REPORT

The Cyber Risk Landscape of the U.S. Healthcare Industry

SecurityScorecard

Introduction

This paper surveys cybersecurity hygiene and risks in U.S. healthcare. It follows up on prior SecurityScorecard research on third-party breaches, which found that healthcare has some of the highest rates and numbers of such incidents. Our separate research on the S&P 500 found that its member healthcare companies had some of the lowest security ratings on that U.S. stock index.

Reinforcing the first point, the release of our third-party breach report nearly coincided with one of the most disruptive cyber attacks in the history of healthcare. The massive payment disruptions for U.S. healthcare providers resulting from the February 2024 BlackCat ransomware attack on Change Healthcare was an extreme yet highly illustrative example of the third-party risks stemming from high interdependence among healthcare organizations. As that example demonstrated, BlackCat did not even have to breach third parties to have a major negative impact on them; it simply disrupted the payment processes on which so many providers depended. The consequences could have been worse if BlackCat had used its unauthorized access to Change Healthcare as an attack vector to compromise the networks of care providers.

This paper aims to help healthcare organizations and their partners reduce such risks. It examines the security ratings of healthcare organizations to identify those areas in which they score lowest and the specific issues with the most negative impact on their ratings. It examines recent healthcare breaches, including ransomware attacks, as many ransomware operators prefer healthcare targets.

Key Findings:

1 Security ratings in our sample were higher than expected. Possible reasons for this variance include: our sample of large, publicly traded companies, which often have better security; and the majority of Pharmaceuticals & Biotechnology companies in our sample.

2 Manufacturers of medical devices and distributors of medical equipment and supplies were the only sector of this industry with noticeably lower scores. We attribute this variance to differences in their attack surface, some of which may resemble those of non-healthcare manufacturers more than those of other healthcare organizations.

3 Our search for the general factors that lower security ratings in this industry identified two key areas of concern: Application Security and Endpoint Security. Application Security issues are the most common sources of score-lowering risk, but the severity of those issues is often low or medium. In contrast, Endpoint Security issues are less common as the source of the most negative score impacts, but when they do have that greatest negative impact, it tends to be more severe than that of other security factors.

4 Many different Application Security issues that contribute to this factor's widespread negative impact on scores. In contrast, low Endpoint Security scores stem mostly from the use of outdated web browsers; other Endpoint Security issues are much less common.

5 9% of the organizations in our sample had either a publicly reported breach in the past year or evidence of a compromised machine in the past 30 days (if not both). 5% had a publicly reported breach in the past year. 6% had compromised machine in the past 30 days. 2% had both.

Key Findings:

6 Medical device manufacturers and distributors of medical equipment and supplies were disproportionately common in the above subset of our sample, while Pharmaceuticals & Biotechnology companies were less common in it than in our overall sample. The former sector was also overrepresented in the lowest-scoring 10% subset of our sample.

7 Ransomware can affect all four healthcare sectors, not just the care providers that have been the most well-known examples. Risks stemming from such attacks include: the use of patient data for fraud; the threatened exposure of high-value pharmaceutical IP for extortion; and the disruption of business processes, as in the case of Change Healthcare.

8 Healthcare organizations can have third-party breaches via either vendors with access to their data or vulnerable software. The massive MOVEit campaign of mid-2023 had major third-party impacts on healthcare because it involved both types of third-party breaches.

9 Other sources of third-party risk for healthcare organizations include: specialized third-party platforms or other technology designed specifically for the healthcare industry; the outsourcing of non-clinical functions, such as administration and finance-related functions, to third-party vendors; and the delegation of specialized clinical tasks, such as lab tests and diagnostic imaging, to third-party care providers.

Methodology

We further limited the scope to the 500 largest healthcare companies whose stock is publicly traded in the U.S., based on their market capitalization.

We defined a sample small enough to be manageable but big enough to yield useful statistics. We focused on U.S. healthcare for our primarily U.S. audience but also for substantive reasons. The U.S. is the world's largest economy and thus a top target for criminals for that reason. Also, for its linguistic accessibility. The use of the world's lingua franca facilitates reconnaissance and social engineering attacks on English speakers and use of their data. U.S. healthcare also differs in significant ways from that of other countries with similar political systems and economies.

This list does include some businesses with non-U.S. operations. The role of large multinational corporations in the U.S. economy and its global reach makes exceptions to our domestic U.S. focus unavoidable.

Covering the financially largest companies aims to ensure that our sample includes companies with greater impact on the market and the patient pool. It also echoes the targeting of ransomware operators, who often choose targets on the basis of financial criteria. Many of them believe that companies with more revenue or higher market value can pay higher ransoms.

We divided this industry into four sectors:

Front-line care providers, as well as specialized vendors that support their services;

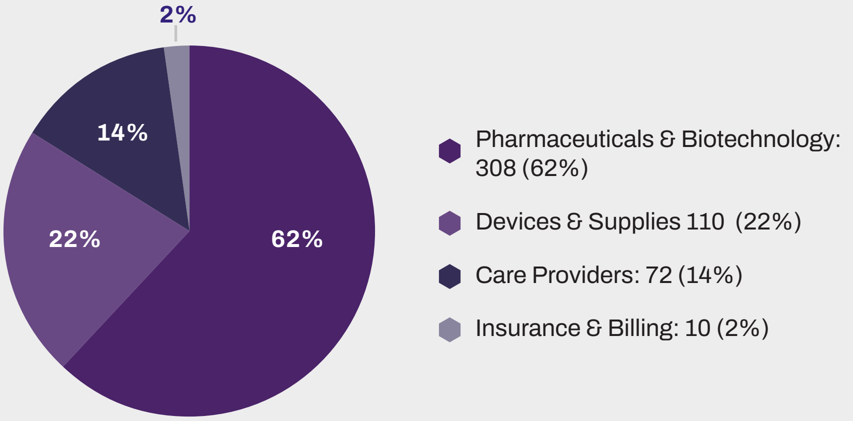
Health insurance companies as well as billing & revenue cycle management companies

Pharmaceutical, life sciences, and biotechnology companies

Medical device manufacturers and distributors of medical equipment and supplies.

