mimecast®

Email Security in Healthcare

Confronting Cyber Challenges in the Wake of the Pandemic

Contents

section

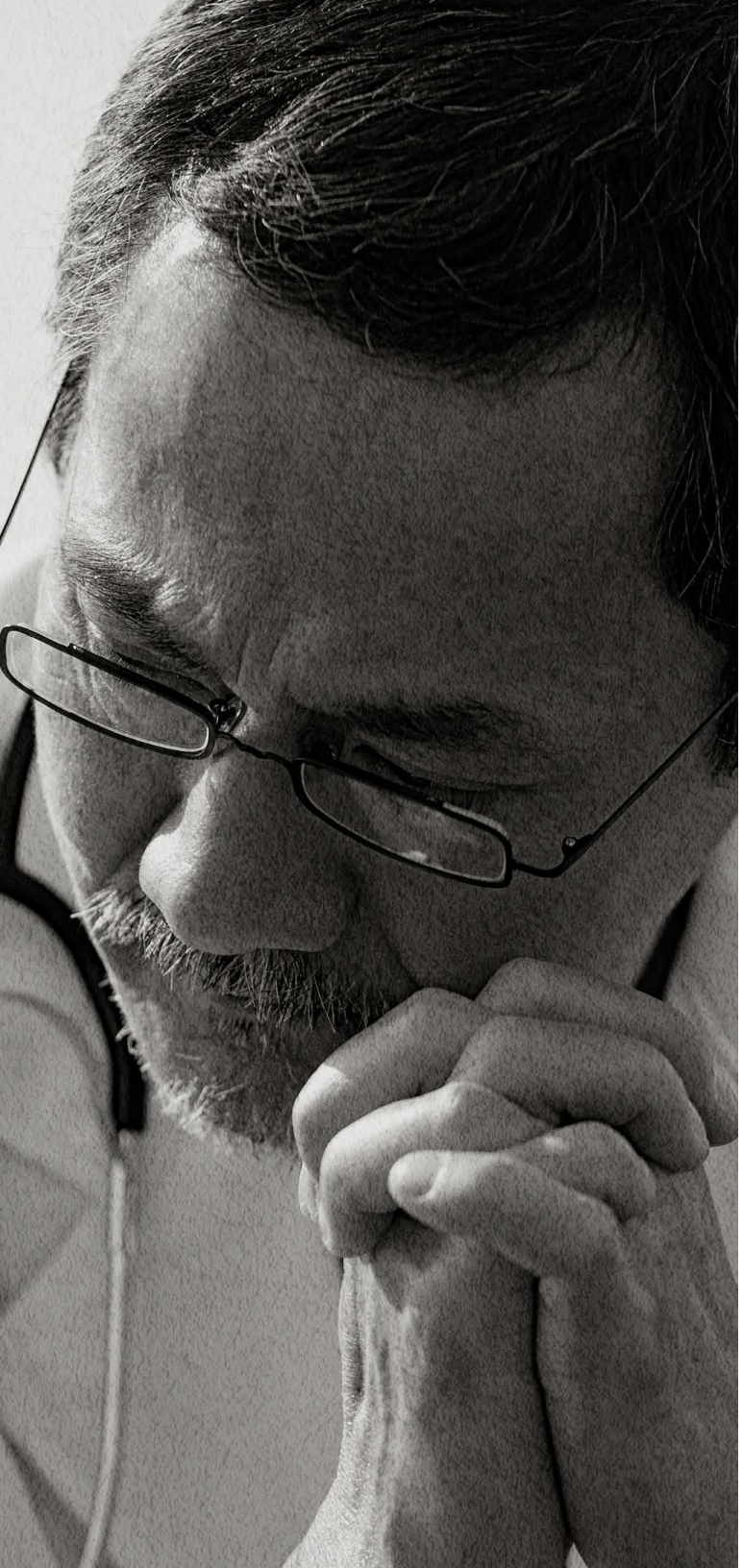
one.

For the U.S. healthcare industry, the danger posed by COVID-19 has been an unprecedented threat, but it hasn't been the only one. Healthcare also faces an unparalleled level of cyberattacks.

