# A Weak Link for Healthcare Security

## Addressing supply chain cyber risk and patient safety

Securing health institutions is challenging because the universe of potential threats is vast and ever-expanding. After all, healthcare data is considered the most valuable commodity sold on the information black market, making it a prime target for threat actors. Ransomware is a significant threat because if an exploit is successful, patient safety is immediately compromised until the ransom is paid. Even the simple failure to secure patient privacy can result in significant fines, a tarnished reputation but, more importantly, can ultimately harm patients in ways that can haunt a healthcare organization for years.

Although these may be the concerns that keep healthcare CIOs and CISOs awake at night, the attacks that cost the most money are business email compromise and invoice fraud. According to data from the Federal Bureau of Investigation (FBI), companies reported $26.2 billion in losses from 166,349 domestic and international incidents over three years between June 2016 and July 2019.[1]

In this respect, healthcare is no different from other industry verticals. The *2020 HIMSS Cybersecurity Survey*, based on feedback from 168 U.S.-based healthcare cybersecurity professionals, reported that seven out of 10 experienced recent "significant security incidents." Among all exploits, business email compromise—in the forms of general phishing or targeted spear-phishing—is by far the most common type of significant security incident they face.[2]

"That survey showed that 89% of all attacks on health systems start with an email," said Ryan Witt, Managing Director of Proofpoint's healthcare industry practice. "And it's been that way now for three or four years. That tells you where the problem is."

Produced in partnership with
HIMSS™

*"A single compromised email account can lead to a situation where an organization can't provide patient care, where they are forced to turn away cancer patients for treatment or stop procedures. … It's clear that a strong cybersecurity posture directly relates to healthcare's overarching mission, providing safe, effective patient care."*

**Ryan Witt** | Managing Director, Healthcare Industry Practice | Proofpoint

## Targeting healthcare's supply chain

If email represents the attack vector, who are the targets in healthcare? Surprisingly, the bull's-eye isn't on patient data.

"Financial information is king," the HIMSS report found, ranking it ahead of employee information and patient data. "A broad range of threat actors may benefit from stolen financial information … to compromise bank accounts and divert wire transfers of funds into accounts that are controlled by them."[3]

The message for health IT security is clear: If you're trying to identify your VAPs (very attacked people) and your MVD (most vulnerable data), look no further than your supply chain.

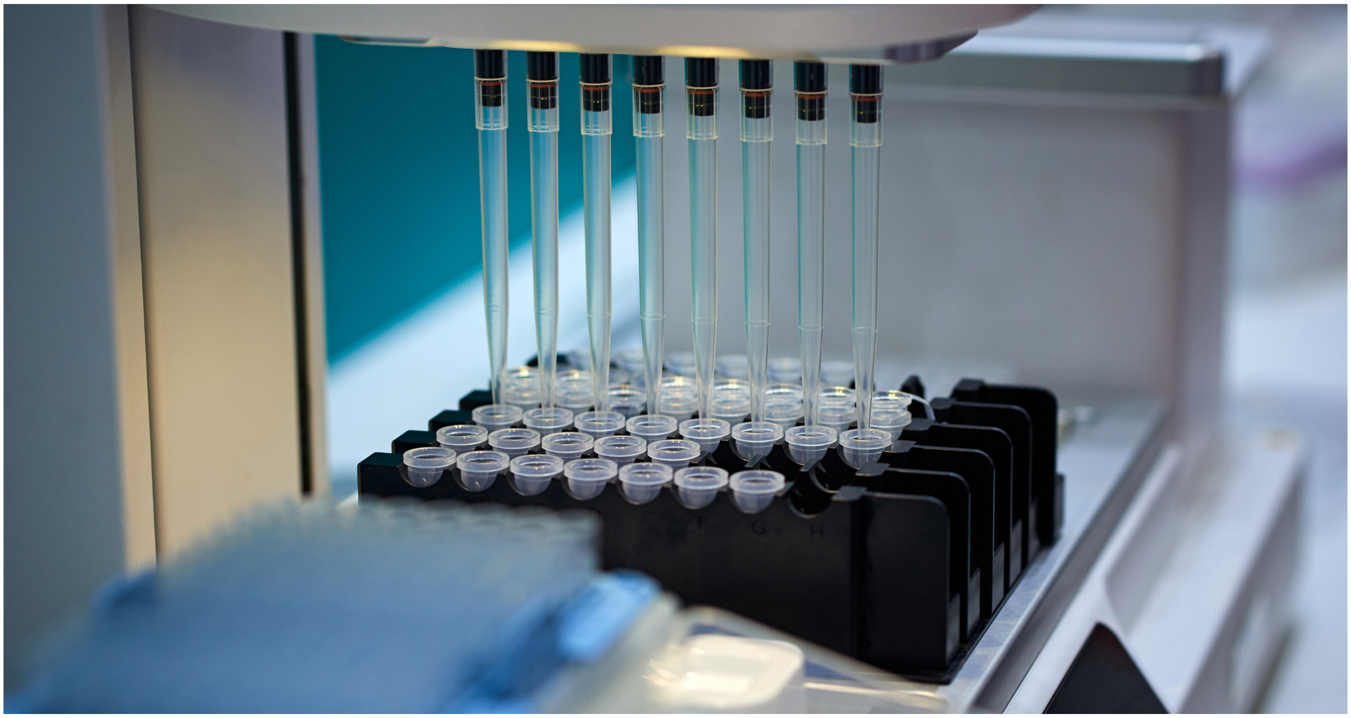
One reason for this focus is limited resources. The HIMSS survey noted that cybersecurity accounts for just 6% of an average hospital's IT budget.