DISTRIBUTION OF SAMPLE BY SECTOR

This sample of 500 companies had this distribution of companies in each sector:



This distribution raises key points. Much coverage of cyber attacks on healthcare focuses on care providers, but they constitute only a fraction of this sample. Many care providers would not fit our criteria, as they are often small or medium-sized businesses or even non-profit, academic, or religious organizations. This shift away from the usual emphasis on care providers is nonetheless helpful in developing a broader and more holistic perspective on this large, diverse industry.

From our finance-centric perspective, Pharmaceuticals & Biotechnology companies have greater significance. These capital-intensive businesses often make massive investments in extremely high-value intellectual property (IP). Their high-value IP makes them more desirable targets for both ransomware operators and state-sponsored cyber espionage groups. The high value of pharmaceutical IP makes it an ideal target for the data disclosure threats of many ransomware operators. Some pharmaceutical IP is of high enough strategic value that foreign governments, such as those of China, Russia, Iran, and North Korea, also seek to obtain it via cyber espionage.

The low proportion of health insurance providers in our sample came as a surprise. We opted to retain this category despite its small size because some insurers are so large that their impact on the industry is impossible to ignore. The widespread disruptions to care providers resulting from the ransomware attack on Change Healthcare, a subsidiary of one of these huge companies, illustrates why it is important to cover them, even if they are few in number. Indeed, the heightened “concentration risk” of having a relatively small number of companies play such a critical role in the market makes it even more imperative to cover them.

General Statistics

The mean score for these 500 companies was 88; the median was 89. The global cross-industry mean for the 12 million organizations in our platform is 86. These scores were the same as those of members of the S&P 500 stock index. These scores were also somewhat higher than those of the top 150 technology vendors, whose mean and median scores were 84 and 87, respectively.

These respectable scores are at odds with the common perception of substandard security in this industry. Our broader perspective on this industry, with over half of our sample coming from the often more well-funded Pharmaceuticals & Biotechnology sector, may correct or at least add nuance to this perception. Prior SecurityScorecard research found strong correlations between financial means and security hygiene. Security costs money, and organizations with more money, such as many of those in our sample, thus often tend to have stronger security.

The division of our sample into four different sectors also yielded little variation other than somewhat lower mean and median scores in the Devices & Supplies sector. Average and median scores in the three other sectors were consistent with those of the whole sample. Vulnerable medical devices are well-known as a distinctive risk factor in this industry, but mainly for the care providers that deploy them in their attack surfaces, rather than the companies that manufacture or distribute them. The attack surfaces of some medical device manufacturers may have more in common with those of non-medical manufacturers than they do with organizations in other healthcare sectors. Complex manufacturing environments, such as those with Industrial Control Systems (ICS), introduce more layers of security risk and new points of failure. We will review ratings for this sector separately below to gain further insight into these lower scores.

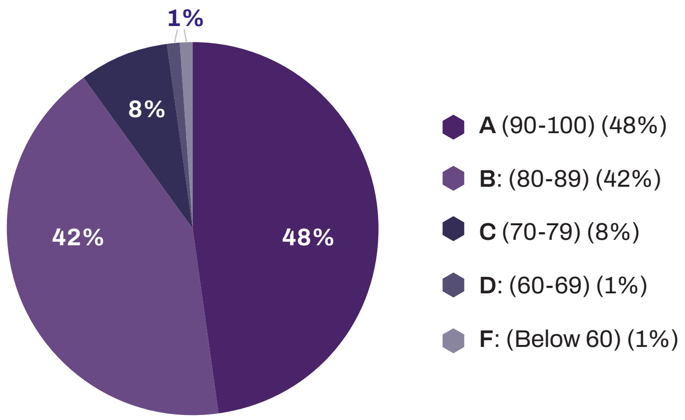
AVERAGE & MEDIAN SCORES FOR EACH HEALTHCARE SECTOR

Pharmaceuticals & Biotechnology	89/89
Devices & Supplies	86/87
Care Providers	89/89
Insurance & Billing	89/89

The distribution of letter scores for the numerical grades of these 500 organizations paints a generally favorable portrait. 90% of the sample had either strong "A" or good "B" ratings. Only 10% had weak "C" or lower ratings. The only anomaly in this distribution is that there were slightly more "F"s than "D"s (it usually is the other way around). According to our ratings methodology, a "B" rating indicates a 2.9x greater likelihood of a breach than an "A"; a "C" rating indicates a 5.4x greater likelihood of a breach; a "D" rating indicates a 9.2x greater likelihood of a breach; and a "F" rating indicates a 13.8x greater likelihood of a breach.

DISTRIBUTION OF LETTER SCORES

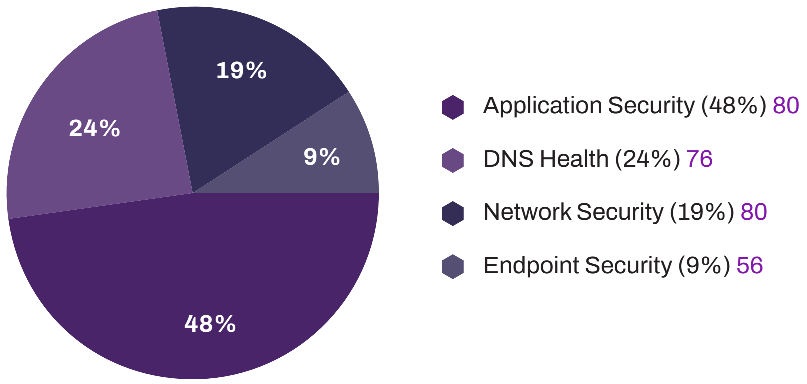
We will further examine the bottom 10% with the lowest ratings as a special subset below.



