. They appear to have discovered the right prescription for keeping that large Internet footprint relatively hygienic. Manufacturers of various types of healthcare apparatus and instruments show a similar profile of extensive assets yet fewer findings. It's rather interesting, therefore, that the remaining industry in the manufacturing sector—Medical Equipment—exhibits an inverted ratio for exposure and Internet surface area. Something to consider for healthcare firms that are highly integrated with third parties that manufacture medical equipment.

FIGURE 7: COMPARISON OF RISK SURFACE DIMENSIONS ACROSS THE BROADER HEALTHCARE ECOSYSTEM



> It's important to realize that the broader healthcare ecosystem spans numerous industries. Such entities often have deep connections into the healthcare provider's facilities, operations, and information systems. This, of course, has significant ramifications for third-party risk management.

As a reminder that not all supply chains are physical, the digital supply chain is well-represented in Figure 7. The information-heavy industries of medical insurance, electronic health records (EHR) systems providers, and collection agencies occupy three of the top four slots for the highest rate of security findings. And lest one doubt that Collection Agencies deserve to be in the list, consider the example of the American Medical Collection Agency (AMCA). A breach of its systems in May 2019 compromised the personal information of over 24 million individuals. Most of the individuals affected had no direct relationship with AMCA; they provided their data to other healthcare entities and those entities sent the data to AMCA for debt collection. Even though only AMCA's systems were compromised, those other organizations suffered substantial financial fallout from the breach.

Bottom line: when considering where the next breach might strike, don't neglect to assess the supply chain and broader third-party networks. Healthcare is much more than meets the eye.

A note from Errol Weiss, CSO at H-ISAC

"In 2020, Health-ISAC members across healthcare delivery, big pharma, payers and medical device manufacturers saw increased cyber risks across their evolving and sometimes unfamiliar supply chains. Adjusting to the new operating environment presented by COVID-19 forced healthcare companies to rapidly innovate and adopt solutions like cloud technology that also added risk with an expanded digital footprint to new suppliers and partners with access to sensitive patient data. This report is an important read for any CISO or third-party risk practitioner to gain insights on measuring risk surface in the healthcare industry."

Why are we doing this?

Managing risk across Internet-exposed assets and across extensive third party relationships is one of today's top cybersecurity challenges. Understanding that risk surface through research as you see in this report is one way that RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments. Learn more: www.riskrecon.com

Two Things to Consider

1. Change the way you think about managing third-party risk. Consider the rigor that goes into assessing and mitigating cyber risk internally. Then compare that to how third-party risk is often handled. Would you base your internal risk assessments on surveys and attestation? Of course not. Why then has this become the standard for third parties?

2. Managing risk—whether internal or third-party—requires focus. There are simply too many things to assess and do, giving rise to the endless "hamster wheel of risk management." A better approach starts with obtaining an accurate picture of your risk surface and the critical exposures across it (which includes third-party relationships).

riskrecon
mastercard

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

www.riskrecon.com

119 Cyentia INSTITUTE

The Cyentia Institute produces compelling, data-driven research with the aim of improving knowledge and practice in the cybersecurity industry.

www.cyentia.com

HEALTH - ISAC NAVIGATOR™ PROGRAM

Health-ISAC Inc. is a trusted non-profit community and forum for coordinating, collaborating and sharing cyber threat intelligence and best practices with each other.

www.h-isac.org

How To Use Findings From This Report

With multiple roles at healthcare providers responsible for managing third-party risk in multiple capacities, it's important to understand who and how to take action. Not all findings are applicable to everyone, so below you'll find a checklist of ways to leverage these insights functionally into your role.

CISOs and Security Directors

- Its time for healthcare CISO's to move beyond managing vulnerabilities and start managing their risk surface on the Internet. Since the rate of critical findings in healthcare is the worst comparably to any other sector in the broader data set, it is critical to assess your current management of sensitive data and functionality that has exposure to the Internet. Are you concentrating risk in as few systems as possible? Where are those high-risk systems hosted? As this study shows, leading sectors are paying attention to these factors.
- The healthcare sector is struggling to achieve the quality of cybersecurity in cloud-hosted environments that they have realized on-prem. If you think you are ready, you'll have to be doing something dramatically different than your peers. Is that really the case?
- While your organization may be doing well, data shows your critical vendors and partners in other sectors may not be. Does your third-party risk team have the resources to ensure they perform to your standards? What can you learn from your critical, yet low-risk vendors?

Third-Party Risk Teams

- Consider shaping the breadth and depth of your third-party assessments based on industry. The data suggest it is worth allocating more resources to challenged sectors such as healthcare and professional services while backing off on leaders such as credit card issuers and commercial banks.
- Effective control of cloud computing is problematic for all industries. Do you know the extent of your vendor's cloud-computing usage? Is your cloud assessment methodology holding vendors to a high standard of performance?

Internal Security Teams

- It is on you to define and execute on the strategies to successfully manage your risk surface across all dimensions. Implement processes to shape your risk surface to be more defensible even if it means accepting the reality of poorly performing risk scoring as a starting point to build a more robust program.
- The patterns and expertise for managing on-prem computing were developed over decades. Today's pressing threat pressure does not provide the same luxury of time for figuring out cloud computing security. It is on you to raise the red flag if cloud computing is moving faster than your teams are capable of securing it.

Something EVERYONE Can Do IMMEDIATELY

If this report got you thinking about the state of your own firm's Internet risk surface, take action now by downloading our Third Party Risk Management Playbook.