MORPHISEC

CONSUMER HEALTHCARE CYBERSECURITY

2021 THREAT INDEX

Table of Contents

Executive Summary

For the second straight year, more than 1-in-5 Americans had a healthcare provider impacted by a cyberattack over the last twelve months.

27% of patients state that if their healthcare provider was a victim of a cyberattack and their healthcare record was breached, they would switch providers. This number was up from the 21% of patients who said in 2020 they would consider changing their healthcare provider under these circumstances.

Email phishing defenses, you are the weakest link.

For the second year in a row, healthcare provider's email phishing defenses are consumers' biggest worry, with 26% saying that they believe this is their providers' weakest link when it comes to their cybersecurity defenses. This came in just above patient portal defenses (25%), followed by web browser defenses (20%), endpoint defenses (18%), and medical/IoT defenses (11%).

With ransomware attacks on the rise, over a quarter of consumers (26%) are most concerned about a ransomware attack shutting down their access to care. This was significantly more than those who were worried about attacks giving hackers access to internet-connected medical devices (17%).

56% of patients

have used telemedicine alternatives to in-person healthcare visits during the pandemic, increasing the attack surface for cybercriminals.

Overview

While COVID-19 impacted every industry in 2020, no sector felt the pandemic's brunt more than the healthcare industry. As frontline healthcare professionals worked around the clock to care for a never-ending wave of COVID-19 patients, healthcare executives were forced to rethink their traditional management, organizational, and operations structures seemingly overnight.

This need for new structures extended to those leading healthcare IT departments as they scrambled to support hybrid and increasingly mobile teams offering care from an array of virtual locations around the clock. The number of healthcare employees working from home increased 10-times within many hospital networks as providers evolved non-intensive care units into telemedicine practices. Meanwhile, the number of endpoint devices increased exponentially to support employees logging in on the go to access patient information.

As these dedicated IT professionals busied themselves building out technology infrastructures to save lives and support distributed care teams, cybercriminals zeroed in on a new favorite target. With healthcare providers needing to stay operational 24/7 and their attack surface increasing each day further into the pandemic, attackers found a target with numerous weak spots and a propensity to make large payouts to regain immediate access to their networks. The threat was so severe near the end of 2020 that the FBI and Department of Health and Human Services issued cybersecurity advisories to encourage hospitals, practices, and public health organizations to take precautions against attacks.

Yet, despite the warnings, healthcare organizations continued to be attacked at more than double the average rate of other industries through the remainder of 2020. Furthermore, the average cost of a breach for providers increased to $7.13 million according to IBM Security. More worrying for patients was that cyberattacks on the healthcare sector turned fatal for the first time in 2020 when a ransomware attack in Germany encrypted a hospital network and delayed treatment for a critical care patient. Although authorities later determined that the ransomware attack had no impact on the patient's eventual death, the point remains that ransomware lockdowns have a negative effect on medical care.

The gravity of the pandemic did little to dissuade cybercriminals from targeting healthcare providers with more sophisticated ransomware attacks. In fact, cyberattackers appeared to be emboldened with the opportunity to go after increasingly vulnerable and valuable healthcare organizations in their most dire moments. Attackers carried out these ransomware campaigns with targeted phishing and drive-by-download attacks designed to infiltrate employee endpoints and move laterally to exfiltrate data and then encrypt as many computers and servers as possible.

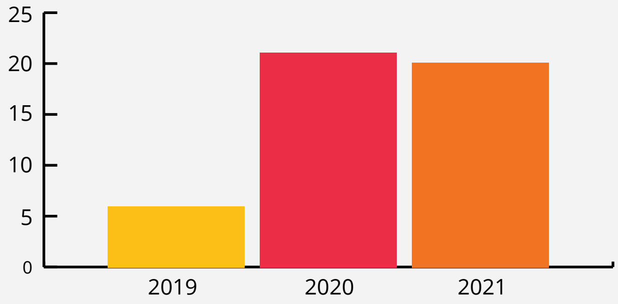
Cyberattacks similar to the Trickbot/Emotet delivered phishing campaign Morphisec researchers uncovered in September tormented healthcare organizations during the pandemic with data exfiltration before encrypting hospital networks with Ryuk ransomware. One such attack on UHS Hospitals, the $11.4 billion healthcare organization, completely disabled phone and computer access for employees across the country while delaying and severely limiting patient care.