Score Factors and Problem Areas

For each of the 500 organizations in our sample, we identified the one out of the ten scoring factors for which each organization earned its lowest score. The mean lowest score in any scoring factor for all 500 organizations was 77; the median was 80. The lower mean indicates that a small number of extreme low values are dragging down the average of the whole sample.

PERCENTAGES OF ORGANIZATIONS with their Lowest Score Factor in Each Area, and their Average Scores in Those Lowest-Scoring Areas



What types of relationships are responsible for third-party breaches?

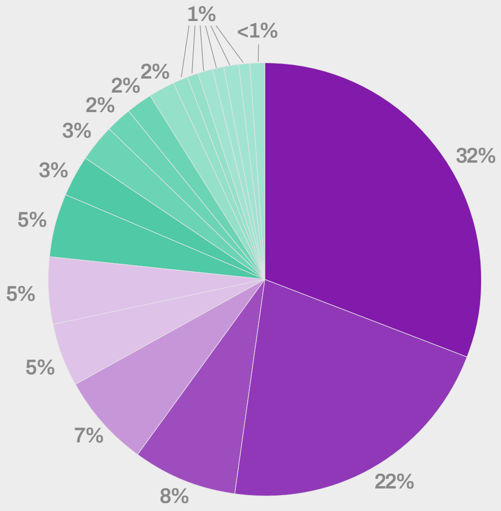
Four of the ten factors by which we rate security did not appear on the list: Cubit Score, IP Reputation, Social Engineering, and Information Leak. Two appeared so rarely (once each) that they warrant no further consideration: Hacker Chatter and Patching Cadence. Two companies had perfect scores (100) and thus lacked low-score areas. Only four scoring areas were truly consequential: Application Security, DNS Health, Network Security, and Endpoint Security.

Application Security was clearly the most common problem area. Nearly half of the companies in our sample (239 organizations, or 48%) had their lowest scores in this area - more than twice as many as the next-most common low-scoring area (DNS Health, which had 24%).

The average Endpoint Security score (56) for the relatively small number and percentage of companies scoring lowest in that area (43 organizations, or 9%) was well below norms for the overall sample (77/80). Endpoint Security may be the weakest area for the smallest number of companies, but it has a more negative impact on those few companies that perform worst in it.

Our researchers delved further into our ratings in search of specific issues responsible for the lower scores. Below is a breakdown of the issues that had the single-most negative impacts on organizations' scores. For those individual issues with fewer than 5 findings (which would equal 1% of the sample), we consolidated them as "Miscellaneous" under the rubric of the relevant score factor.

ISSUES WITH THE MOST NEGATIVE IMPACT ON SCORES



Redirect Chain Contains HTTP (32%)
SSL/TLS Service Supports Weak Protocol (22%)
Unsafe Implementation of Subresource Integrity (8%)
Outdated Web Browser Observed (7%)
SPF Record Contains a Softfail without DMARC (5%)
Website Copyright is Not Current (5%)
Miscellaneous Application Security Issues (5%)
SPF Record Missing (3%)
Website References Object Storage (3%)
Site Does Not Enforce HTTPS (2%)
Session Cookie Missing "HttpOnly" Attribute (2%)
Session Cookie Missing "Secure" Attribute (2%)
Site Does Not Use Best Practices Against Embedding of Malicious Content (1%)
Miscellaneous Application Security Issues (1%)
Content Security Policy is Missing (1%)
Miscellaneous DNS Health Issues (1%)
Miscellaneous Hacker Chatter Issues (1%)
Miscellaneous Patching Cadence Issues (1%)
None: 2 organizations (< 1%)

As one might expect from the more general discussion of score factors above, ten Application Security issues accounted for a majority (57%) of those issues having the most negative impact on the scores in our sample. Given the breadth of security risks that these ten individual issues cover, there does not seem to be any obvious recurring theme within these issues, beyond the prevalence of one issue well above all others: the use of HTTP in redirect chains.

In contrast, there seems to be much narrower focus in the less common low-scoring areas of Network Security, DNS Health, and Endpoint Security. Indeed, the use of weak SSL/TLS encryption protocols was the only Network Security issue that met our threshold of five or more findings to warrant its own entry on the list, and it was also the second-most common entry on the entire list. In an even more extreme example, the observation of outdated web browsers in use was literally the only Endpoint Security issue to make it onto the list at all, despite the markedly lower Endpoint Security scores of those organizations scoring lowest in that area. DNS Health issues had a marked focus on two specific Sender Policy Framework (SPF) issues - in this case: the non-optimal use of SPF "soft fails" that allow suspicious emails to proceed into spam folders, or into inboxes with suspicious question marks; or the absence of any SPF at all.

Breaches and Compromised Devices

One goal of these ratings is to gauge the risk of a breach at an organization. Our platform collects open-source reporting on breaches from various sources, including news reports and press statements. A review of this coverage indicated that 26 of the 500 organizations in our sample, or just over 5%, experienced a publicly disclosed breach in the past year (as of this writing).

Such reporting cannot claim to be comprehensive. It requires both the detection of the breach and its disclosure to the public, either by the victim, attackers, journalists, or security researchers. Breaches often go undetected by victims, news outlets, and researchers for extended periods of time, and there may be further delays before a detected breach becomes public (if at all).

We thus supplemented this breach coverage with select findings from the IP Reputation score factor that indicate possible malware infections or other compromises at an organization. These findings do not necessarily indicate a full-scale breach or compromise of the organization in question. Indeed, they could mean little more than precisely what they indicate: the infection or compromise of at least one machine in the past 30 days (as of this writing). They can nonetheless shed light on potential breaches that the press has not reported yet, or that victims may not have detected yet. A compromised machine could be just the tip of the iceberg, or an initial access point from which a threat group moves laterally and expands its access across the network.

