MORPHISEC
Moving Target Defense

THREAT REPORT

MORPHISEC'S 2020

CONSUMER HEALTHCARE CYBERSECURITY

THREAT INDEX

Overview

Data breaches cost healthcare providers over $4 billion in 2019 as attacks became more frequent and sophisticated. In fact, the Department of Health and Human Services investigated more than 300 cases in 2019; almost 32 million patients' records were stolen in the first half of the year alone. That was double the total records stolen in all of 2018.

Targeted ransomware is undoubtedly leading the pack of new threats facing healthcare providers. Rather than broadly deployed cyberattacks or spam, cybercriminals target healthcare organizations with the goal of exfiltrating data and then encrypting as many computers and servers as possible. This leads to data-locking ransomware serving as a second-stage attack after password-stealing malware has allowed cybercriminals to use ransomware as a second-stage attack, first deploying password-stealing malware and then encrypting machines afterward.

A look at the ransomware attacks in the healthcare industry throughout 2019 that made headlines includes:

- Talley Medical Surgical Eyecare Associates in Indiana suffered an attack in April that may have breached 106,000 patient records
- Pleasant Grove in Utah suffered an attack that compromised 320,000 patient records
- The Cancer Center of Hawaii in December faced an attack that suspended radiation treatments for patients as administrators struggled to regain network access

These new types of targeted ransomware attacks often rely on what industry analysts refer to as 'big game' ransomware. One ransomware of choice for malicious parties is BitPaymer ransomware, which first rose to prominence in 2017 when it was used to breach multiple Scottish hospitals. Morphisec has been closely monitoring the increasing use of BitPaymer ransomware over the last twelve months.

In April of 2019, Morphisec found attackers using supply chain solution providers to deliver the Bitpaymer ransomware. After first infiltrating suppliers via phishing emails, attackers looked to gain a foothold of their targeted network before stealing Active Directory credentials. Then, usually during the weekend when IT administrators were out, they deployed Bitpaymer. In September, Morphisec found that attackers were using an even more creative route to deliver Bitpaymer to enterprises via a vulnerability in the Apple Software Update utility that came packaged with iTunes for Windows.

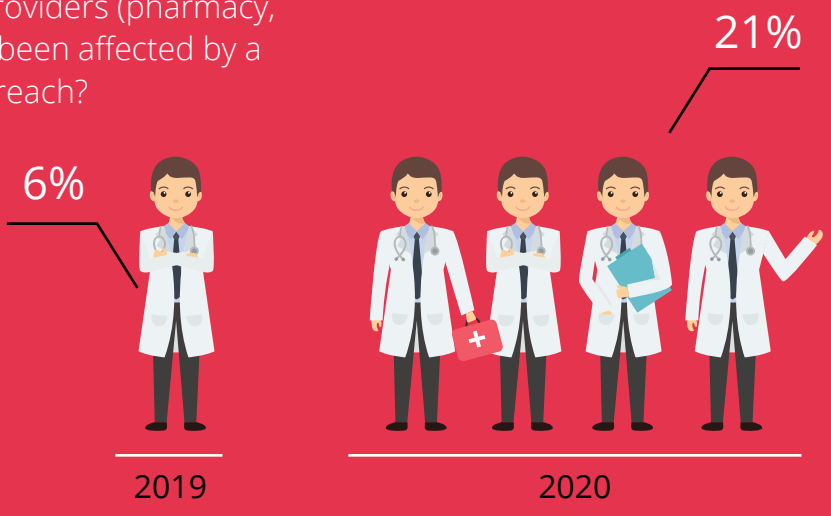
As Morphisec continues to assist healthcare providers with improving their cyber defenses and protecting patient data, Morphisec commissioned its second annual **Consumer Healthcare Cybersecurity Threat Index** to examine how the increasing amount of ransomware and other cyberattacks, and the possibility of getting their personal healthcare information compromised, is impacting the mindset of consumers. A survey was administered in February 2020 to 1,000 US consumers aged 18+ and weighted for the US population by age, region, and gender. Here's what we found:

- Consumers have started paying more attention to healthcare breaches, and more of them have seen their data stolen in a breach
- Consumers increasingly hold healthcare providers responsible for securing their personal health information

INCREASED CONSUMER AWARENESS & IMPACT

The last twelve months were marked with major healthcare cyberattacks that increasingly impacted consumers. From simply being alerted that their patient portal login information may have been compromised to having to delay actual treatment because their healthcare provider's network was down, all types of impacts were felt. It was also the year that consumers began to pay increasing attention to cyberattacks as they dominated the news cycle.

