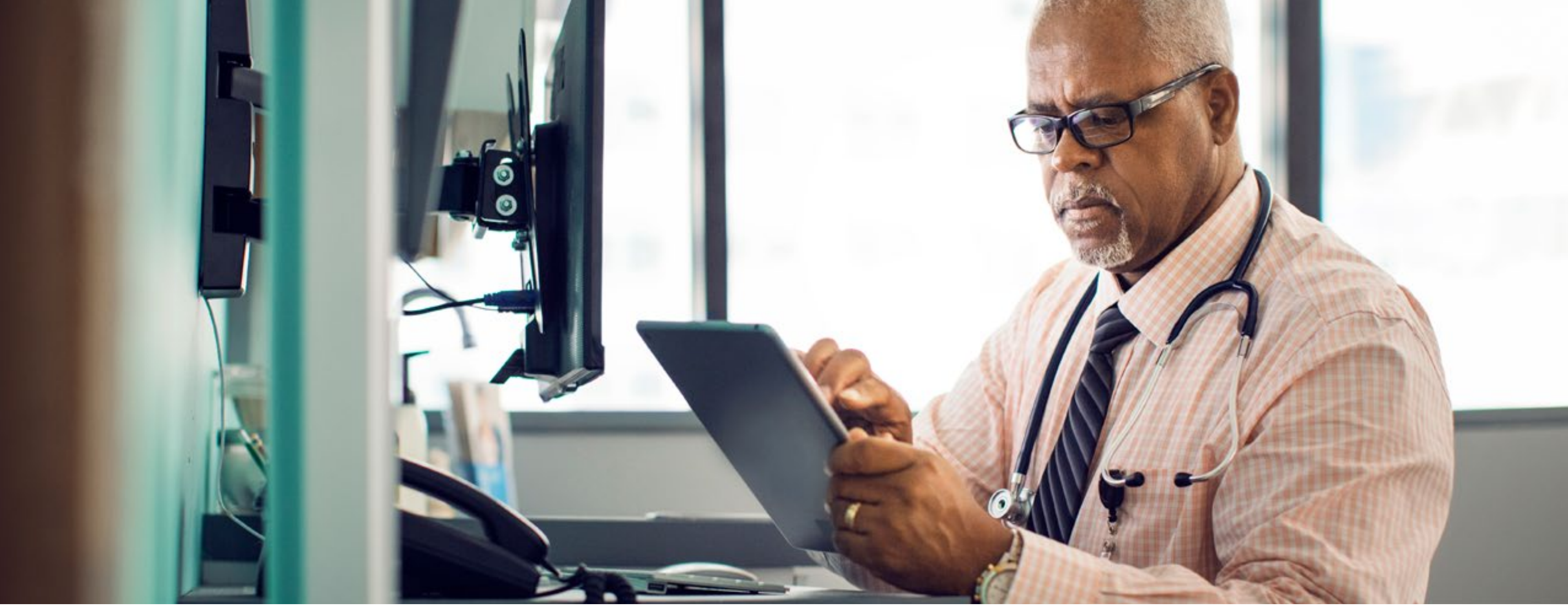
WHITE PAPER

proofpoint.

SECURING DIGITAL HEALTHCARE:

A PEOPLE-CENTERED APPROACH TO ADVANCED CYBER THREATS



INTRODUCTION

Cybersecurity in healthcare—like the healthcare industry itself—is all about people, not the doctor's office.

Patients' quest for more control and improved health outcomes is driving the industry beyond the four walls of the typical medical setting. Today's healthcare is moving towards something more expansive: an interconnected technology-powered ecosystem.

Wearable medical devices, electronic health records (EHRs), cloud-based data storage, and an avalanche of mobile health (mHealth) apps are transforming diagnosis, treatment and monitoring. Health data now flows well beyond the network perimeter.

Unfortunately, these advances have also expanded the opportunities for cyber crime, including:

- Stealing patient data
- Exploiting medical device vulnerabilities
- Siphoning off institutional data
- Holding patient records for ransom

Security is more critical than ever for healthcare organizations. At the same time, the sector has become one of the most easily targeted. Hospitals, for example, are falling victim to new kinds of cyber attacks such as ransomware and business email compromise (BEC).[1] Ransomware locks away victims' data until they pay the attacker to unlock it. BEC attacks trick victims into sending money and sensitive data by sending email requests that appear to be from an executive.