This query determined that 32 unique organizations, or more than 6% of the whole sample, had evidence of at least one compromised machine on their networks in the past 30 days. Of note, these 32 organizations had a significant overlap with the subset of organizations that had publicly reported breaches in the past year. 11 organizations had both publicly reported breaches in the past year and IP Reputation findings suggesting the compromise of at least one device in the past 30 days. Merging the two lists and removing the duplicates yielded a total of 47 unique organizations - more than 9% of the total sample - that had either a publicly reported breach in the past year or IP Reputation findings consistent with a compromised device in the past 30 days.

We will further examine the statistics for this subset of 47 organizations, along with the above-mentioned bottom 10% of the sample with C or lower ratings, as special subsets.

Special Subsets

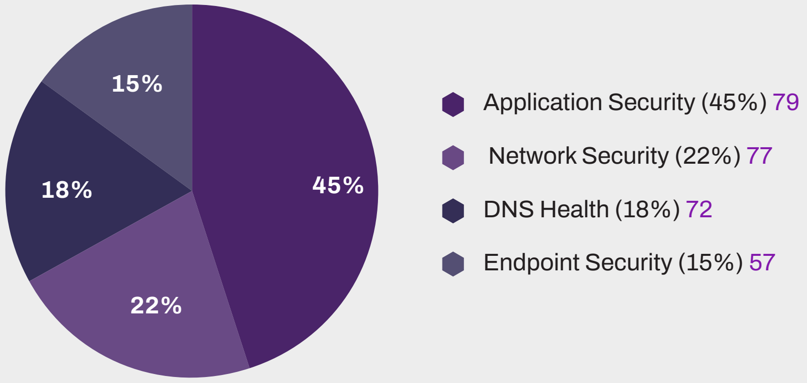
This section examines three subsets of organizations with higher risk profiles, in search of clearer insights into risk factors relevant to the whole sample. Manufacturers of medical devices and distributors of medical supplies tend to score lower than the other three sectors of this industry in our sample; it is worth asking why. The bottom 10% of the sample, with "C" or lower scores, are also at a significantly higher risk of compromise. It is worth identifying factors that increase their risk. Those organizations that have already had breaches in the past year or a compromised device in the past 30 days may also shed more light on threats to other organizations.

Devices & Supplies

Medical device manufacturers and distributors of medical supplies were the only healthcare sector with below-average ratings. An examination of the lowest-scoring security factors for the 110 organizations from that sector in our sample yielded the following distribution.

PERCENTAGES OF DEVICES & SUPPLIES ORGANIZATIONS with their Lowest Score Factor in Each Area, and Their Average Scores in Those Lowest-Scoring Areas

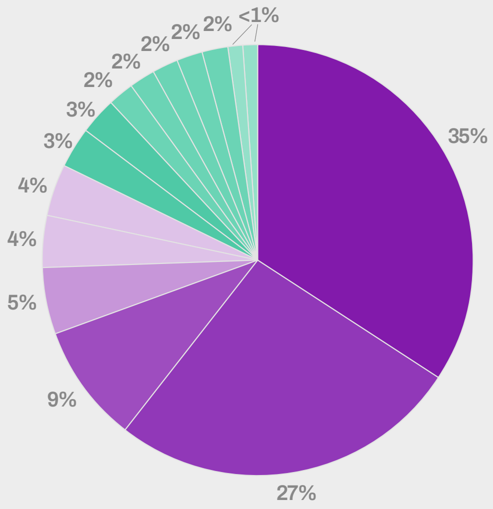
(Percentages may add up to more than 100% due to rounding error.)



The most significant difference between these figures in this Devices & Supplies sector and the whole sample is that Endpoint Security is a more frequent source of lowest-factor scores in the former, even though it is still the least common of the four main problem areas. Otherwise the distribution of lowest-scoring risk factors and their average scores are broadly consistent with those of the overall sample - including the tendency for Endpoint Security scores to be significantly lower (e.g. in the 50s) for those scoring lowest in this area.

A further review of the security issues with the most negative impact on scores provides more insight into this finding. The distribution of the top issues is similar to that of the overall sample, except that the Endpoint Security issue of outdated web browsers is slightly more common in this subset than in the overall sample. This shift partially explains why Endpoint Security is more common as a lowest-score factor in this subset. For issues with only one finding, we have consolidated them into broader categories under their respective risk factors, wherever possible.

ISSUES WITH THE MOST NEGATIVE IMPACT ON DEVICES & SUPPLIES SCORES



Redirect Chain Contains HTTP (Application Security): 35%

SSL/TLS Service Supports Weak Protocol (Network Security): 27%

Outdated Web Browser Observed (Endpoint Security): 9%

Unsafe Implementation of Subresource Integrity (Application Security): 5%

Website References Object Storage (Application Security): 4%

Website Copyright is not Current (Application Security): 4%

DNS Server Accessible (Network Security): 3%

Session Cookie Missing “Secure” Attribute (Application Security): 3%

Site Does Not Use Best Practices Against Embedding of Malicious Content (Application Security): 2%

Site Emits Visible Browser Logs (Application Security): 2%

Miscellaneous Application Security Issues: 2%

Miscellaneous DNS Health Issues: 2%

Miscellaneous Network Security Issues: 2%

High-Severity Vulnerability in Last Observation (Patching Cadence): 1%

None: 1%

(Percentages may add up to more than 100% due to rounding error.)