Q Has any healthcare providers (pharmacy, clinic, etc.) you utilize been affected by a cyberattack or data breach?



Morphisec's 2020 Consumer Healthcare Cybersecurity Threat Index found that the percentage of consumers who were impacted by a cyberattack against their healthcare provider more than tripled from 6 percent in February 2019 to 21 percent in February 2020. The increased frequency of ransomware attacks is only one reason for the year over year rise of consumers impacted, and it's not even the most likely one. The most likely reason for the substantial change is that the data breaches that did happen were much larger than before.

For instance, the American Medical Collection Agency (AMCA) data breach may have impacted as many as 25 million people, as it interrupted additional entities such as LabCorp, BioReference, Penobscot Community Health Center and Clinical Pathology Laboratories. This was the largest healthcare data breach in 2019, which resulted in AMCA's parent company filing for Chapter 11 bankruptcy protection in June 2019. The eight-month data breach that was discovered in March 2019 set off a cascade of events, including the loss of consumers' personal health and financial information, and the company ended up having to pay so much to account for the breach that they needed to liquidate.

This is an extreme example but is nevertheless indicative of the extreme consequences that healthcare organizations can face when they experience a data breach. The next largest loss of patient data in 2019 was insurer Dominion National, and that impacted 2.96 million patient records in a hack that lasted nine years. Both these hacks occurred in the first half of 2019, which gives 2019 the dubious distinction of being the worst year on record for patient data security.

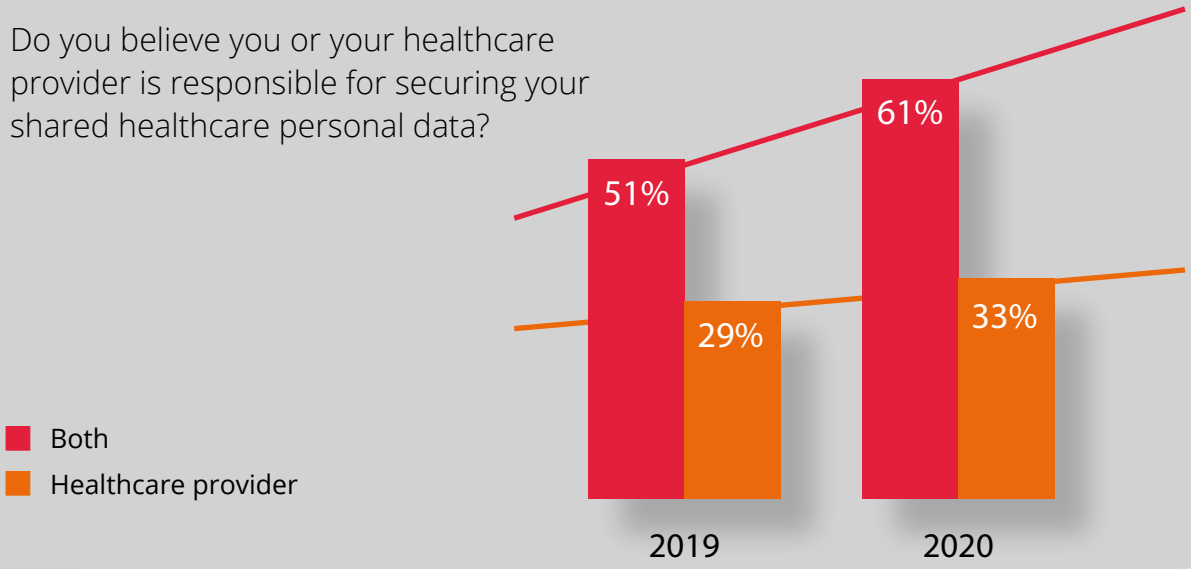
As these attacks are covered in the media, consumers are growing more aware of the threat. Nearly 80 percent of consumers indicated they were at least slightly aware of data breach and cyberattack news. Additionally, over a quarter of consumers said they were very aware of cybersecurity news, reading about it frequently.

Growing patient awareness means that healthcare organizations -- from hospitals to insurers and everyone in-between -- must pay closer attention to their data security going forward. This is especially relevant because of the continuing trend toward consolidation in the healthcare field, as larger entities make even more attractive targets to threat actors.

WHO'S RESPONSIBLE FOR PATIENT DATA?