As Morphisec continues to assist healthcare providers with improving their cyber defenses, protecting patient data, and keeping operations running with zero downtime for patients, Morphisec commissioned its third annual **Consumer Healthcare Cybersecurity Threat Index** to examine how the increasing amount of cyberattacks, and the possibility of getting their healthcare information compromised or being locked out of care by ransomware, is impacting the mindset of consumers. A survey was administered in January 2021 to over 1,000 US consumers aged 18+ and weighted for the US population by age, region, and gender. Here's what we found:

For The Second Straight Year, More than 1-in-5 Americans Had A Healthcare Provider Impacted By a Cyberattack

The healthcare industry was already reeling from several major cyberattacks that significantly impacted consumers at the start of 2020. From alerts that warned them that their patient portal login information might have been compromised to network breaches forcing them to delay treatment, patients felt the effects at many different levels. But it's fair to say that once the COVID-19 pandemic hit, the ramifications of stolen data became that much more severe, causing consumers to pay closer attention to the cyberattacks that dominated news cycles.

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



Morphisec's 2021 Consumer Healthcare Cybersecurity Threat Index found that 20% of consumers were impacted by a cyberattack or data breach on one of their healthcare providers within the past year. That number was nearly identical to the 21% of consumers that said in February 2020 a cyberattack had impacted them in the twelve months prior. That number has skyrocketed since 2019, when only 6% of consumers noted they had been affected by a healthcare data breach or cyberattack.

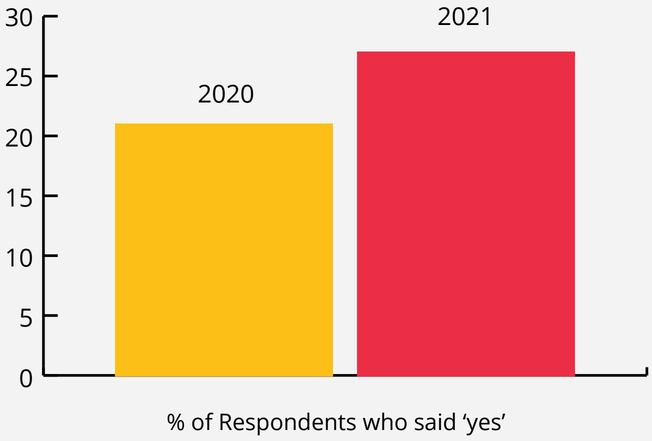
What is undoubtedly a contributor to this stark increase in consumers impacted by cyber healthcare incidents in the past few years is hackers paying closer attention to the healthcare industry. The most sophisticated cybercriminals understand that healthcare providers have a zero-tolerance policy for breaches or disruptions and need to preserve their ability to provide life-saving care 24/7. That means they are much more likely to pay ransomware demands than other sectors, and the payouts can be much larger.

When these cyber attackers go big-game hunting in the healthcare space, they increasingly turn to the Ryuk ransomware. While information hasn't yet been released on the attack that took down UHS hospitals, the average ransom payout for a Ryuk hit climbed to $1.4 million in 2020. Even before 2020, cybercriminals using Ryuk demanded an average ransomware payment of $288,000 for the release of systems, compared to the $10,000 average price demanded by criminal gangs using other types of ransomware.

Increase in Attacks Means More Consideration of Switching Providers

The impact of COVID-19 on consumer behavior has been widely reported across the board, especially when it comes to their rising expectations of companies they do business with. In a healthcare market that's already dealing with significant financial losses due to the drop in elective procedures, the threat of cyber attacks also leading patients to alternative providers is a worrying sign.

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



Morphisec found that almost 3-in-10 (27%) patients state that if their healthcare provider was a victim of a cyberattack and their healthcare record was breached, they would switch providers. This number was up from the 21% of patients who said in 2020 they would consider changing their healthcare provider if their personal healthcare information fell into malicious hackers' hands.

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

Of course, telehealth solutions' availability as an alternative to in-person visits is a contributor, too. But the truth is, with healthcare holding a more significant share of the news cycle than ever before, consumers are casting a closer eye on the patient experience in its entirety, including how safe they feel their sensitive data is with a particular clinician.