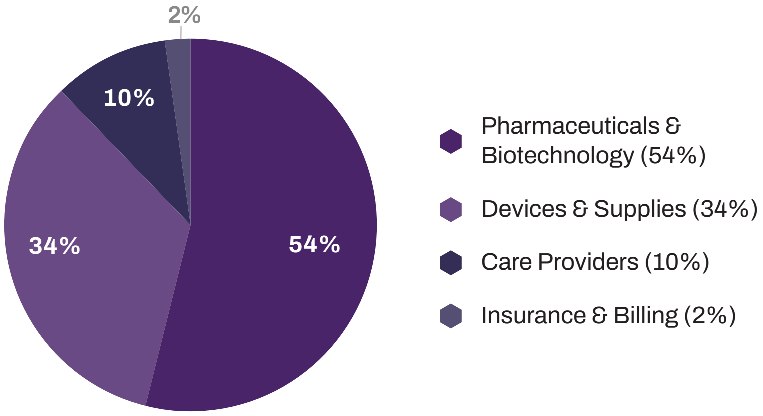
Out of the 26 organizations in the sample with publicly reported breaches in the past year, 6 of them, or 23%, involved organizations from the Devices & Supplies sector. That figure is just 1% higher than the percentage of Devices & Supplies organizations in the whole sample. In a more marked contrast, the percentage of Devices & Supplies organizations with evidence of compromised machines in the past 30 days was 12% (13 out of 110), or twice that of the overall sample. Our scoring system aims to estimate the likelihood of compromise. Organizations with lower scores, such as in the Devices & Supplies sector, are at greater risk of compromise. It thus stands to reason that they would be more likely to have evidence of compromised machines, which could be signs of a deeper problem or an initial access point enabling further compromise.

The Bottom 10%

The bottom 10% of the sample, or 50 organizations with scores in the "C" range or lower, had a mean score of 73 and a median score of 76. The lower mean score indicates that a handful of extremely low values are dragging down the average in this "left-skewed" subset.

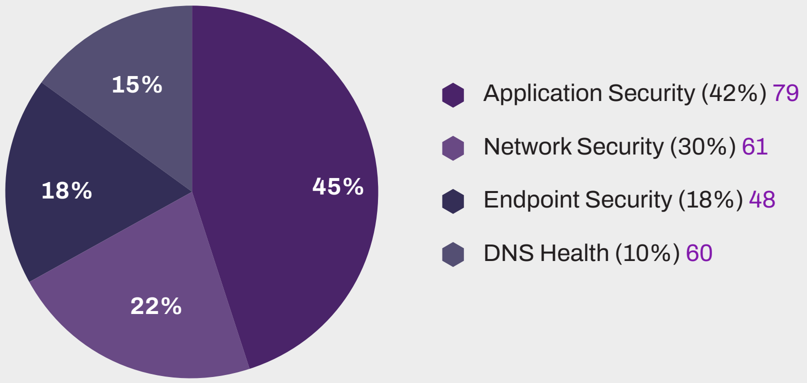
The distribution of the bottom 10% of the sample by sector indicates that organizations from the Devices & Supplies sector represent a disproportionately large share of this subset. Devices & Supplies represents 22% of the overall sample but 34% of the lowest-scoring 10% of that sample. This figure reinforces the above finding that Devices & Supplies organizations tend to score lower than their counterparts in other sectors. The Pharmaceuticals & Biotechnology sector still represents the majority of this subset, but by a smaller margin than in the overall sample.

DISTRIBUTION OF BOTTOM 10% BY SECTOR



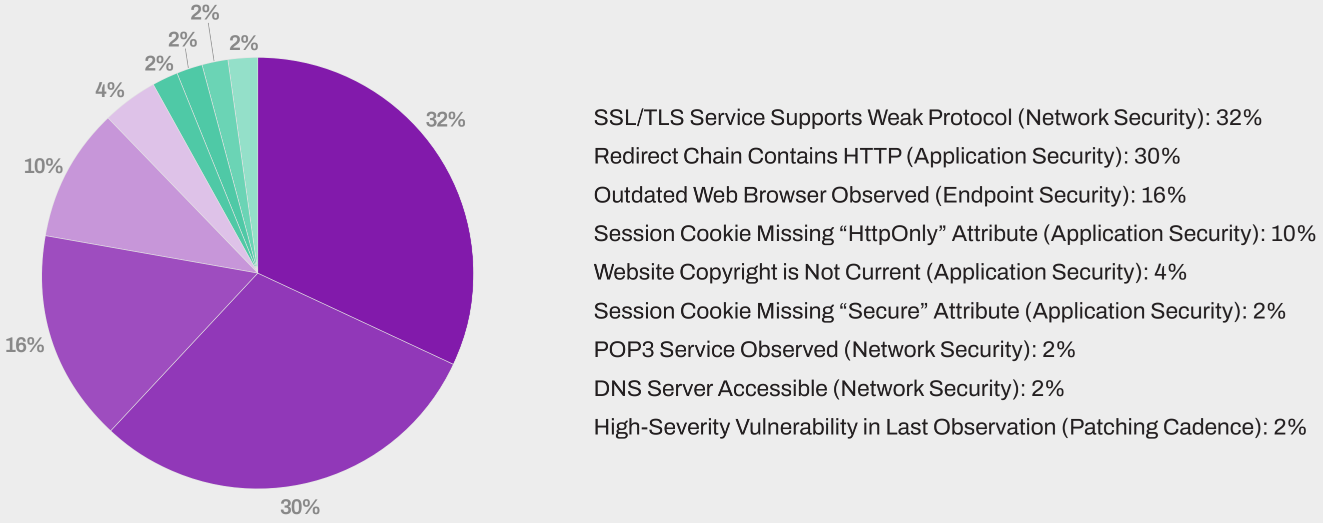
The distribution of lowest-scoring security factors among the bottom 10% differs most significantly from that of the overall sample in that Endpoint Security has moved up to become the third-most common source of lowest scores. We saw in the overall sample that Endpoint Security was less common as a lowest-scoring area, but it had a more substantially negative impact on the scores of that smaller number of organizations with their lowest scores in that factor. We also saw in the Devices & Supplies sector, where scores tend to run lower, that Endpoint Security was more common as a source of lowest scores. It is thus not surprising that Endpoint Security is more common as a lowest-scoring factor in the bottom 10% of the sample.

