MORPHISEC
Moving Target Defense

MORPHISEC 2019 CONSUMER HEALTHCARE Cybersecurity Threat Index

Cybersecurity is one of the top ten challenges of healthcare organizations for 2019.

While the $36B shift to Electronic Health Records (EHRs), and adoption of new technologies, has improved the quality of care over the last decade, it has also made the industry vulnerable to cyberattacks.

Just last month, the team at Morphisec Labs identified an ongoing cyberattack where known hacker group FIN6 expanded beyond retail targets to attack a diagnostic image processing firm in the healthcare field.

Sophisticated cyberattackers are becoming aware of the growing number of vulnerabilities that exist within the healthcare industry as it plays catch up to the threat protection seen in other sectors. Today, healthcare organizations are attacked at more than double the average rate seen across different markets.

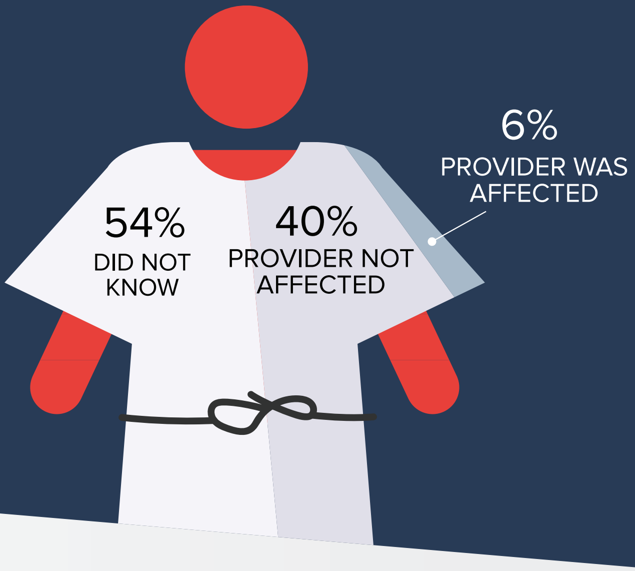
The HIPAA Final Rule on Privacy & Security that HHS brought into law in 2013 still serves as the guideline for most healthcare companies when it comes to assessing their cybersecurity defenses. Nearly 90% of health organization CISOs say they purchase cybersecurity software to meet HIPPA requirements. However, merely ensuring that cybersecurity defenses meet HIPAA requirements isn't always enough to protect healthcare organizations from advanced attacks from the likes of FIN6 and others.

Cyber defense vulnerabilities within the healthcare sector not only pose a considerable risk to healthcare organizations but most importantly the patients whose data they are responsible for securing. As Morphisec continues to assist healthcare providers with improving their cyber defenses and protecting patient data, we decided to examine how the increasing amount of healthcare cyberattacks, and the possibility of getting their personal healthcare information compromised, is impacting the mindset of consumers.

To take the pulse of consumers in the U.S., we commissioned Morphisec's 2019 U.S. Healthcare Cybersecurity Threat Index, a survey administered in February to 1,000 US consumers aged 18+ and weighted for the US population by age, region, and gender. Here's what we found:

54% of Consumers Don't Know if Their Providers Have Been Hit By a Cyberattack

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

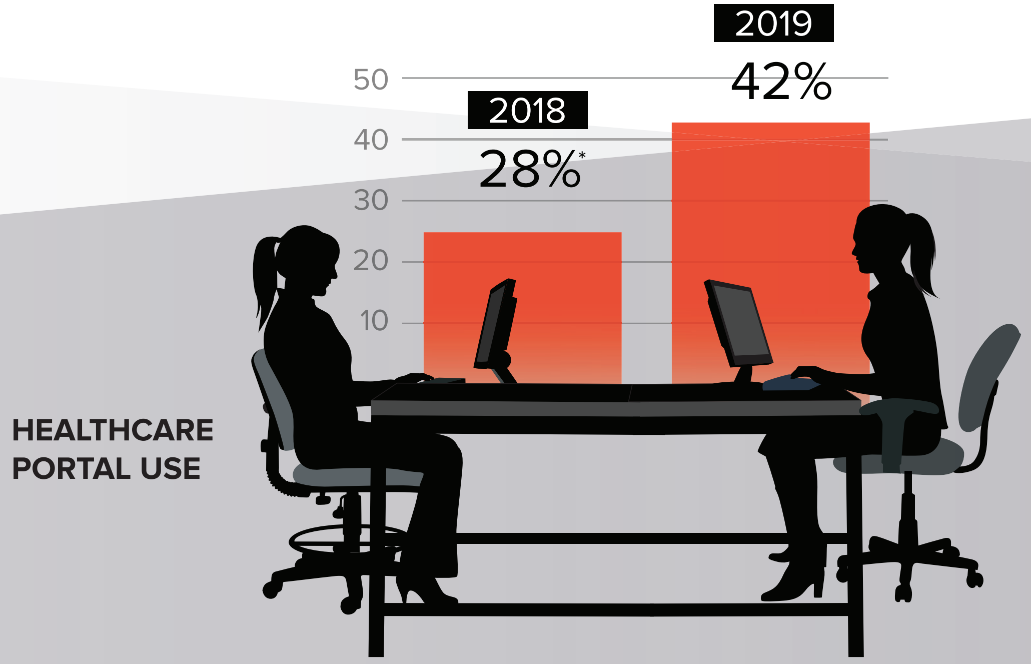


When consumers were asked if they knew whether or not their healthcare providers have been affected by data breaches or cyberattacks, more than half (54%) did not know the answer.

However, this likely isn't the result of their healthcare providers not attempting to inform them. Current HIPAA laws require healthcare providers to notify patients when their information has been compromised, and new state laws like CaCPA require print or email notifications of breaches.

With more than 2,500 healthcare data breaches since 2009, each involving more than 500 records, it's estimated that about 190 million healthcare records have been exposed over the last decade. That's equivalent to 59% of the U.S. population. So most of those who don't know if their provider has been breached may actually have had their data compromised. Despite improvements to notification requirements, and attempts by providers to contact them, consumers seem not to be fully cognizant of their providers' cyber health.

Healthcare Portal Use Growing, Increasing Consumer-facing Risk



*Source: The Office of the National Coordinator for Health Information Technology

EHR access data from 2018 indicated that 52% of consumers had access to patient portals, but only 28% actually used them. Morphisec's 2019 U.S. Healthcare Cybersecurity Threat Index reports that 42% of consumers are currently using portals to get shared data from their healthcare provider — illustrating a 14% jump over the last year.

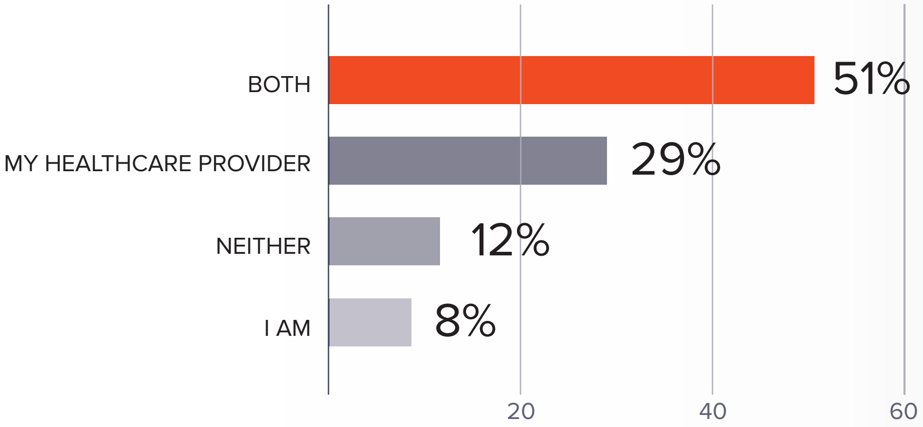
With more consumers accessing healthcare information such as lab results, imaging, visit summaries and prescriptions, healthcare organizations have a rapidly growing consumer cybersecurity channel to worry about protecting as well.

That means protecting an internet-facing website, which hackers are actively targeting. Healthcare companies need to be able to adequately protect against advanced threats, such as password stealing malware, and more basic threats, such as login information being manually obtained by someone other than the patient.

With the use of patient portals growing, organizations should readily adopt encryption techniques and two-factor authentication to gain portal access. They would also be wise to employ a security solution that can protect against advanced browser-based threats.

Majority of Consumers Believe They Play a Role in Protecting Healthcare Data

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



While only 8% of consumers think they are wholly responsible for protecting the healthcare data that is exchanged digitally between them and their providers, the majority of respondents do believe information security is a joint effort (50%).