No Relief for an Industry in the Crosshairs

While businesses across the U.S. have faced extreme pressures since the start of the pandemic, by many measures it has been the healthcare sector that has been under the most duress. Overwhelmed by the safety precautions and urgent care requirements imposed by the health crisis, it was simultaneously confronted by an unrivaled number of malicious emails that added to the pandemic-fueled chaos.

For cybercriminals, patient records and medical data have high value, which makes healthcare providers and their affiliated businesses an attractive target. Providers also have no tolerance for system downtime that could disrupt patient care, making them especially vulnerable to ransomware. The strains and pressures of responding to the coronavirus contagion have only heightened these vulnerabilities.



Beginning in April 2020, Interpol, the UK's National Cyber Security Centre, the Canadian Centre for Cyber Security and the Cybersecurity and Infrastructure Security Agency in the U.S. all issued warnings that criminal hackers — many of whom were foreign agents — were actively targeting healthcare institutions and that much of this activity was centered in the U.S. Since then, the scope and frequency of these attacks have continued to accelerate, creating a second crisis for U.S. healthcare.

73%

of global healthcare institutions expect to be harmed this year by an email attack.

These realities are reflected in Mimecast's recent **State of Email Security 2021 (SOES) report**, a global survey of 1,225 information technology and cybersecurity professionals. When CIOs, CISOs and other IT executives from the healthcare sector were asked how likely it was that their institution would be damaged this year by an email-borne attack, 73% of them responded that it was likely, extremely likely or inevitable.

What follows is a closer look at the nature of these threats and the healthcare industry's readiness to defuse them.

section

two.

The Healthcare Industry Is Under Attack.

According to the FBI, by early April 2020 the number of cyberattacks across all industries had soared by up to 300% from just before the start of the pandemic — with the healthcare industry becoming a prime target.[1] At about the same time, the World Health Organization noted that the number of cyberattacks targeting their organization had increased fivefold.[2] Providers were overwhelmed by the COVID-19 pandemic, and bad actors seized the moment to intensify their assaults.

Replete with personal and financial information, medical records are an irresistible lure for identity thieves, and the widespread embrace of home offices and telemedicine during the pandemic presented them with many new opportunities to breach health provider systems. This led to the surge of attacks that the WHO warned against: Cyberattacks on U.S. healthcare companies rose over 55% in 2020, compromising the protected health information (PHI) of some 26 million Americans.[3]

Healthcare cybercrime is now a $13.2 billion industry, costing providers an average of $499 per record breached.[4]

In 2020, cyberattacks on healthcare companies rose over **+55%**

Phishing

For cybercriminals, email remains the most common method for carrying out their incursions. This is supported by a **joint study by Mimecast and HIMSS Media**, which found that 90% of healthcare organizations endured at least one email-borne threat in 2020.