BOTTOM 10% OF THE SAMPLE with their Lowest Score Factor in Each Area, and their Average Scores in Those Lowest-Scoring Areas



In keeping with the above, the Endpoint Security issue of outdated web browsers was more than twice as common (percentage-wise) as the single most score-lowering issue in the bottom 10% of the sample than it was in the overall sample. Otherwise, a variety of Application Security issues remained the top concern overall, but the Network Security issue of weak SSL/TLS protocols displaced the use of HTTP in redirect chains as the single-most common worst issue.

ISSUES WITH THE MOST NEGATIVE SCORE IMPACT ON THE BOTTOM 10%



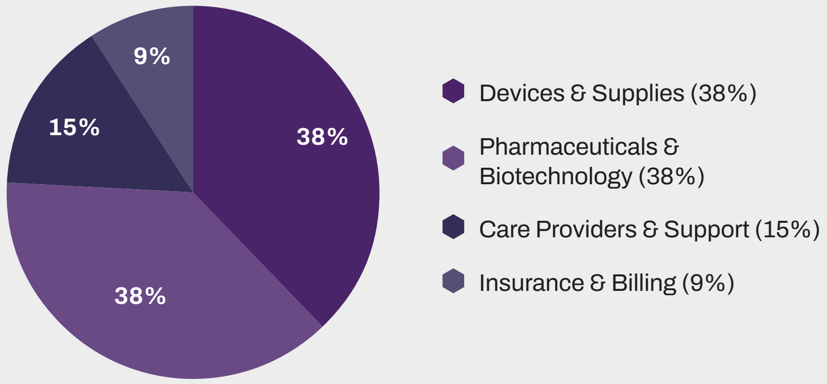
Unexpectedly, out of the 26 organizations in the sample of 500 with publicly reported breaches, only 2 of them fell into the bottom 10% of the sample subset. The rate of publicly reported breaches in this bottom 10% subset is thus slightly lower than that of the overall sample (5%). However, this bottom 10% subset also included five organizations where our platform detected evidence of a compromised device in the past 30 days. Those five organizations account for 10% of this subset, so the rate of potentially compromised devices is thus notably higher in this subset than it is for the overall sample (6%). Organizations with lower scores are at greater risk of compromise, so it makes more sense for them to have more compromised machines.

Confirmed Breaches and Potentially Compromised Devices

The distribution of publicly reported breaches and machine compromises by sector echoes and amplifies the above findings about the Devices and Supplies sector. That sector accounted for 38% of the organizations with either publicly confirmed breaches in the past year or detected machine compromises in the past 30 days. That percentage is markedly higher than the representation of Devices & Supplies in the overall sample (22%). The Pharmaceuticals & Biotechnology sector also represented 38% of this same subset, but that large percentage was much lower than that of this sector's representation in the overall sample (62%). In other words, Devices & Supplies organizations appear to be experiencing breaches and machine compromises at a disproportionately high rate, whereas their Pharmaceuticals & Biotechnology counterparts appear to be experiencing compromises at a markedly lower rate.

DISTRIBUTION OF SECTOR OF PUBLICLY REPORTED BREACHES

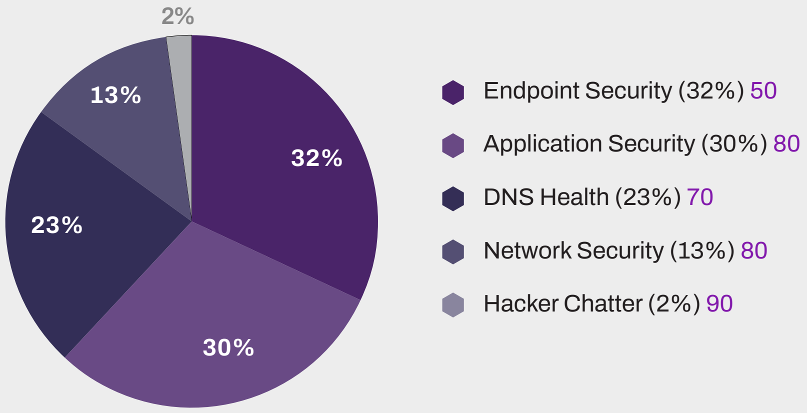
in the Past Year and Compromised Machines in the Past 30 Days



The distribution of lowest-scoring factors is also quite different in this subset. Application Security was the most common lowest-scoring factor in the overall sample and in the other subsets, but not in this subset. Indeed, this group of actually or potentially compromised organizations was the only subset where Endpoint Security was the most common lowest-scoring factor. As we saw above, Endpoint Security was less common as a lowest-scoring factor in general but a:) was more common as a lowest-scoring factor for lower-scoring subsets, like Devices & Supplies and the bottom 10%; and b) had more significantly negative score impact on that minority of organizations for which it was the lowest-scoring issue. It is thus not surprising that a subset of definitely or potentially compromised organizations would be the one and only subset in our sample in which Endpoint Security breaks through into first place.

DISTRIBUTION OF LOWEST-SCORING AREAS FOR ORGANIZATIONS WITH PUBLICLY REPORTED BREACHES

in the Past Year or Compromised Machines in the Past 30 Days, and Their Average Scores in Those Areas



Case Studies of Publicly Reported Breaches from Our Sample

Ransomware

Healthcare organizations, particularly care providers, have long been popular targets for ransomware. For example, Just Kids Dental, AKA Acadia Healthcare Company, suffered a ransomware attack in August 2023. The attackers compromised personally identifiable information (PII) for its pediatric dental patients, their parents/guardians, and current and former employees - as many as 130,000 people. The affected PII included key data points, such as dates of birth, Social Security numbers (SSNs), drivers' license numbers, and insurance policy details.