Throughout 2019, and indeed through the first quarter of 2020, consumer perception on who is responsible for securing their healthcare has slightly shifted. While last year, 29 percent of respondents stated they believed that healthcare providers should be responsible for securing a patient's shared personal healthcare data, we saw this figure rise 33 percent this year. Perhaps those respondents are living the aftermath of their own information being implicated.

Q Do you believe you or your healthcare provider is responsible for securing your shared healthcare personal data?



But what's perhaps even more noteworthy, is the increase in consumers who say the responsibility to protect personal patient data is shared between their provider and themselves. Ten percent more people believe this to be the case this year compared to last. In fact, in 2020, more than 6-in-10 (61 percent) consumers assert dual responsibility. And with data breaches expected to continue to be a threat, a prevailing view that responsibility is shared could result in a more active dialogue between patients and healthcare organizations.

If this indicates that more patients are theoretically willing to take part of the responsibility for securing their shared personal healthcare data, we can expect to see more published tips, tricks and communication for how to ensure best practices are followed.

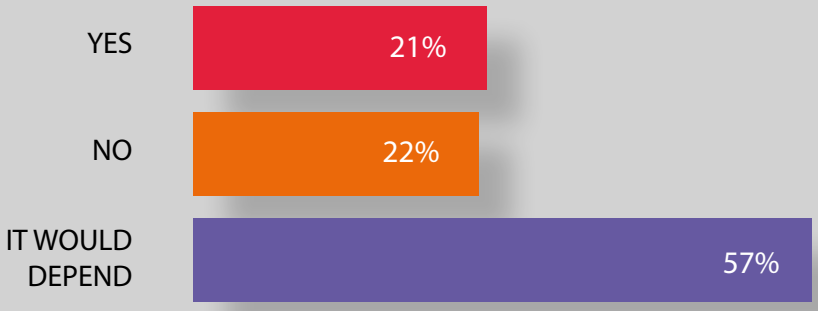
BREACHES CAN LEAD TO PATIENTS SWITCHING PROVIDERS

Choosing a healthcare provider at one time involved word of mouth, determining which doctors were in the insurance network, family ties, and which providers were local. The advent of telehealth and high deductible health plans, however, has shifted the way patients find their primary care doctors as well as their cost consciousness.

The percentage of adults aged 18 to 64 on high deductible health plans, or HDHPs, increased from 10.6 percent in 2007 to 24.5 percent in 2017, according to the CDC's National Health Interview Survey. As this percentage of consumers higher-cost plans increase, patients become more price sensitive and more aware of externalities beyond the traditional factors that govern how consumers choose their doctor.

The rise of telehealth has also driven some of the provider mobility in the marketplace, with Massachusetts General Hospital finding that 79 percent of patients said that scheduling a telemedicine follow-up visit was more convenient than arranging an in-person follow-up. Telemedicine also tends to be cheaper than in-person office visits, with net cost savings per telemedicine visit calculated to range from $19–$121 per visit, according to a study in The American Journal of Emergency Medicine.

These two factors, as well as the reliance on online reviews of providers, has resulted in consumers taking a closer look at everything about their healthcare experience. As part of that, protection or lack of protection of patient data online, can be one reason why a patient would swap providers.



Q If your healthcare provider was a victim of a cyberattack and your personal healthcare record was breached, would you consider changing your provider?

Over one-in-five respondents said they would consider changing their provider if their protected health information (PHI) was stolen in a data breach. An additional 57 percent noted that changing a provider after a cyberattack would depend on how the provider handled a breach.