These attacks target people rather than technical vulnerabilities. [2] And for some medical facilities, they can be a matter of life and death. That's why healthcare companies must take a people-centered approach to detecting, blocking, and responding to them.

Healthcare is adapting to patients' changing needs. In the same way, healthcare-related cybersecurity also needs to evolve. Protecting patients—and their trust in you—means preventing, blocking, and resolving threats that target that data beyond your network perimeter.

[1] Kelly Sheridan (InformationWeek). "Major Cyberattacks On Healthcare Grew 63% In 2016." December 2016.
Proofpoint. "The Human Factor 2016." February 2016.

[2] Proofpoint. "The Human Factor 2016." February 2016.

THERE IS NO PERIMETER IN THE CONTINUUM OF CARE

Before the digital revolution, healthcare followed a clear path from provider to customer. Everything was contained within a static environment. Patients engaged with their primary care physicians, who then referred them on to a defined network of care providers.

Securing that environment was far more straightforward. All devices running on the network were controlled and largely located in one place or within a campus environment. Most clinicians also worked within that location. When deployed correctly, traditional perimeter-based security was a reasonable approach (albeit one that was not regularly used).

Fast forward to today's healthcare environment. Healthcare consumers are using all manner of mHealth apps, wearable medical devices, and home based medical technology. They expect this technology to improve their care experience and provide more flexibility. Accustomed to the service and convenience of Amazon, Uber, and Instacart, they want the same from their healthcare providers.

NEW DELIVERY MODELS, NEW ATTACK VECTORS

Safeguarding the network remains an important part of any hospital's security posture. But clinicians are working in new ways. As a result, they have become much more vulnerable to cyber criminals. In today's clinical workflow, care is coordinated across providers, insurers, and a multitude of devices. That means security must now extend beyond the hospital's natural borders.

With email, social media and "bring your own everything" now the norm, perimeter-based security is merely a building block. A broader security strategy must focus on people—the ways they work and the ways protected health information (PHI) it stored and sent when coordinating and delivering care.

PROTECTING DATA EVERYWHERE IT GOES

Modern care provision goes way beyond health systems' clinical staff. Patient health information now travels between a wide range of clinicians, third-party consultants, and business partners.

At the same time, advances in digital health will mean that a patient's home will increasing resemble a mini clinic. They'll use a wide variety of medical devices, all capturing, storing and transmitting patient data. And all of it needs to be secured.

Even "next-generation" network security tools weren't architected for such an environment.

THE ABCs OF MOBILE HEALTH

Meanwhile, mobile health, or mHealth, applications are heralded as the next big thing in patient engagement. Doctors and others at the frontline of healthcare delivery see countless opportunities to improve patient care through mHealth. Some have even joined the ranks of application developers and are generating their own mHealth apps. Marketplaces for mHealth apps are springing up everywhere; they're proving to be a bonanza for app providers. By 2020, the global mHealth market is expected to balloon to more than $49 billion.[3]

But all the benefits of increased patient engagement, better health monitoring, and improved outcomes are lost if you can't secure the sanctity of the doctor-patient relationship. If data is insecurely stored with third parties or sent unencrypted then patient information is exposed.

A recent study found that 86% of the 71 most popular mHealth apps were vulnerable to at least two of the top 10 risks outlined by the Open Web Application Security Project (OWASP). About 80% had poor transport layer protection. With so much at stake, security provisions should be a bigger priority.

HOW HEALTHCARE SECURITY IS LAGGING

As a whole, the healthcare industry has embraced technology. Doctors, hospitals and insurers have flung open the doors of the network to serve everyone who has a mobile phone and an online healthcare account.