Just Kids Dental negotiated with the unnamed attackers, who agreed to delete the compromised data and refrain from selling or disclosing it. Trusting criminals to keep such promises is a risky proposition; verifying compliance is impractical, if not impossible. Identity theft, such as obtaining fraudulent lines of credit, is a primary use case for PII theft - particularly from healthcare organizations, who typically have more detailed PII on their patients than other industries have on their customers. The temptation to use PII from this breach is also higher because of its pediatric source. Children typically have no credit history, so their PII gives fraudsters a "blank slate" on which to obtain lines of credit. Children are also unlikely to check their credit reports, giving fraudsters more time to commit fraud in their names undetected.

Care providers, such as hospitals, may be the most well-known healthcare targets for ransomware operators, but they are not the only ones. Medical device manufacturer TransMedics suffered a ransomware attack in late April 2023 by the KaraKurt threat group. The attackers reportedly collected 85GB of data, including company finance and accounting records, business contracts, executive correspondence, and employee PII. The attackers threatened to release this data and specifically predicted that the company's stock price would drop accordingly.

Ransomware and other attacks on medical device manufacturers can expose patients' PII and protected health information (PHI). Manufacturers may have PHI/PII on patients who receive their devices, such as implants or prosthetics. For example, LockBit ransomware operators compromised Livanova, a manufacturer of cardiac and neuromodulation devices, in October 2023, and compromised data on as many as 180,000 U.S. patients. The patient data included: dates of birth; SSNs; insurance policy details; medical conditions and treatments; and medical device serial numbers. Livanova estimated the cost of the incident at around $2.6 million USD.

Pharmaceutical companies can also become ransomware targets. The often high value of pharmaceutical IP can leave them more vulnerable to the data disclosure extortion that has become a common feature of ransomware attacks. In March 2024, what remained of the recently disrupted LockBit ransomware group claimed to have compromised Crinetics Pharmaceuticals and demanded a $4 million USD ransom. Crinetics confirmed in media comments that there had been some degree of compromise but downplayed its extent. LockBit later claimed that Crinetics had violated its terms of negotiation by speaking with the media and accordingly rejected Crinetics' counteroffer of $1.8 USD million, as indicated in logs of chat negotiations with Crinetics that it later released. LockBit also threatened to send Crinetics' data to its competitors and to the Humane Society, which had previously reported on the company's animal testing practices. LockBit also indicated that it was willing to walk away from Crinetics' counteroffer empty-handed as a warning to future victims that it would not tolerate such alleged misconduct.

Failed ransomware negotiations can have significant negative consequences for victims, such as in two successive BlackCat ransomware attacks on medical supplier Henry Schein. The original October 2023 incident compromised the PII of approximately 29,000 employees and their dependents. Third-party breaches often expose a vendor's customers, but in this case, the breach exposed the bank account details of the companies' suppliers as well, which the attackers tried to use fraudulently. The company indicated that the downtime resulting from the incident would likely disrupt projected sales, leading the company to offer discounts to inconvenienced customers. The threat group re-encrypted this company's files in November 2023, just as the company had almost finished restoring them, due to a breakdown in ransom negotiations.

One side effect of a recently introduced SEC rule requiring companies to report breaches is that at least one ransomware group has tried to use this requirement to put more extortionate pressure on victims to pay ransoms. The BlackCat ransomware group initially tried to use this tactic against a financial services victim in November 2023 but failed because the requirement had not come into effect yet. The group tried to use this extortion tactic again in a purported December 2023 attack on Viking Therapeutics, a U.S. pharmaceutical/biotechnology company. They took the tactic a step further by reportedly coercing an employee of the company into reporting the company's alleged failure to disclose the incident to the SEC. The extortion attempt nonetheless failed again due to the group's misunderstanding as to when exactly the SEC requirement came into effect. There were no further details on the purported compromise of Viking Therapeutics.

Beyond the already extensive coverage of the Change Healthcare ransomware attack and its widespread "collateral damage" to providers unable to receive payments, there is one point that bears repeating. Trusting ransomware operators to keep their word, by decrypting files or by refraining from selling or disclosing them, is a risky proposition. Coding errors may prevent even sincere ransomware operators from restoring encrypted files. Another risk is that criminals can break their promises for any number of reasons, particularly greed, if they perceive that a victim is vulnerable to further extortion. In the case of Change Healthcare, it would appear that criminals cheating each other may have resulted in a second ransom demand after payment of the first. It would appear that the BlackCat ransomware franchise program's owners walked away with the $22 million USD payment in an apparent "exit scam," leaving their franchisees unpaid. The unpaid franchisees thus demanded another payment from the victim under a new name.

Third–Party Breaches

Many data breaches affecting healthcare organizations, as in other industries, occur via third-parties holding their data, rather than at the organizations themselves. Many breaches in healthcare organizations, as in other industries, also occur via the exploitation of vulnerabilities in third-party software, rather than any flaws in the security posture of the organization itself.

The massive May-June 2023 campaign of the criminal group C10p to exploit a vulnerability in MOVEit file transfer software (CVE-2023-34362) was one of the most extensive examples of both types of third-party breaches. Many organizations, including some in the healthcare industry, suffered breaches either directly, via their own MOVEit installations, or indirectly through a vendor using it. At least one organization in our sample - the health savings account administrator (HSA) HealthEquity - appeared in a list of victims and their data disclosures that C10p published. C10p also claimed separately to have compromised the pharmaceutical company Abbvie. The pharmaceutical company Bristol Myers Squibb disclosed that it had also suffered a MOVEit-enabled breach of employee PII, including dates of birth and SSNs.