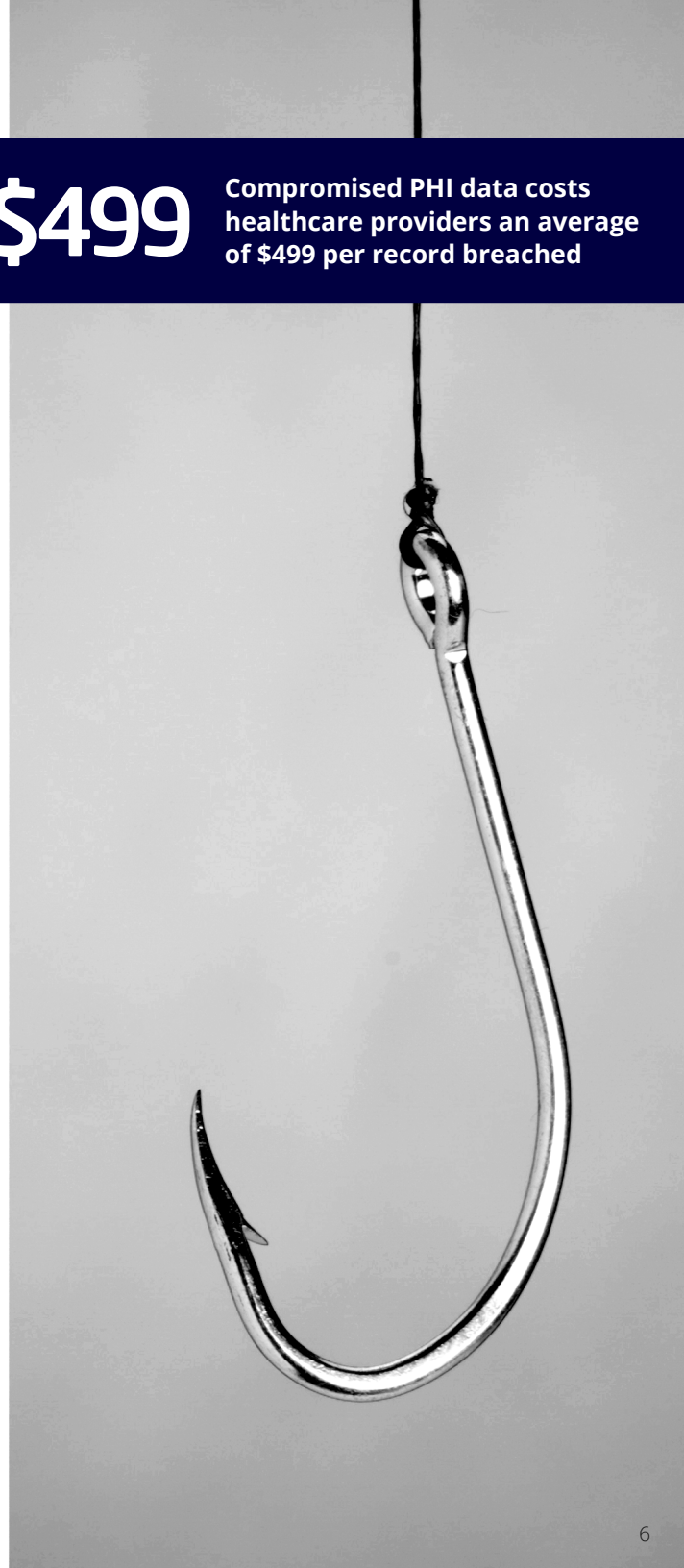
Phishing in particular is a massive threat that has become much more pernicious since the start of the pandemic.

"Phishing attempts have increased substantially, especially highly targeted and very sophisticated attacks aimed at our executives," notes Dean Lythgoe, Vice President for Infrastructure Operations and Security at CHG Healthcare, which offers temporary professional staffing services to healthcare providers throughout the U.S. and internationally.

Similar attacks have targeted hospitals in New York, Oregon and Vermont. Last fall in Massachusetts, UMass Memorial Health Care, Holyoke Medical Center and Signature Healthcare were among the hospitals whose top executives received fraudulent messages. These claimed to be requests for COVID-19 statistics from the U.S. Department of Health and Human Services.[5]

Characteristic of this latest wave of threat-laden email is the professionalism they project, making them much more difficult to detect. In CHG's case, the attackers played off of existing relationships among the members of the executive team, and between them and their clients and suppliers. The content and presentation of these missives appear to be legitimate, as do the signatures and titles of those who have purportedly sent them. As Lythgoe acknowledges, "It's become much harder to tell that it's not the real thing."

$499 **Compromised PHI data costs healthcare providers an average of $499 per record breached**



Collaboration Tools

Collaboration tools, the use of which exploded during the pandemic, have also created a new set of vulnerabilities for healthcare institutions.

With travel severely restricted and both employees and clients working from home, companies have become increasingly dependent on tools such as Slack, Microsoft Teams and Zoom.

Indeed, virtually all (98%) of the SOES 2021 respondents, across all sectors, are making use of team building and productivity software.

70%

of participants are concerned over the risks **posed by archived business conversations**

At the same time, more than two-thirds of them (70%) are concerned about safeguarding and archiving the often-privileged business conversations that take place on these platforms.

CHG is a case in point. When the pandemic hit, the healthcare staffing provider had just finished rolling out Zoom and MS Teams, and the two programs immediately became integral to the company's business continuity efforts.