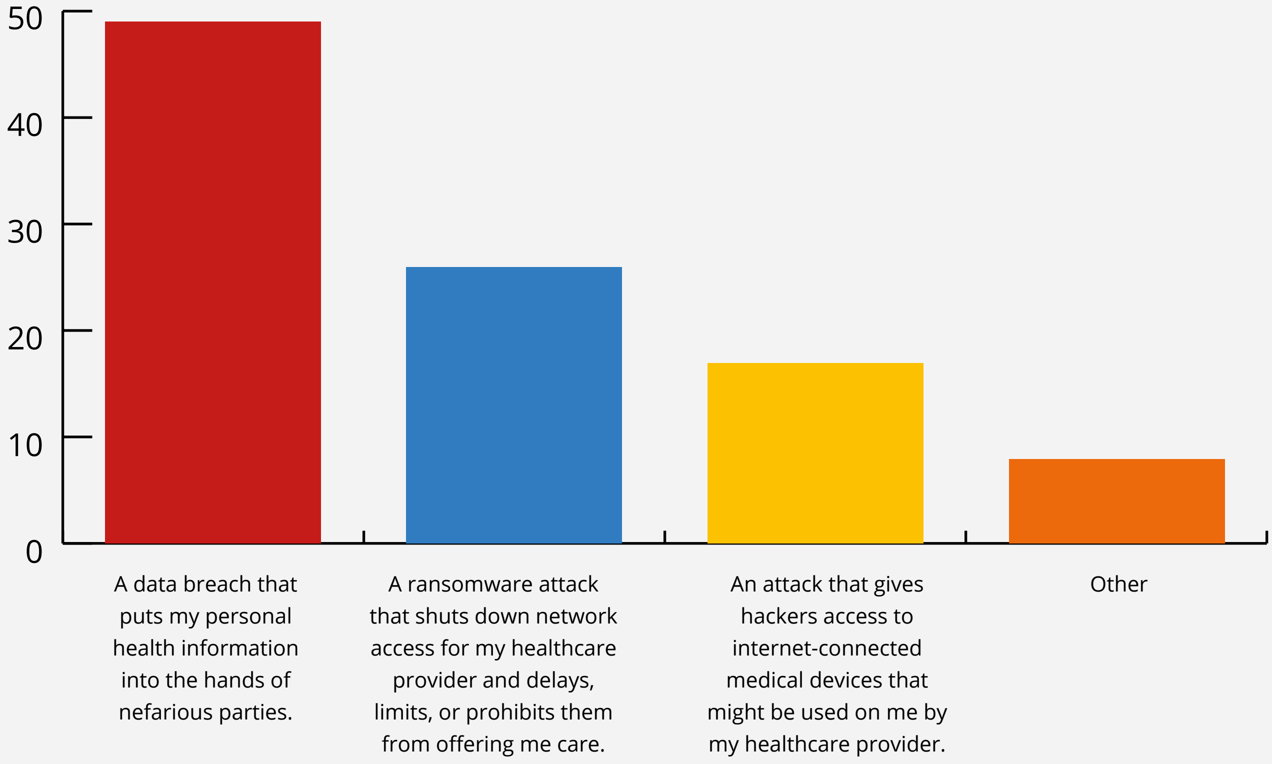
According to HIPAA Journal, more than 29 million healthcare records were breached in 2020. That number includes 642 healthcare data breaches of 500 or more medical records throughout the year — 25% more than 2019, which was also a record-breaking year. Interestingly, the largest healthcare data breach of the year was the ransomware attack on cloud service provider Blackbaud. The actual number of records exposed and obtained by the hackers has not been made public, but more than 100 of Blackbaud's healthcare clients were affected, and more than 10 million records are known to have been compromised.

The target on medical records by hackers is due to their extended shelf life and the stolen asset's appreciation over time. If a hacker breaches a financial institution and steals credit card data, consumers can quickly request a new card number and cancel the stolen one. Hospitals lack that capability because the protected health information they store cannot be changed. It follows consumers no matter where they go, which means that a hacker leveraging a ransomware attack can potentially blackmail individuals for life.

Ransomware Stopping Care Provides a New Worry

With high profile attacks on the rise, consumers' heightened anxiety is understandable. Just as patients were getting used to the idea that their personal healthcare information was a threat to be breached by hackers, 2020 brought around the realization that a cyberattack could delay, limit or prohibit their provider from offering them care in the middle of a pandemic.