"In an ideal world, we would all have the gold standard of cybersecurity," Witt said. "But that's not practical in healthcare, where there are significant challenges, both from a budgetary and a resource standpoint. So it's about choosing the right control for what activity you're trying to protect."

Another reason to concentrate on the supply chain is the sheer volume and value of business conducted by email. During a seven-day survey of its clients, Proofpoint found that the average healthcare organization received about 200,000 emails from over 10,000 different domains, including those belonging to research organizations, construction companies, grantors and foundations and insurers, as well as classic supply chain participants.

"Of these clients, 98% received some email-based threat, and 97% received threats from at least one of their suppliers' domains via impersonation or business email compromise," said Rob Holmes, Vice President and General Manager of Email Fraud Defense, Proofpoint. "So it's really rife. Some of the attacks we've seen are chasing invoices worth $2.5 million. That is not uncommon."

Supply chain employees are working in incredibly vulnerable ways, which is compounding the problem more and more often, according to Witt: "It's one of those job functions where you need to download files, … invoices, proposals, billing information and other documents, and so you need to click on links. And then, of course, you're working with money."



> *"If you want to solve for invoice fraud, you need to make sure that you can't pay people based on an email. I would encourage a CISO to work with the chief financial officer to scrutinize their payment processes and incorporate systemic controls when they review, accept, approve and execute wire transfers."*
>
> **Rob Holmes** | Vice President and General Manager of Email Fraud Defense | Proofpoint

But perhaps the most important reason to focus on supply chain is its potential impact on patient safety. Instead of seeking out technical vulnerabilities in a healthcare organization's networked infrastructure, today's attackers use social engineering lures to compromise email accounts, impersonate employees and incrementally gain access to critical systems.

"This is so much bigger than a HIPAA violation," said Witt. "A single compromised email account can lead to a situation where an organization can't provide patient care, where they are forced to turn away cancer patients for treatment or stop procedures, or even re-create medical records from scratch because of the severity of the attack. It's clear that a strong cybersecurity posture directly relates to healthcare's overarching mission, providing safe, effective patient care."

## A comprehensive strategy for email fraud defense

Defending against email fraud requires a quantum shift in thinking. Just three or four years ago, attackers hid malware into the email itself, so protecting users meant scanning the email body or attachment for known viruses, trojan horses and other black hat technology, according to Holmes.