As Lythgoe explains, "We do a lot of work with credentialing — making sure that a doctor has all the right documentation to work at a hospital. Now we're taking all that highly sensitive information, which wasn't all that secure in the first place, and making it more accessible by converting it to a digital format. That represents a considerable risk."

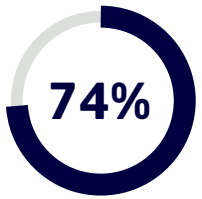
Brand Spoofing

Another front in the industry's cyber war is site spoofing and **brand impersonation**. This is a very serious risk facing many healthcare providers.

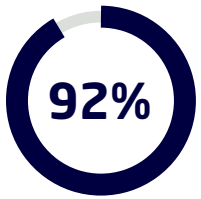
Per the SOES survey, during the past year more than two-thirds (67%) of healthcare companies experienced incidents where their brand was impersonated or misappropriated to create a counterfeit website, while more than one-in-five of these organizations (21%) were threatened in this manner on 10 or more separate occasions.

In response, more than nine out of 10 healthcare institutions (92%) are taking steps to safeguard their brands by making use of a service to detect and protect against counterfeit websites and other attempts at brand impersonation. Of these, nearly three out of four (74%) have already deployed such a service.

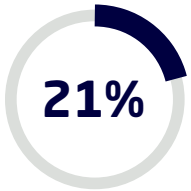
67% **of healthcare institutions have had their brands spoofed or impersonated**



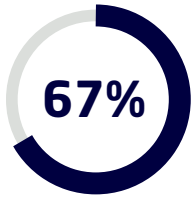
have already deployed a service



are taking steps to safeguard their brands by making use of a service to detect and protect against brand impersonation



of these organizations were threatened in this manner on 10 or more separate occasions



of healthcare companies experienced incidents where their brand was impersonated or misappropriated

Ransomware

The most pervasive threat to the sector by far is ransomware.

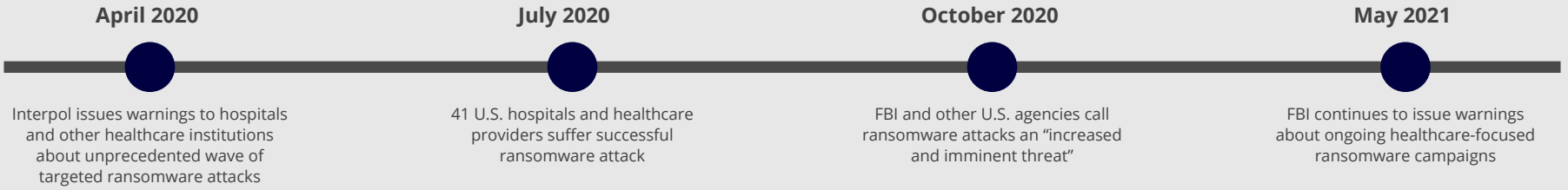
50% **of healthcare providers have been impacted by ransomware during the past 12 months**

In April 2020, Interpol issued warnings that hospitals and other healthcare institutions on the front lines of the fight against the coronavirus were the targets of an unprecedented wave of ransomware attacks. The agency also noted that these attacks were spread primarily via emails that often claimed to contain pandemic-related updates or advice from a government agency.[6]

By July of 2020, there were reports that at least 41 U.S. hospitals and healthcare providers had suffered a successful ransomware attack. Then last fall, a new wave of attacks threatened hospitals in Massachusetts, New York, Ohio and Tennessee.[7] All this was captured by the SOES 2021 report, in which fully half (50%) of the healthcare sector respondents reported that their institution had been impacted by ransomware during the past 12 months.

In October 2020, the FBI and other U.S. agencies said these incidents represented an "increased and imminent threat" against the healthcare sector, noting that they primarily involved Conti, **TrickBot ransomware** and BazariLoader malware.[8] Then in May of 2021, the FBI issued another set of warnings about an ongoing Avaddon ransomware campaign directed against healthcare agencies.[9]

"Ransomware is a terrifying threat," concedes CHG's Lythgoe. "But what's worse than a ransomware attack is the inability to recover from one." Paying heed to this, his cybersec team has devoted much of the past year to improving CHG's backup and business continuity capabilities. Their aim, he says, "is to quickly get the company back to a functional level — even if we have to give up a week or so of data."



section

three.