What type of cyberattack on a health provider of yours are you most worried about?



With this in mind, almost half (49%) of consumers admit that they're most worried about a data breach impacting their healthcare provider this year. However, over a quarter (26%) are already most concerned with ransomware attacks shutting down their access to care. In fact, 61% of consumers told Morphisec that they're more worried today about their healthcare provider being locked out of their network by ransomware and being unable to provide them care than they were a year ago.

Both data breaches of healthcare information and ransomware attacks that shut down care were seen as more worrying than attacks that give hackers access to internet-connected medical devices that might be used on patients by their healthcare provider (17%). While these types of potential attacks have been played up as the worst-case cyberattack in scenarios straight out of science fiction, the more significant current concern among cybersecurity professionals are attacks shutting down access to various internet-connected medical services rather than nefariously altering the service they are providing.

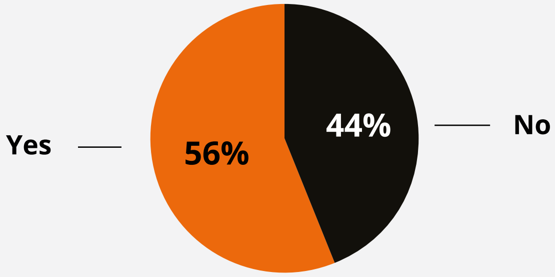
The September cyberattack on the University Hospital Dusseldorf that was initially suspected in a patient's death forced the hospital to postpone planned and outpatient treatments and route some patients to alternative medical facilities. The attackers exploited a vulnerability in the Citrix ADC that had been known since the previous January, but the hospital, unfortunately, had not yet implemented the patch.

This type of critical care interference is becoming common in ransomware attacks. Ryuk, for instance, typically affects the user interface that manages, monitors, and controls devices such as imaging equipment. This medical equipment and the computers connected to them are often ransomed in tandem, rendering them unusable and leaving healthcare staff unable to care for patients. Cyberattackers know that these organizations will pay anything to take care of their patients — especially during a pandemic. The vast increase in ransomware attacks targeting the healthcare industry during COVID-19 is anything but a coincidence.

COVID-19 Drives Interest in Telemedicine and New Cyber Safety Concerns?

While the pandemic has been a catalyst for cyberattacks, it has also directly led to more positive technological innovation within the industry — namely the offering and use of telemedicine services. The U.S. Telehealth market was valued at $9.5 billion in 2020, a tremendous growth of 80% over 2019. It's expected that 80% of consumers will still choose virtual visits post-pandemic.

As the COVID-19 pandemic has continued, have you used Telemedicine alternatives to in-person healthcare visits?



Morphisec found that 56% of patients have used telemedicine alternatives to in-person healthcare visits during the pandemic. This includes 55% of those 60-years-old and older, and 59% of women. While the increasing use of hybrid care options can be extremely beneficial for healthcare providers and patients alike, just like patient portals, telemedicine portals necessitate additional security protocols.

Patients must also learn to become comfortable within these settings with sharing their personal healthcare information. Of those that say they have used telemedicine alternatives to in-person healthcare visits during the pandemic, over half (53%) stated they are more worried about the security of their personal health information in a telemedicine setting as compared to an in-person setting.

The surge in adoption of virtual tools has certainly left more people open to attacks in these virtual settings. Prior to the pandemic, telehealth visits made up a very small fraction of medical visits. Once COVID-19 became the threat that it is today, however, and the federal government temporarily relaxed HIPAA restrictions on telehealth to meet demand, many providers began conducting visits on unsecured networks at home. Hackers have been dueling with clinicians ever since, and it has been an unfair fight.

This is because, like all WFH employees, remote physicians working around the clock to keep up with telehealth appointments are often a step behind their attackers in preventing damage. They are also reliant on collaboration apps like Zoom to communicate with patients, despite their widely reported cybersecurity vulnerabilities. This type of remote access for providers often requires setting up a Virtual Desktop Infrastructure (VDI), which results in a new virtualized endpoint to secure against attack. This increases hospitals' attack surface, which creates additional cyber risk.