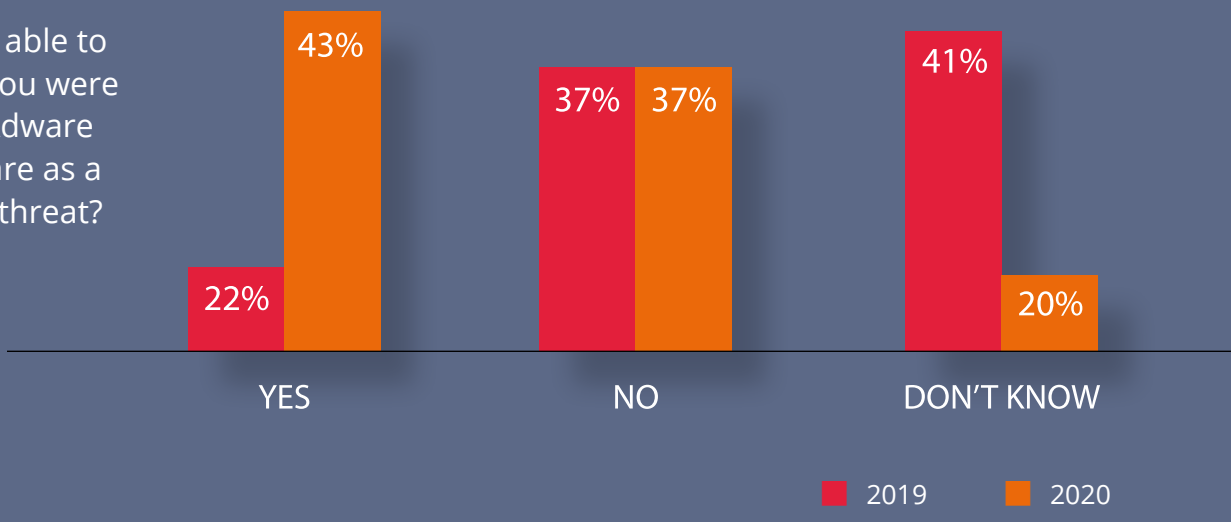
With various unavoidable factors potentially determining a patient's decision to switch clinician (accepted health insurance, geographical move, etc.), the lasting impact of defendable cyber attacks is worrisome news for healthcare providers already battling the increasingly high responsibility that's placed on their shoulders to protect valuable patient data.

RANSOMWARE OR ADWARE?

With ransomware attacks on the rise, and driving news headlines, consumers were nearly twice as likely to report they would be able to understand if they were dealing with a ransomware threat versus adware. In 2019, 22 percent of consumers said they would be able to identify ransomware versus adware, while in 2020, 43 percent said they would be able to do the same.

Meanwhile, the number of respondents who say they would not be able to determine if they were dealing with Adware versus Ransomware stayed deadlocked at 37 percent in both 2019 and 2020, leaving the percentage of people who say they "don't know" at 20 percent this year, more than a 20 percent decrease from the 41 percent that said "I don't know" last year.

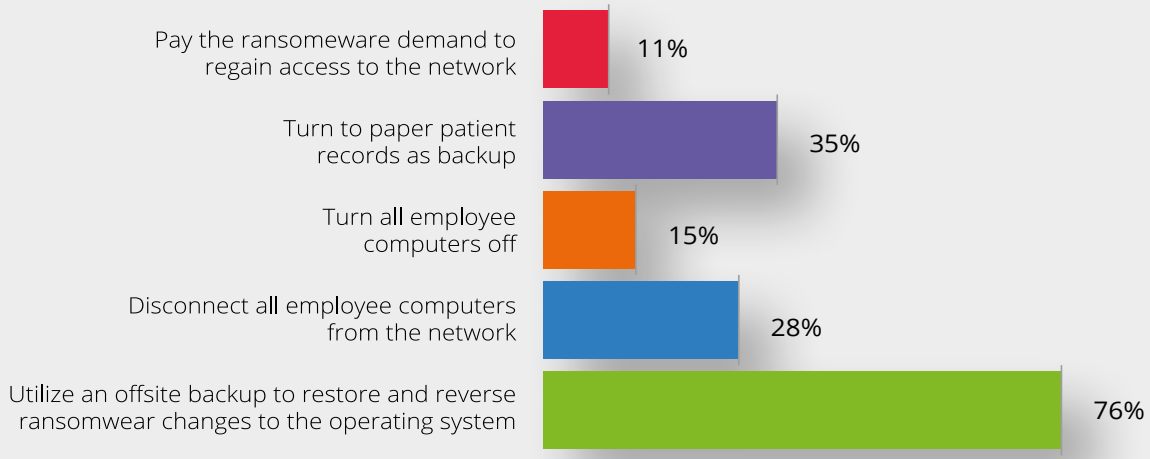
Q Would you be able to determine if you were dealing with Adware vs. Ransomware as a cybersecurity threat?



Both of these threats are common in the healthcare industry, although adware is often much more of a benign threat. However, one in four would provide the wrong Advice

ONE IN FOUR WOULD PROVIDE THE WRONG ADVICE FOR HEALTHCARE IT PROFESSIONALS DEALING WITH RANSOMWARE

Q How do you believe Healthcare IT professionals should respond to a Ransomware attack that prevents caregivers from accessing your aptient records?