Are Healthcare Providers as Cyber Resilient as They Should Be?

Healthcare providers have a reputation for being laggards when it comes to defending against cyber threats. But this is not entirely true.

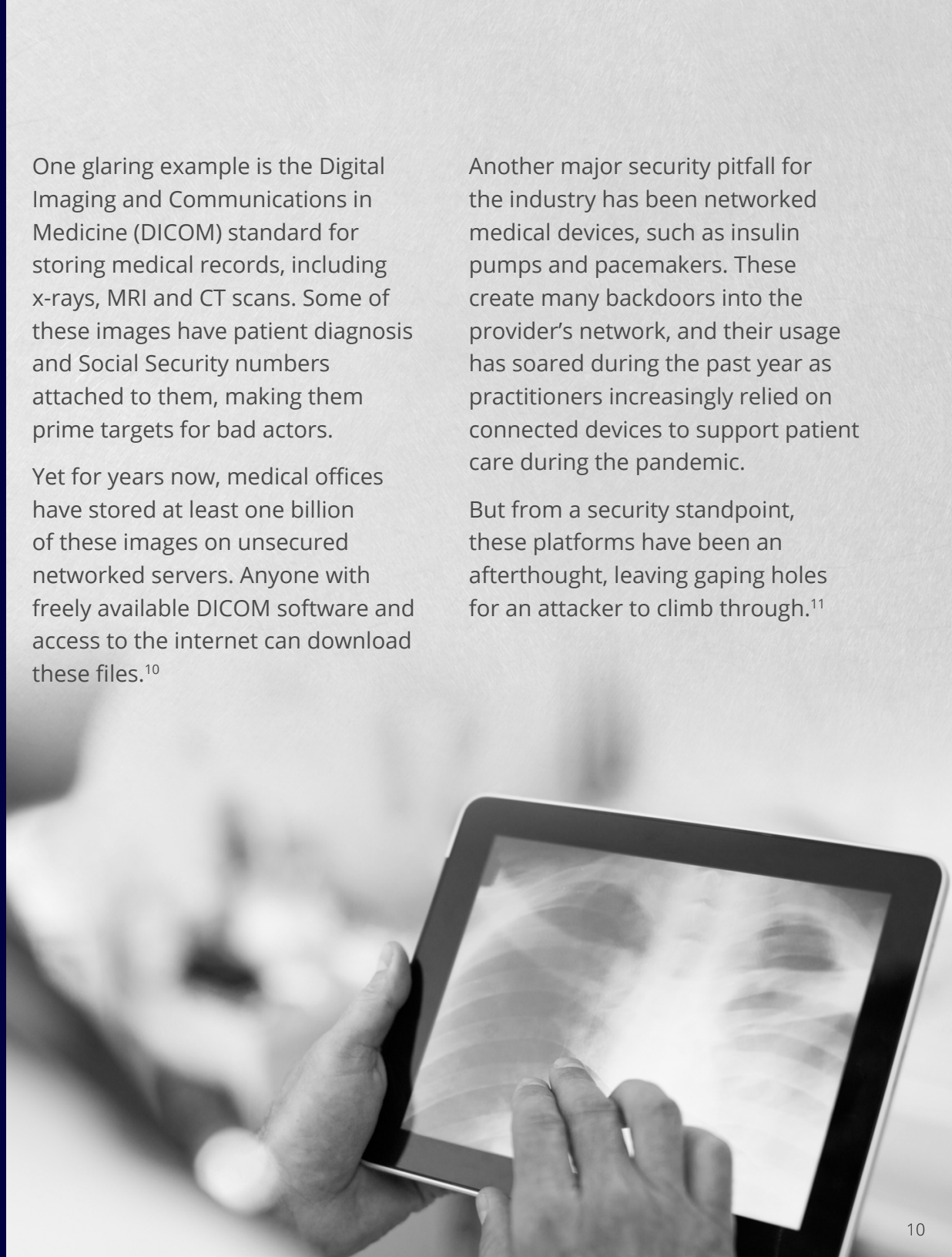
What is true is that the healthcare sector faces some unique challenges when it comes to cybersecurity, and some of these have not always been dealt with as promptly as needed.