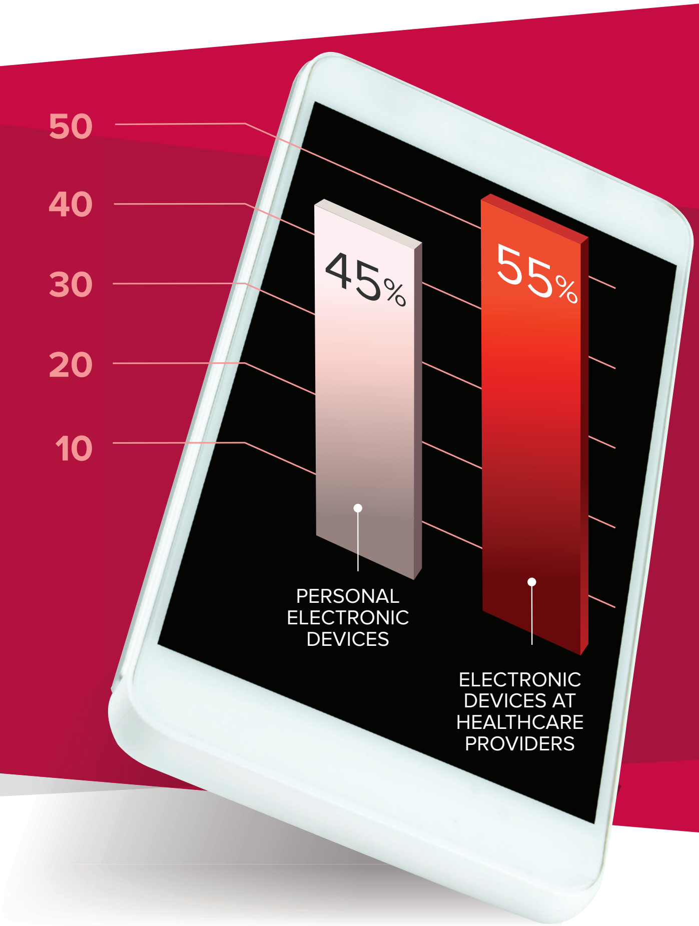
Approximately 30% believe that their healthcare provider holds sole liability for protecting their healthcare data. Given so many consumers are accessing their EHRs via portals, it's not surprising that many feel a need to play a role in protecting data they access online.

However, it should be noted that regardless of who captures a consumer's medical information, once it is shared or documented in electronic form with a provider, the provider has the property right to that data and is in charge of securing it.

As healthcare providers open up different channels for sharing data, and even encourage the sharing of patient-generated data (PGD), such as physical activity, heart rate, sleep, food, and blood glucose levels, they should be clear with consumers on who maintains ownership of that data as it is shared.

Consumers Believe Health Data on Their Own Phones is Nearly as Secure as Their Data on Devices Within Healthcare Organizations

Q: Do you believe your health information is more secure on your personal electronic device or on the electronic devices within your health-care-related providers?



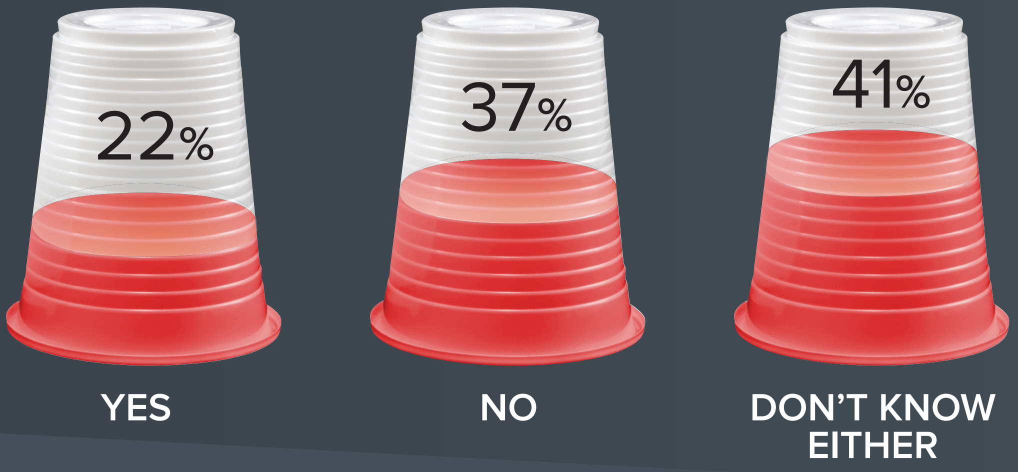
Consumer electronic devices — especially mobile phones and wearables — are increasingly the de facto real-time keeper of consumer health data. Previous studies have found that nearly one-third of Americans track their health data using these consumer electronic devices. As data tracking increases, so do fears of protecting that data. Prior market research from Parks Associates found that over 40% of consumers worry about the data security risks of their smartphones.