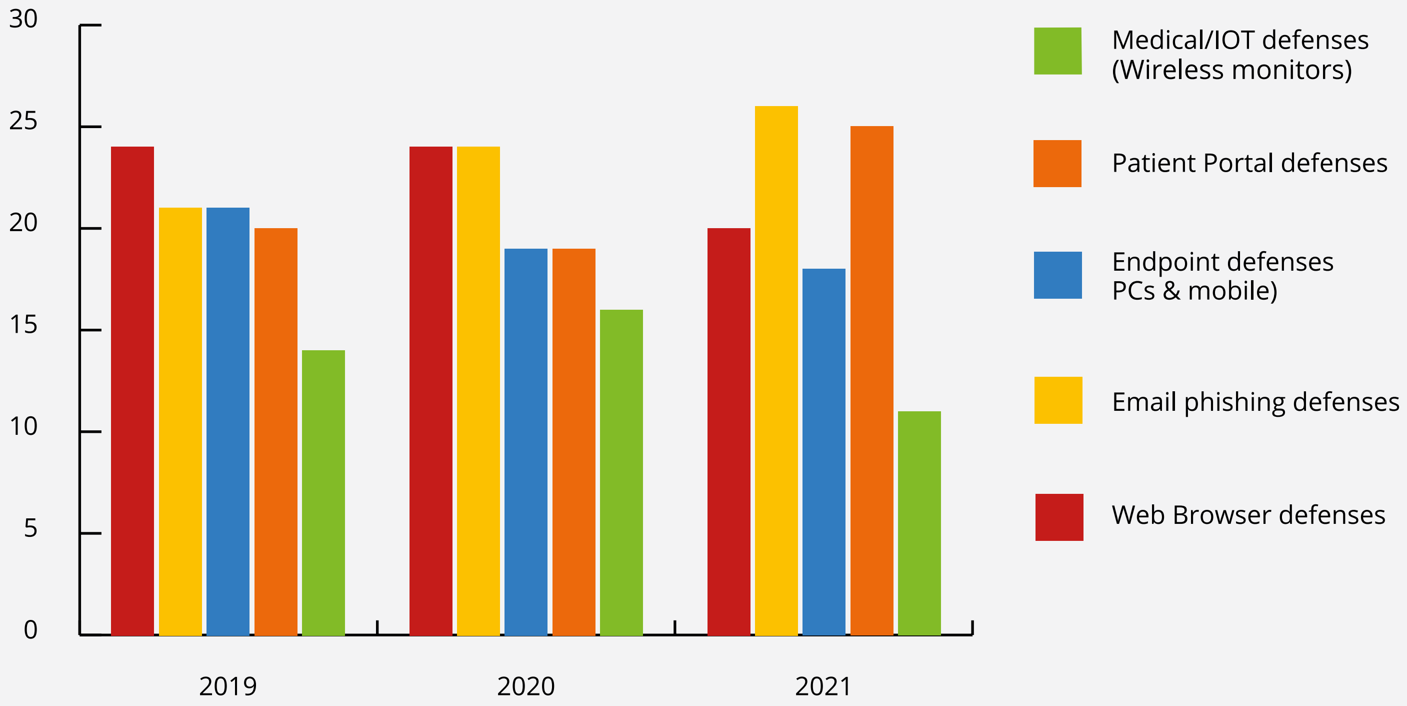
Making matters worse is that most antivirus solutions are ill-suited to VDI, as each virtual machine tends to only have the precise amount of memory needed to run critical applications. The heavyweight nature of most AV solutions often has a negative impact on VDI consolidation ratios, meaning that hospitals would be able to deploy fewer virtual instances on each host-server. Moreover, AV solutions require frequent updates to function correctly, and in non-persistent VDI environments those updates can easily overwhelm corporate networks. Overall, 57% of consumers Morphisec surveyed said that they believe healthcare providers working remotely during the pandemic and using these virtual tools have increased the risk of their personal health information being compromised.

Portal and Email Defenses are Looked at As Weakest Link in Providers' Cyber Security

Numerous cybersecurity vulnerabilities have emerged in recent years as healthcare, like almost every industry, has undergone a digital transformation. The past year in particular has been a transformative time, not just because of the rapid rise in adoption of telehealth solutions and digital care tools, but also because of the space's shift to more nimble cloud and virtual environments.