One glaring example is the Digital Imaging and Communications in Medicine (DICOM) standard for storing medical records, including x-rays, MRI and CT scans. Some of these images have patient diagnosis and Social Security numbers attached to them, making them prime targets for bad actors.

Yet for years now, medical offices have stored at least one billion of these images on unsecured networked servers. Anyone with freely available DICOM software and access to the internet can download these files.[10]

Another major security pitfall for the industry has been networked medical devices, such as insulin pumps and pacemakers. These create many backdoors into the provider's network, and their usage has soared during the past year as practitioners increasingly relied on connected devices to support patient care during the pandemic.

But from a security standpoint, these platforms have been an afterthought, leaving gaping holes for an attacker to climb through.[11]



Layered Defenses

Yet, in the face of these and other perils, healthcare organizations are fighting back and have made significant investments in cybersecurity technologies.

Even more telling, however, is that close to all (97%) of these providers are pursuing a comprehensive cyber resilience strategy, and well over half (56%) already have one in place.

These multilayered approaches to cyber defenses are designed to help organizations adapt to new types of threats and to respond quickly to an attack.

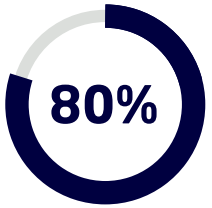
Not surprisingly, the SOES survey found that those healthcare providers with a cyber resilience strategy were far more confident in their ability to fend off and manage an assortment of threats, including ransomware and other email-borne attacks.

Conversely, close to a third or more of the providers surveyed blamed business disruptions, financial losses and other undesirable outcomes during the past year on their lack of cyber preparedness.

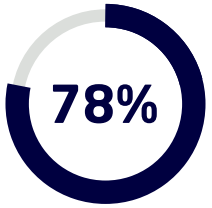
97% **of healthcare providers are pursuing a cyber resilience strategy**

56% **already have one in place**

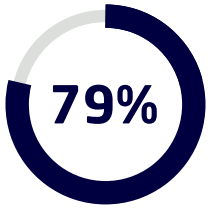
The HIMSS Media study on How U.S. Hospitals and Health Systems Approach Email Security found that:



of the 101 survey respondents have installed firewalls



Nearly 8 out of 10 (78%) have deployed email security systems



have implemented data backup and recovery solutions

section

four.

Security Awareness Training for Healthcare Workers

Healthcare providers are in the business of caring for patients, and cybersecurity is about much more than safeguarding data; it's about protecting the welfare of patients and their privacy. Any employee who deals with patient data needs to be aware of this and how securing the provider's data is imperative for patient safety.

This means that cybersecurity awareness is paramount for healthcare workers and regular, ongoing **cybersecurity awareness training** is necessary for providers to ensure that employees can recognize a phishing email and are current on the criminal set's latest tactics and ploys.

Because healthcare staffers often work at a frenetic pace and tend to be highly mobile and reactive, they are particularly susceptible to email exploits. They also have less time to spend on formal security awareness training, making it all the more important for healthcare organizations to provide training on the fly that is both highly engaging and relevant to their employees' workday realities.

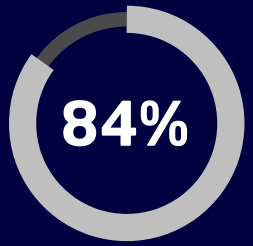
With more healthcare practitioners using their own devices for work and connecting through their own networks at home, regular cybersecurity awareness training is also needed to cope with the greater prevalence of cyber risk in the work-from-home environment. This is especially true given the ever-more-sophisticated phishing attacks targeting employees, who may also be more distracted and therefore more susceptible to misdirection when they're working from home.

Fortunately, there appears to be broad recognition of these dangers within the healthcare industry. More than eight in 10 respondents (84%) to the SOES survey indicated that employee use of personal email represents a significant risk to their organization, as do behaviors such as poor password hygiene (80%) and inadvertent data leaks (80%).