Given this, it was surprising to find that respondents to our survey indicated that they believe the security of their health information on their electronic devices (45%) is nearly on par with the security of their healthcare data on the electronic devices within their healthcare-related providers.

Do consumers believe that their cybersecurity defenses are nearly enterprise grade? Or do they think healthcare providers aren't doing much more than using 'over the counter' antivirus to protect their data on endpoints within an enterprise environment? Based on answers to some of the following questions, it's most likely the latter.

Nearly 80% of Consumers Aren’t Prepared to Handle the Most Active & Dangerous Threats

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



When we asked consumers if they would be able to tell the difference between dealing with an Adware or Ransomware threat to their healthcare data, nearly 80% said “no” or “I don’t know either of those.” Therefore, it seems as though the vast majority of consumers are not adequately prepared to protect their health data from cyberattacks.

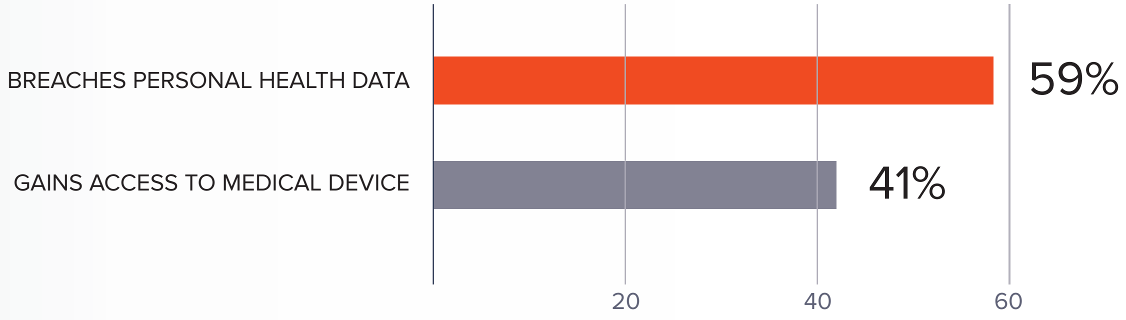
A ransomware attack is one where an attacker takes over control of your computer or device and then threatens you with demands that must be met to get access to your locked or encrypted data. Adware, on the other hand, is software that automatically displays or downloads advertising material (often unwanted) on your device.

Adware has often been thought of as a somewhat benign threat, but malware can be hidden within these unwanted popups, and its existence is widespread — representing 40% of all attacks globally.

Both of these threats are prevalent in the healthcare industry. In June of last year, the Fetal Diagnostic Institute of the Pacific was hit by a ransomware attack that impacted the digital health data of 40,800 patients. Meanwhile, the recent Capitalinstall malware campaign used adware to deliver its payload when unknowingly downloaded by healthcare employees from sites that their IT administrators assumed could be trusted.

Consumers More Fearful of Data Breach than "Murder By Medical Device"

Q: Are you more concerned with a cyberattack that breaches personal health data or one that gains access to Internet-connected medical devices (wireless monitors, etc.)?



The movie version of the worst case healthcare cyberattack is undoubtedly a 'murder by medical device.' The scenario, straight out of science fiction, is one where a wirelessly connected medical device is hacked and weaponized to attack a patient. While this scenario may seem far-fetched, the Internet of Things (IoT) has ushered into hospitals an ever-growing number of wireless medical devices, and they are hard to secure.

Unlike computers, servers and even mobile devices that have similarly designed protocols and can be secured through endpoint protection, IoT devices have an endless array of configurations making it hard to ensure they are protected. Case in point, researchers at the recent RSA security conference illustrated their ability to easily hack a wirelessly connected ultrasound. Once they had access to the IoT device, they altered medical imaging files on it and encrypted them as an example of a ransomware attack. Besides the risk to device data, medical devices also can serve as an entry point to move laterally across an IT network for attackers to collect additional sensitive data.