According to Gartner, worldwide spending on the public cloud rose to $257 billion in 2020, a figure that is expected to rise to over $300 billion in 2021. It's thought that the healthcare market accounted for about $28 billion of that figure last year and that it could more than double in a few year's time. But as healthcare organizations commit to these types of virtual environments, it's vital that they invest in adequate cybersecurity defenses, too. And as it turns out, consumers have their specific concerns.

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



For the second year in a row, healthcare providers' email phishing defenses are consumers' biggest worry, with 26% saying that they believe this is their provider's weakest link when it comes to their cybersecurity defenses. This came in just above patient portal defenses (25%), followed by web browser defenses (20%), endpoint defenses (18%), and medical/IoT defenses (11%).

With regards to the threat of email phishing scams, consumers' worries are most definitely merited. In November, some hospitals in Massachusetts reportedly received emails claiming to be the U.S. Department of Health and Human Services seeking information about COVID-19 statistics – raising fears about spear-phishing attempts aimed at top executives. According to a report in the Boston Business Journal, UMass Memorial Health Care CEO Dr. Eric Dickson, Holyoke Medical Center CEO Spiros Hatiras, and Signature Healthcare CEO Kim Hollon, among others, said they or staff members received such messages, triggering tighter email security protocols throughout the systems.

The suspicious emails came alongside warnings from the FBI, the HHS, and the Cybersecurity and Infrastructure Security Agency about ramped-up attacks against the U.S. healthcare sector. But more recently, government officials have published several additional warnings about the threat of phishing scams that use the promise of a COVID-19 vaccine to target consumers, too. Indeed, COVID-19 has opened up new opportunities for hackers to steal data from vulnerable healthcare organizations and patients, and email phishing scams have become the most common threat.

Coming in a close second is patient portal defenses (25%), which interestingly jumped six points YOY. Patient portals contain information that constitutes electronic protected health information (ePHI) under the HIPAA Security Rule. ePHI is defined as any protected health information (PHI) that is created, stored, transmitted, or received in any electronic format or media. Under the Security Rule, covered entities (CEs) and business associates (BAs) must develop effective administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and availability of ePHI – including patient portal ePHI. But this isn't always the case.

In September, the hacking groups behind Pysa, or Mespinoza, SunCrypt, REvil, and NetWalker ransomware variants posted data allegedly stolen from five separate healthcare entities on the dark web for sale, in an effort to force the organizations into paying their ransom demands. In the weeks prior, blogs posted "proofs" of data stolen from Assured Imaging, University Hospital New Jersey, National Western Life, The College of Nurses of Ontario, and Nonin Medical, a Minnesota-based designer and manufacturer of noninvasive pulse oximeters and regional oximeters for patient monitoring.

Finally, web browser defenses were seen as the third weakest link for healthcare providers. Browser-based attacks affect healthcare to a higher degree because the industry continues to rely on Internet Explorer as the default browser. Even Microsoft calls IE a "compatibility solution" rather than a browser, in large part because it doesn't support new web standards for things like security. By choosing to use something inadequate, healthcare organizations make strong browser security unattainable and expose themselves to attacks like drive by downloads and Adobe Flash exploits.

Conclusion

While healthcare organizations continue to navigate this unprecedented health emergency, it's clear that they're dealing with a cybersecurity one, too. Cybercriminals are now taking the targeted approaches they've used for years to go after "big name" organizations, and are turning to newer, more sophisticated methods to target even rural hospitals that are severely understaffed and unsecure. Indeed, the healthcare industry is under more pressure in 2021 to protect its critical networks 24/7, which only acts to incentivize hackers who know they have much to gain from infiltration.

Of course, what this substantial increase in frequency dovetails into is the rising cost of a data breach. Even when healthcare organizations abide by expert advice and don't pay the ransom, they must still account for the costs that arise when IT networks are shut down over long periods of time. The attack on the University of Vermont Health Network, for example, cost the health system $1.5 million per day in revenue and extra expenses, and it expects the entire incident to cost more than $63 million by the time it resolves. And now that consumers are paying closer attention to news of data breaches, they're willing to hold providers accountable if their data is affected. With all of these factors in place, healthcare organizations must take a hard look at their cybersecurity technology stack to ensure they are doing everything possible to protect patient data against a breach and mitigate any risk downtime. Because as we've seen, failure to do so will see them pay a high price in terms of both money and lives lost.

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 zero trust 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.

MORPHISEC