# ‘DO NO HARM’
## Through Strong Information Security

A large U.S. teaching hospital came under cyberattack in 2019 after malicious hackers used email in an attempt to steal valuable intellectual property tied to three professors’ research. Their work had been publicized on social media and in a recent news article, which made them prime targets.

That email-borne attack was caught by cybersecurity technology before it could do any damage, but it underscores the danger from more advanced threats posed by social engineering targeting healthcare workers who believe they are communicating with trusted sources. Cybercriminals no longer need to exploit vulnerabilities in software, networks, or operating systems; now, they just need to convincingly impersonate someone.

When these attacks are successful, providers, payers, and patients pay the price.

“At a high level, healthcare organizations do take security seriously, especially in light of all the attacks happening,” said Renga Srinivas, Vice President of Industry Solutions and Product Management for Proofpoint, the enterprise security company that flagged those bogus emails aimed at extracting proprietary research. “But are they doing enough? I think the answer is mixed.”

If findings from the most recent Ponemon Institute *Cost of a Data Breach Report* are any indication, healthcare still has work to do. While other annually tracked industries have improved demonstrably at warding off cyberattacks, thereby driving down the average cost of data breach recovery, healthcare has done the opposite. At last count, it cost healthcare organizations an average of $425 per stolen record, or about twice the average cost of other sectors in the report.

Produced in partnership with
HIMSS Media

*“At a high level, healthcare organizations do take security seriously, especially in light of all the attacks happening. But are they doing enough? I think the answer is mixed.”*

**Renga Srinivas** | Vice President of Industry Solutions and Product Management | Proofpoint

Part of that price hike comes from the rising value of medical records on the black market. Unlike compromised credit cards, which can be canceled and replaced, pilfered patient records contain sensitive health data that cannot. The stolen information can then be used to commit fraud and identity theft, or steal money and/or medications. Imagine the complications when fraudulently procured medications are associated with actual patients’ medical records. It could limit remedies and affect care procedures and, ultimately, patient outcomes.

“Think about healthcare’s mission and the Hippocratic oath to do no harm,” said Ryan Witt, Senior Director, Healthcare for Proofpoint, as well as a HIMSS Cybersecurity, Security & Privacy Committee member. “I’m starting to hear a philosophy that says you can’t adhere to that oath and proclaim you do no harm if you’re not safeguarding patient data the same way you safeguard patients from disease.”

Consider hospitals hit with ransomware, suddenly locked out of systems fundamental to providing critical care. News reports show the drastic measures immediately following such an attack, including patients being transferred or turned away from emergency departments — a perilous, but necessary decision to take in a place where minutes matter.

Healthcare organizations remain vulnerable to today’s advanced cyberthreats because the attack surface has grown exponentially with the adoption of cloud-based services, mobile health, telemedicine, and the internet of things. These and other emerging technologies all contribute to a decentralized, perimeterless IT infrastructure much more difficult to protect.

There’s also the nature of clinical work, which requires a focus on providing optimal patient care, often at a rapid pace, rather than deliberating the legitimacy of an email. It’s one reason healthcare practitioners remain easy targets for malicious activity.

“Even if organizations recognize security is important, they still need to look at the overall culture of the organization,” said Lucia Milică, a former chief privacy officer and HIPAA compliance officer now serving as Resident Chief Information Security Officer for Proofpoint. “Is everyone aware of what is happening in a particular organization, knowing that people are the greatest defense against cyberattacks and the greatest vulnerability?”

## The most targeted job functions

Proofpoint has done extensive research to determine the most attacked job functions within a health institution. They include, in order of popularity, the following:

**CLINICAL RESEARCH TEAMS:** These individuals and departments have a much higher propensity to receive targeted attacks, quite possibly because their names and work tend to be published and promoted in trade, news, and social media. That publicity, especially when attached to grant funding announcements, can also grab the attention of monetary-driven hackers on the hunt for new opportunities.

**IN-HOUSE PHARMACIES:** These individuals working in a pharmacy have access to materials, primarily prescription drugs, that can be quickly sold on the black market.

*“Look at security as part of a broader enterprise risk program and break it down so everyone understands how cybersecurity impacts someone’s care delivery utilization.”*

**Lucia Milică** I Resident Chief Information Security Officer I Proofpoint

**NURSES:** Because these professionals touch a medical record more frequently, and often operate at a hectic pace, they are more vulnerable to socially engineered attacks.