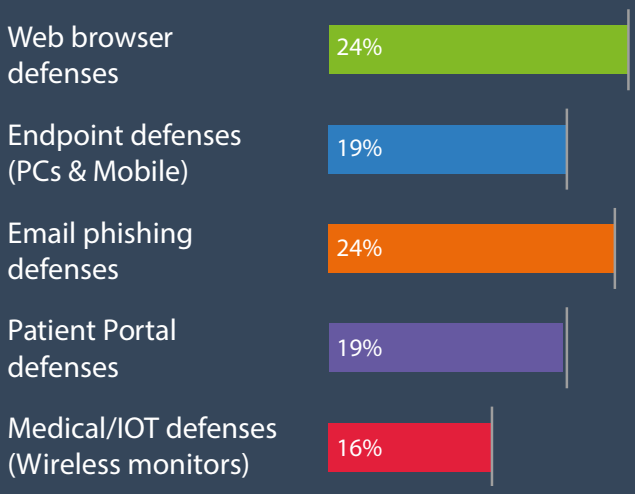
Despite a growing knowledge of the capabilities of ransomware and how it can be detected, when consumers were asked what they believe healthcare IT professionals should do to respond to a ransomware attack preventing them from accessing their patient records, many consumers illustrated they still have some to learn in dealing with ransomware.

While a large majority (76 percent) did correctly note that their providers should utilize an offsite backup to restore and reverse ransomware changinges to their operating system, 11 percent said they would have their healthcare provider pay the ransomware demand and 15 percent said their healthcare provider should turn all endpoints off.

Authorities say that you should rarely pay a ransomware demand to regain access to a network, although some experts propose that paying the ransom should be considered alongside any other business decision. While turning off or rebooting a computer would seem like a safe step, it can actually further the attack and encryption of the machine. It's better to disconnect from the network and leave the device in hibernation mode versus turning off completely.

BIGGEST WEAK SPOTS FOR HEALTHCARE PROVIDERS

It's no secret that a number of cyber vulnerabilities have emerged in the last few years as the healthcare industry adopts the use of online portals and healthcare providers adapt to new IT surroundings — driven by the migration to Windows 10, as well as, more nimble cloud workload and virtual environments.



Q What do you believe is the weakest link in your healthcare providers' cybersecurity defence?

In 2019 we found consumers thought web browsers (24 percent) and endpoint defenses (21 percent) were the weakest links in their providers' cybersecurity defenses, both coming in above patient portal defenses (20 percent) and IoT defenses (14 percent). One year later, their worries remain.

Healthcare providers' web browser defenses (24 percent) have once again come out on top in terms of what US patients believe is the weakest link in their cybersecurity defenses. And these beliefs are merited. As we noted last year, a large percentage of healthcare providers who are operating within Windows environments are still using Internet Explorer (IE) as their default browser, something even Microsoft's cybersecurity head has warned against because of its array of security issues.

And while 2020 saw a large migration to Windows 10, even these enterprises could be in danger as the Morphisec team recently discovered a new TrickBot delivery method targeting security professionals still familiarizing themselves with the new operating system.

Coming in close second for healthcare providers' weakest threat protection link, according to consumers, is email phishing defenses (23 percent). In the past year, phishing attacks have become one of the most pertinent threats to healthcare providers, as they are used to deliver all types of malware payloads.

In fact, a report released by HIMSS in the second half of 2019 found such attacks comprised almost 30 percent of all cybersecurity incidents targeting healthcare professionals. Even more worrisome, phishing attacks can also be the entry point to larger schemes that involve additional malware, ransomware and serious threats to patient data. In August 2019, a Presbyterian Healthcare phishing scam affected 183,000 patient records.

The breach potentially included social security numbers, dates of birth, and health plan information on Presbyterian Healthcare patients in New Mexico. That the scam started with a phishing email isn't unusual, and is in fact indicative of the risks that healthcare organizations face and the steps they must take to enhance security across their entire technology infrastructure.

CONCLUSION

Healthcare organizations face a fraught threat landscape as some of the richest ransomware targets. In 2019 alone, the number of ransomware attacks hospitals and other healthcare companies faced rose 60 percent year over year. This is a substantial increase in frequency, and dovetails into the rising cost of a data breach across industries -- recent Ponemon Institute research found that the cost of a successful cyberattack rose from an average of $7.1 million to $8.94 million per attack. Healthcare organizations need to understand that their risk of facing a cyberattack is higher than ever, and that the reputation risk they face is correspondingly higher too. Consumers now pay closer attention to news of data breaches and, with the alterations in fiscal responsibility, are also more cost conscious and experience minded than they have been in the past. With those two externalities to factor in, healthcare organizations need to take a hard look at their cybersecurity technology stack to ensure they are doing everything possible to protect patient data against a breach.

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology - placing defenders in a prevent-fi rst posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.