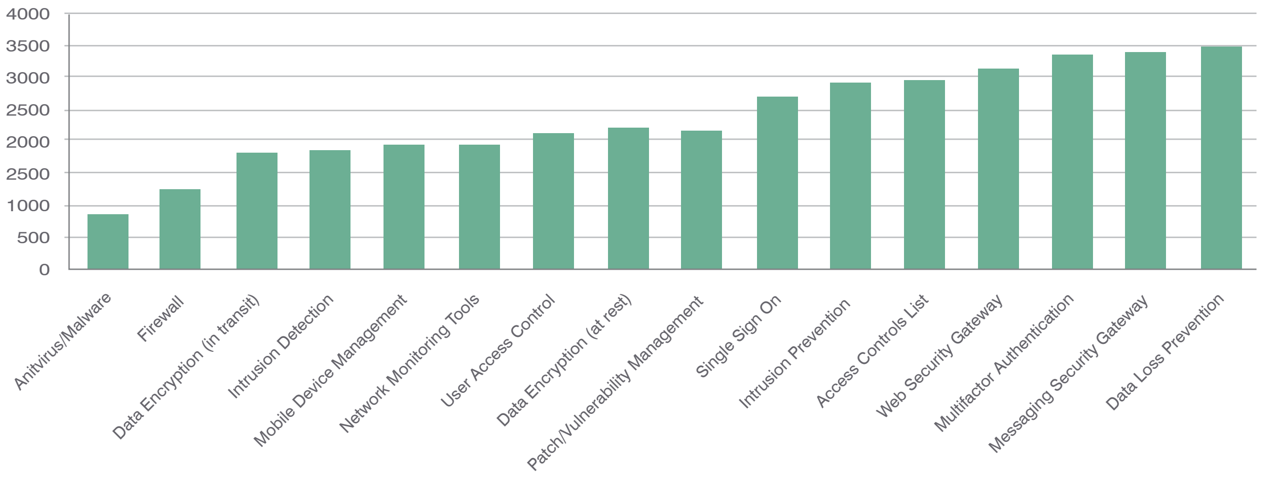
The industry hasn't been as enthusiastic about spending on cybersecurity.

According to a survey by the Healthcare Information and Management Systems Society (HIMSS), a full 15% of acute care healthcare providers have not installed basic antivirus or malware protection tools on endpoints.[4]

As ransomware and phishing attacks plague healthcare, little stands cyber attackers' way. For example, security controls in key areas, such as messaging security gateways, are deployed in less than half of the nation's hospitals.[6]

Number of US Acute Care Hospitals Without Deployed Security Technology

(2016 HIMSS Cybersecurity)



[3] Grand View Research. "mHealth Market Is Expected To Reach $49.12 Billion By 2020." August 2015.
[4] HIMSS. "2016 HIMSS Cybersecurity Survey." August 2016.
[6] Ibid.

NEW ATTACKS TARGET HEALTHCARE

Given this lack of security investment, it's no wonder that 89% of healthcare organizations suffered at least one data breach in the last two years; 45% endured five or more.[7]

Averaging almost two incidents per day, November was a high watermark for healthcare data breaches in 2016, according to the Protenus Breach Barometer. Forty-seven of these incidents accounted for 448,639 breached records in all.[8]

The largest single incident, which stemmed from a third party's insider error, involved 170,000 patient records.

PEOPLE: THE VULNERABILITY THAT CAN'T BE PATCHED

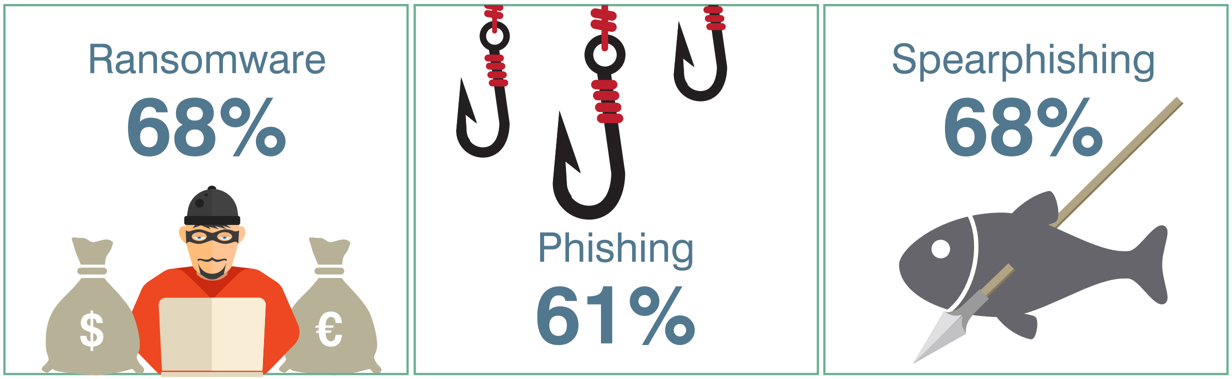
The biggest reason for these losses: employees. They caused 54% of the incidents, mostly by doing the work of attackers and clicking on a malicious email or URL and infecting themselves. 6 HIMSS recently opined that the vast majority of attacks are coming in through social engineering. In other words, people are clicking links in emails from seemingly legitimate senders or on social media sites.[9]