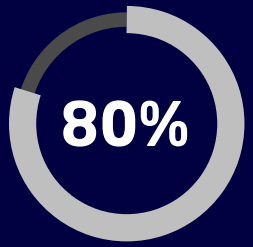
The importance of ongoing security awareness training to counter these risks is also widely recognized. More than three-fourths (77%) of the healthcare providers that participated in the HIMSS Media study agreed that employee-focused awareness training is an essential element to defending against email-borne cyberattacks.

77% **of healthcare providers view employee awareness training as an essential element of their cybersecurity preparedness**

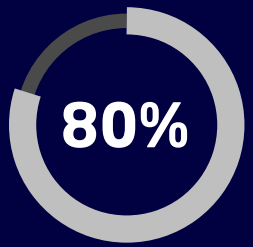
SOES survey responses on significant risks to employees' organizations



personal email usage



poor password hygiene



inadvertent data leaks

section five.

Six Key Takeaways

For the healthcare sector, the COVID-19 pandemic has thrust cybersecurity to the fore and made it a vital aspect of the industry's day-to-day operations. In this regard, here are six key lessons that providers should take to heart:

.01 Elevate cybersecurity practices.

COVID-19 has amplified and accelerated the cyber threats already confronting the industry — and spawned new ones. Given the magnitude of these risks, healthcare institutions must approach cybersecurity in the same manner as any other function that is core to their business: as a discipline that must be practiced to the highest standards in order to ensure patient well-being and optimal business outcomes.

.02 Build multilayered defenses.

For cybercriminals, email remains the most common method for carrying out their incursions, and phishing in particular has become much more pernicious since the pandemic began. To defeat the growing sophistication of these attacks, multiple technologies need to be employed. Such multilayered defenses complement and backstop one another; if a given attack sidesteps one defense, there are others in place that can neutralize the threat.

.03 Protect collaboration tools.

Such defense-in-depth must also take MS Teams, Zoom and other collaboration tools into account. Use of these tools, which has soared during the pandemic, has created new types of vulnerabilities that need to be addressed.

.04 Establish special defenses against ransomware.

Likewise, and to an even greater degree, the threat of ransomware exploded as the pandemic progressed. While the majority of these attacks are email borne and can be mitigated by layered defenses, other protections such as automated backup and secured, off-network archival systems are also required.

.05 Commit to continuous security awareness training.

Healthcare providers are in the business of caring for patients, and any employee who deals with patient data needs to view cybersecurity in this light: To protect their patients' welfare and privacy, the institution's data must be secured. But to ensure that employees understand this and can act accordingly, they must be properly and continuously trained. This is particularly the case given the extraordinary pressures healthcare workers have faced due to the pandemic, as well as the new avenues for deceiving them that have been opened to cybercriminals.

.06 Develop a cyber resilience strategy.

The key to all of this is cyber preparedness. Provider expectations of a successful email attack remain high, and many other vulnerabilities unique to the healthcare industry have only begun to be dealt with. To meet these and other challenges, the importance of a cyber resilience strategy cannot be overstated. Those providers with such a strategy in place are much more confident in their ability to withstand an attack. Going forward, institutions that employ layered defenses, while also training their employees in attack-resistant behaviors, will be in the best possible position to sidestep most attacks — and to quickly recover from those that take place.

mimecast®

Relentless protection. Resilient world.™

[1] "FBI sees spike in cyber crime reports during coronavirus pandemic," The Hill

[2] "WHO reports fivefold increase in cyber attacks, urges vigilance," World Health Organization

[3] "Healthcare Cyber Attacks Rise by 55%, Over 26 Million in the U.S. Impacted," CPO Magazine

[4] Ibid

[5] "Hospitals on high alert after phishing emails target executives," Boston Business Journal

[6] "Cybercriminals targeting critical healthcare institutions with ransomware," Interpol

[7] "Hospitals tighten email security, restrict external messages to prevent ransomware," Becker's Health IT

[8] "Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector," Cybersecurity & Infrastructure Security Agency

[9] "US and Australia warn of escalating Avaddon ransomware attacks," Bleeping Computer

[10] "One Billion Medical Records, All Containing Images, Exposed Due to Common Security Oversight," CPO Magazine

[11] "Medical Device Security, Mitigation Needs to Reduce Patient Safety Risk," Health IT Security

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.