Many different types of relationships between healthcare organizations can enable third-party breaches. For example, a July-August 2023 breach at Prospect Medical Holdings exposed PHI/PII for patients of the insurance company Humana. Prospect Medical Holdings runs a network of healthcare facilities in the Northeast and California and provides administrative services for care providers that contract with Humana. The compromised data included: dates of birth; SSNs; diagnosis and treatment details; lab results; and health insurance policy details.

Revenue cycle management (RCM), in addition to administration, is another non-clinical function that care providers often outsource to third-party vendors - creating another opportunity for third-party breaches. For example, in November 2023, it emerged that a breach at a prominent RCM outsourcing vendor compromised the PHI/PII of approximately 16,000 patients of Dignity Health's St. Rose Dominican Hospital de Lima. Compromised data points for these patients included: dates of birth; SSNs; diagnoses; and details of clinical services.

The complexity of modern healthcare, with its many highly specialized functions, often requires care providers to outsource certain clinical services as well. For example, the cancer screening service Guardant Health inadvertently exposed the PII/PHI, medical conditions, treatment details, and test results of cancer patients to threat actors, who copied it between September 2023 and February 2024. They had not been direct patients of Guardant Health per se; rather, their doctors and other care providers sent their samples to Guardant Health for cancer screening. This incident highlights a complicating factor for third-party breaches in the care providers sector: many patients have data in the possession of third-party service providers without even knowing it. For example, as in this case, many physicians and hospitals send samples from their patients to third-party laboratories for testing purposes. Many patients are unaware, or only vaguely aware, of these third-party relationships that put their data at greater risk of exposure.

Technology can help care providers and patients navigate the often complex web of third parties from which they receive various components of their care and coverage. Such platforms can also create more attack surfaces for threat actors to exploit. For example, the healthcare platform of a subsidiary of a major U.S. pharmaceutical company, with over 1 million users as of 2022, experienced a compromise of patient data via its technology vendor IBM as of August 2023. The compromised data included PHI, such as conditions, medications, and health insurance details, as well as regular PII. It was unclear how the attackers compromised IBM, but the investigation suggested that they may have exploited a vulnerability or security misconfiguration.

Recommendations

Devices & Supplies

Historically, security professionals have focused on medical devices as particularly vulnerable components of the attack surface of care providers, such as hospitals. Our findings warrant a more expansive view of cyber risks associated with the manufacturers of these devices, along with other vendors of medical equipment and supplies. As members of the only sector of the healthcare industry with noticeably lower scores in our sample, they warrant greater scrutiny from the third-party risk management (TPRM)/vendor risk management (VRM) teams of organizations in other sectors of the healthcare industry that do business with them. Such TPRM/VRM scrutiny should expand beyond the traditional focus on vulnerabilities in medical devices and the frequent difficulty of patching them to consider other risks, such as:

- the compromise of PHI/PII for the patients of care providers that receive devices from these vendors, as in the case of TransMedics;
- the exposure of billing and other financial details in transactions with these vendors;
- the potential use of any compromised infrastructure of these vendors as an attack vector against their customers; and
- medical supply chain disruptions that could result from ransomware attacks on these vendors, as in the case of Henry Schein.

Application and Endpoint Security

The number and breadth of Application Security issues that we found in our sample makes it hard to pin down more specific areas for improvement, beyond that general rubric. Nonetheless, many Application Security issues that our platform factors into its scoring come from an organization's public-facing website, so that would be a good place to start. Frequent testing, audits, and reviews can catch many problems, and our platform is also useful for self-monitoring, not just monitoring one's vendors. In contrast, the solution to the one Endpoint Security issue that stood out in our findings is quite clear: require and enforce frequent web browser updates.

Ransomware

Some of the ransomware attacks covered in this paper raise a key point: the risks of paying ransoms to ransomware operators, or of even negotiating with them. We do not recommend paying ransoms, but we also recognize that, in some situations, victims may have few or no alternatives. Organizations that are considering ransom negotiations and payments must nonetheless recognize that it is not a silver bullet; it also comes with its own risks.

Aside from purely technical errors that may prevent sincere ransomware operators from restoring encrypted files as promised, unscrupulous ransomware operators pose multiple risks for victims that pay, or are willing to negotiate, ransoms. The most obvious risk is that they simply will not keep their word. Compliance with the file decryption terms of a ransom deal is easy enough to verify, but ensuring the confidentiality of compromised files is not. They can easily sell compromised files to other criminals without the knowledge of victims who paid to maintain the confidentiality of those files, leaving them with less incentive to keep their word. More insidious is the perception of willingness to pay ransom as a sign of vulnerability or responsiveness to extortion, encouraging the same ransomware operator or another to attack the same organization again, or leading the same attacker to demand additional ransom for the same attack.

The Henry Schein and Crinetics Pharmaceuticals attacks raise another problem: simply engaging in negotiations poses risks. Ransomware operators may respond vindictively to breakdowns in negotiations, or to real or perceived violations of the terms of ongoing negotiations by victims, making a bad situation even worse. The second ransom demand for Change Healthcare raises another key point: ransomware operators cannot trust their own criminal partners, which in this case caused a breakdown on their side of the deal that left a paying victim in the lurch.

Third-Party Risk Management

TPRM and VRM is a critical function for any industry, but it is even more important in an industry with as many third-party relationships as healthcare. Simply keeping track of these numerous relationships, let alone evaluating their cyber risk implications, is part of the challenge. SecurityScorecard recently launched MAX to facilitate this task by providing TPRM/VRM as a service, in conjunction with the TPRM/VRM use of our platform and its scoring system.

Third-party risk awareness is another consideration for patients of care providers in particular. Many patients probably do not realize the degree to which their data often goes well beyond their primary care providers to other organizations, such as testing labs, diagnostic imaging services, the manufacturers of medical devices that they receive, or billing consultants. Care providers should ensure that patients understand when these third parties come into play in their care cycle.

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io