In May 2016, several Los Angeles County Department of Health Services employees were targeted in a phishing attack. The employees had been trained to recognize and reject phishing email. Even so, 108 of them succumbed to the attack, providing their usernames and passwords. Those compromised workers led to a breach of more 750,000 records.[10]

RANSOMWARE: HOW MUCH IS YOUR DATA WORTH?

In February 2016, the Hollywood Presbyterian Medical Center fell victim to Locky ransomware. It came through an email attachment disguised as a Microsoft Word invoice. The hospital paid a $17,000 bitcoin ransom to unlock its patient data. That's an expensive click—and just one example how ransomware is hurting healthcare providers.[11]

Most Concerning Forms of Attacks



Ponemon Study 2016

[7] Ponemon Institute. "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data." May 2016.
[8] Protenus. "Breach Barometer Report: Year in Review." January 2017.
[9] HIMSS. "HIMSS17 Cybersecurity Preview: Ransomware Reality Check." January 2017.
[10] Tony Barboza (Los Angeles Times). "L.A. County targeted in phishing cyberattack; private information of 750,000 people compromised." December 2016.
[11] Richard Winton (Los Angeles Times). "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating." February 2016.

Seventy percent of businesses hit by ransomware in 2016 paid the attacker to regain access to systems and data, according to IBM X-Force's Ransomware survey.[12] Of those attacked, 20% paid more than $40,000 to retrieve data. More than half paid more than $10,000.

And paying up is the rule, not the exception. In the survey, nearly 60% of business leaders said they would be willing to pay between $20,000 to $50,000 to regain access to vital financial records, intellectual property, business plans, or consumer data.

Ransomware made up 40% of spam emails sent in 2016.[13] That statistic underlines the point that attackers target people because it's effective.

SECURITY IS ABOUT PEOPLE, NOT THE PERIMETER

As Virgin Group founder Richard Branson famously puts it, "Success in business is all about people, people, people." [14] You can same the same about healthcare data security.

Nearly 70% of healthcare organizations fear negligent or careless employee behavior above all other security threats, according to a recent Ponemon study.[15]

Electronic health records (EHR) have greatly aided care collaboration. And that has led to better health outcomes. But it also presents huge data security issues for providers. Key issues include:

- Third-party contractors employed as clinicians increase the number and type of users with legitimate access to patient data.
- Data is accessed both on and off the network using a variety of remote or mobile devices.
- Traditional network security controls don't address many of the extended security needs of contractors and their off-campus communications.

These factors illustrate why a security strategy based on defending the hospital network no longer works. The threat vectors have changed. Attackers now target people and how they work.

WORKER TRAINING IS A BAND-AID, NOT A CURE

Many clinicians receive emails from what appear to be safe contacts, such as a work colleague, that turn out to be from an attacker posing as one. Some ask the recipient to open a malicious attachment that looks like a regular work document. These highly targeted email attacks are quickly becoming one of the most significant threats facing hospitals today – and a key reason that healthcare cyber crime cost now costs $6.2 billion per year according to Ponemon.

Unfortunately, you can't "educate away" the phishing and BEC emails from your organization. Just one well-placed click or seemingly normal wire transfer can upend months of security training and awareness efforts.

To reduce the risk of employee "clickers," companies have focused mostly on training and education. They try to teach clinical staff to recognize malicious emails and not to click on suspect URLs or attachments.

But just as hope is not a strategy, neither is telling employees "Don't click."

[12] Heather Landi (Healthcare Informatics). "Study: 70 Percent of Businesses Hit with Ransomware Paid the Ransom." December 2016.
[13] Ibid.
[14] Jack Preston (Virgin). "Richard Branson: Why business is about people, people and people." August 2014.
[15] Ponemon Institute. "Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data." May 2016.