**SUPPLY-CHAIN VENDORS:** Outsourcers must download invoices or proposals using third-party applications that malicious actors can exploit to build campaigns.

Despite the many new technologies available, malicious hackers continue to rely on one communication channel above all others: email. Srinivas noted that Proofpoint customers, which include global Fortune 100 companies, have seen a 300% jump in imposter email attempts during the past year. An employee, contractor, or specific job function with one of the most targeted email addresses is known as a VAP, or Very Attacked Person™.

## A more people-centric approach to cybersecurity

Milică said it’s important that health systems start viewing patient safety through a different lens. Most healthcare organization leadership, from the board of directors on down, have strong medical backgrounds but not the technical expertise to understand their cyber risks. “Too often people look at it as an IT thing and a cost center,” she said. “One focus should be to truly look at security as part of a broader enterprise risk program and break it down so everyone understands how cybersecurity impacts someone’s care delivery utilization.”

As part of that wider approach, be sure the organization has nailed down cybersecurity basics: password management, patching, identity access management, asset inventories, vulnerability management, and so on. Start with a risk assessment across the environment to better understand how that exposure will affect organizational viability during a compromise. Also consider an advanced threat protection solution that analyzes and extracts threat intelligence to guard against targeted attacks using email, mobile applications and social media.

Once that’s done, organizations can build on that foundation with security awareness training, data loss prevention-tools, and encryption to better secure communications. Health systems with more mature cybersecurity programs should consider incorporating cloud access security brokers, building in automation and orchestration, and adopting threat support and social selling protection.

Proofpoint experts recommend healthcare leaders consider the following tactics to improve everyone’s cyber hygiene:

- Require a people-centric approach to security in which employees within an organization are trained to spot social engineering attacks, such as sophisticated phishing ploys. This should be conducted during onboarding and then on an ongoing basis.

- Get more advanced threat analytics beyond basic defenses. Using advanced machine learning, behavioral analyses, and so on, will better protect against advanced and emerging threats.

- Consider using DMARC (domain-based message authentication, reporting, and conformance) to vet vendors that could unwittingly be used in an attack.

- Devote adequate resources to protecting email accounts from being compromised and then used to infiltrate an organization.

*“If you know which functions are most likely vulnerable, you can put specific controls on those job functions. That way you get better mileage out of your security budget.”*

**Ryan Witt** | Senior Director, Healthcare | Proofpoint

## Knowing where to start

“If you’re going to build a security architecture to protect patient data, one of your starting points should be considering who is being attacked in your entity,” Witt said. “Then ask: If you had that knowledge, what would you do differently? How would you change your approach if you knew who is actually being attacked?”

A critical investment, according to Milică, must be made in staff, clinicians, physicians, and executives involved in patient care. “Knowing that people are the best defense against some of these threats, and having a proactive approach to protecting them, will empower everyone to make a difference. The key is to change the mentality and view to where security is part of everyone’s job. It’s not just someone else’s problem; it’s all of our problem.”

To those with serious budget constraints, Witt suggests conducting an internal investigation with a trusted partner to determine the most attacked people or job functions within an entity. Next, determine what controls should be established to help those people, such as better security awareness and training, multifactor authentication, or encryption.

“It’s not necessarily a one-size-fits-all, but if you know which functions are most likely vulnerable, you can put specific controls on those job functions. That way you get better mileage out of your security budget,” he said.

The key, Witt added, is to see security differently.

“More progressive organizations are linking cybersecurity to protecting patient data. We talk about not doing certain things because you don’t want to harm your patients. Well, if you aren’t doing certain things to protect their data, you are harming those patients, maybe not in a traditional way, maybe not in a way you’ve been trained, but you are still harming them in a demonstrable way,” he explained.

“So, you — the doctor, nurse, or clinician — have to think long and hard about the importance of that data and that patient holistically,” Witt said. “Sure, we need to be focused on wellness, but wellness today should encompass the full spectrum of a patient — and that includes good data hygiene.”

Protect your clinicians, safeguard patient data, and secure your communications. Begin at **Proofpoint**.

proofpoint.

**About Proofpoint:**

Proofpoint gives you protection and visibility for your greatest security risk—your people. We provide the most effective security and compliance solutions to protect people on every channel including email, the web, the cloud, and social media.

Produced by HIMSS Media | www.himssmedia.com | © 2019