However, at this point, fears of hackers gaining access to medical devices is secondary (41%) to hackers breaching health data in the minds of consumers (59%). Interestingly, Gen Z respondents were the age group most concerned about cyberattacks that gain access to wireless medical devices (46%). Perhaps they better understand that the threat is a more near-time reality than science fiction.

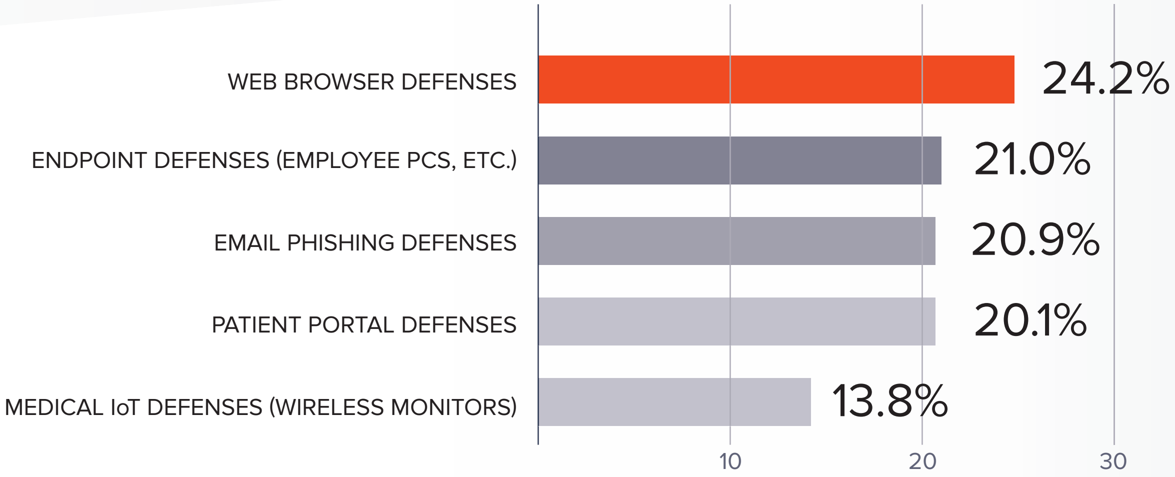
Consumers Believe Web and Endpoint Defenses are Providers' Weak Links

While new healthcare cyber vulnerabilities are emerging with patient portal and IoT use, when consumers were asked what they believe is the weakest link in their providers' cybersecurity defenses, web browsers (24%) and endpoint defenses (21%) were their top concerns. Both coming in above patient portal defenses (20%) and IoT defenses (14%).

Consumers may be right to be worried. With a large percentage of healthcare providers operating within Windows environments, their web browsing may still be done in-office on Internet Explorer (IE), which even Microsoft's cybersecurity head has stated should not be used as the default browser within enterprises because of its array of security issues. Other browsers have their own share of vulnerabilities and third-party plug-ins or extensions further broaden the attack surface. Exploit kits, built to automate scans for vulnerable browser-based applications, even made a comeback in the cyberattacker's arsenal last year, thanks to their adoption of new Flash and Acrobat zero-day vulnerabilities.

As noted earlier, consumers probably are right to question if their healthcare provider takes more stringent precautions than they do at home to protect their health data as it is accessed via laptops and other devices by healthcare employees. With BYOD policies and virtual network use increasing within the healthcare industry, and

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



employees logging into the network at different places and times to access patient data, endpoint threats are growing. With Microsoft's end of life announcement for Windows 7, this promises to get worse before it gets better. Healthcare providers that have not made the switch to Windows 10 by January 14, 2020 will no longer receive updates – unless they sign up for Microsoft's costly extended security update service.

In addition, as threats become more advanced, the traditional approach to protecting endpoints within provider organizations with antivirus is no longer working. New forms of malware and zero-day attacks are not picked up by the signature detection techniques used by antivirus.

Rounding out the top three weakest links that consumers see with their providers' threat protection was email phishing defenses. Phishing attacks have evolved to look extremely realistic, causing many people to fall into the trap. Because of this, 78% of providers experienced an email-related cyber attack in 2017. Phishing attacks can also be the entry point to larger schemes that involve additional malware, ransomware and serious threats to patient data. In February, it was announced that an employee at Memorial Hospital in Mississippi responded to a phishing email, which led to 30,000 patient records being breached.

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology - placing defenders in a prevent-first 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 wexisting cybersecurity model.

MORPHISEC
Moving Target Defense

www.morphisec.com