COMPLIANCE IS NOT SECURITY

With to $34.7 billion in EHR incentives issued over the last several years,[17] 96% of healthcare institutions are now EHR certified.[18] Part of this process requires organizations to show they adhere to "meaningful use" criteria for EHR systems. They also must follow security and privacy practices mandated by the Health Insurance Portability and Accountability Act (HIPAA).

But being compliant is not the same thing as being secure. Stolen medical records are prized among cyber criminals. These records contain a wealth of information that can be used to steal an identity.

Yet U.S. hospitals remain alarmingly vulnerable to cyber security attacks. That's because their security investment have focused on keeping hospitals on the right side of HIPAA rules and "meaningful use" mandates.

Attackers, by contrast, are not concerned about compliance. They have quickly discovered that most hospitals' data defenses are easy to get around.

Hospitals are defending themselves against a new generation of targeted attacks directed at users of EHR and mHealth apps.

[17] John Lynn. "$34.7B Spent on Meaningful Use". July 2016.

[18] Office of the National Coordinator for Health Information Technology. "Adoption of Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals 2008 – 2015". May 2016.

CONCLUSION AND RECOMMENDATIONS

When it comes to securing the connected healthcare environment, prevention is better than a cure.

More than 90% of advanced attacks start with an email.[20] As the No. 1 threat vector, email is used to deliver zero-day threats, ransomware, polymorphic malware, weaponized documents, and credential phishing attacks.

By the time you detect a threat in your network or on an endpoint, it is already active in your environment—hurting your people, stealing your data, and tarnishing your brand. You need to stop these threats before employees even get the chance to click and infect themselves.

Most email gateways can filter email and keep spam out of your organization. It's good basic protection to help you manage the volume of email you receive. But it is not enough to block advanced threats, including socially engineered attacks.

Healthcare organizations need advanced protection that works in the flow of email to secure the way they deliver and coordinate care—inside and outside of their environment.

Consider solutions with the following capabilities.

CLOUD-BASED SANDBOX ANALYSIS

Look for a solution that works in the flow of email and analyzes suspicious files and URLs using static and dynamic techniques across multiple stages of an attack. It should capture advanced threats and record the patterns, behaviors, and tradecraft used in each attack. A side-by-side view of this data and the intended recipients gives security teams vital forensic insight about who is attacking and what they are after.

AUTOMATED DATA LOSS PROTECTION (DLP) AND ENCRYPTION

Securing data that leaves your environment is more important than trying to secure the myriad of devices that access it. Healthcare workers collaborate using PHI all the time. More often than not, they send it unencrypted through email.

Consider automated capabilities that can help you find data within your environment that needs to be protected. It should protect data whether it's "at rest" on your file storage or "in motion" when emailed. Automated encryption is also key to protecting any data that makes its way outside your network. It should be based on set policies rather than the individual judgement of employees.

QUARANTINES FOR ALREADY-DELIVERED EMAIL

Cleaning up malicious email is often a manual process that starts with an alert or complaint that a malicious email got through. Look for a solution that can retract malicious emails already delivered to users' inboxes.

Look for a solution that can automatically retract the original message—and any copies of the message forwarded to other users. This enables security teams to contain email threats far more quickly and reduce exposure time.

[20] Dark Reading. "91% of Phishing Attacks Start With an Email". December 2016.

EMAIL AUTHENTICATION

You can prevent every phishing attack that spoofs trusted domain names. This includes an entire class of email fraud such as BEC emails. Email authentication protects your organization from phishing attacks that piggyback domains that belong to you or trusted business partners and customers.

With visibility into who is sending email across your enterprise, you can authorize all legitimate senders and block fraudulent ones— before they reach your employees, partners, and patients.

GET STARTED TODAY

Learn more about the risks you may not be seeing. Schedule a free Proofpoint threat assessment. Our simple, non-invasive process will help you assess your security posture. You'll get a clear picture of threats and vulnerabilities in your environment.

EMAIL

Our email risk assessment shows you who is being targeted and how. We'll uncover ransomware, credential phishing, BEC, and more.

MOBILE

Our mobile defense risk assessment shows you what mobile applications your users have on their phones and what each of those apps is doing with your data.

SOCIAL

Our social risk assessment provides a snapshot of all accounts associated with your brands—corporate, unauthorized, and fraudulent.

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

proofpoint™ www.proofpoint.com