"We have done a pretty good job against that kind of attack by inspecting URLs on a static and dynamic basis and classifying them as fraudulent or malicious," he said. "But there's this relatively new class of attacks where there's no malicious payload for you to inspect. In these social engineering attacks, cybercriminals will strive to compromise or impersonate the identity of somebody you trust, which may ultimately end in some kind of exploit. This dynamic has forced people to pay as much attention to the 'from' field of email as they do for the email body or attachments."

Holmes and Witt recommend a "people, processes and technology" approach to defeat email fraud. It's critical to deploy authentication controls (e.g., Domain-based Message Authentication, Reporting and Conformance [DMARC]; DomainKeys Identified Mail [DKIM]; and Sender Policy Framework [SPF]) to examine the source and ensure that external emails come from legitimate accounts. Furthermore, emails from suppliers known to have been compromised, or which have not locked down their own domains, ought to face greater scrutiny. Finally, these technologies should block any emails using spoofed or look-alike domains before a user ever receives them.

But a comprehensive strategy also empowers frontline users to become part of the security team. According to Raj Chopra, Vice President of Product Management for Email Security, Proofpoint, that means the old approach to training will no longer suffice.

"It requires educating the users on an ongoing basis—not some training that people do once in six months and then never think about it again—but continual education *as they're interacting with their email*," he said.

For example, Chopra said, a defense-oriented gateway should tag suspect email with warning labels, alerting the user in situ that he or she should be on guard. And since gateway data forensics should identify who your VAPs are and precisely how they are targeted, individual users should receive highly specific training to help them recognize the threats they face.

Finally, organizations should incorporate processes and policies into automated workflows to prevent the most common kinds of supply-chain fraud.

"If you want to solve for invoice fraud, you need to make sure that you can't pay people based on an email," Holmes said. "I would encourage a CISO to work with the chief financial officer to scrutinize their payment processes and incorporate systemic controls when they review, accept, approve and execute wire transfers."

## Stopping data exfiltration

Prevention may be the best defense, but it shouldn't be the only one in your email security playbook. That's where data exfiltration prevention (i.e., data loss prevention [DLP]) comes into play. Even when an exploit circumvents your filters and your highly trained staff, technology can help prevent harm.

One method Witt recommends is the ability to sandbox user actions in a way that examines malicious code in embedded URLs or attachments from an organization's infrastructure. Recognizing the large number of third-party workers in healthcare, Witt also emphasized the importance of isolation technology, which allows the safe usage of apps and messaging

> *"You don't want any security measure to become a speed bump. What might be an irritation in a different environment can be life-impacting in healthcare. You never want to get in the way of clinical staff who need to access data to care for a patient."*
>
> **Raj Chopra** | Vice President of Product Management for Email Security | Proofpoint

tools: "Implemented correctly, there's no possibility of moving data beyond that container, in or out. So a bad actor can't use a third-party messaging app as a launchpad to get into your network, and the healthcare worker can't exfiltrate data out of your network because it's all been containerized."

Another critical step in curbing data loss can be achieved by paying as much attention to outgoing email as you do with inbound messages, according to Chopra. By instantiating an organization's policies into an analysis of outbound emails before they exit the gateway, you can prevent significant data loss and fraud.

"This approach asks—under our policies, is this the kind of information that can be sent out, *period?* Does it have more than 10-number IDs and Social Security numbers? Because, if that is the case, then email is not the right tool to send this information," he explained.

An organization should also define and watch for suspicious behavior; a sudden change can indicate a compromised account. "People are defined by their habits," Chopra said. "Why are you suddenly sending attachments to a Gmail account? Why are they encrypted now? If you've never seen encrypted emails being sent out from an internal account before, it's critical to investigate."

Finally, Chopra added, both email fraud defense and DLP must be implemented as seamlessly as possible when the mission is patient care and safety.

"You don't want any security measure to become a speed bump," he said. "What might be an irritation in a different environment can be life-impacting in healthcare. You never want to get in the way of clinical staff who need to access data to care for a patient."

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

**References**

1. Federal Bureau of Investigation. 2019. Business email compromise the $26 billion scam (Alert # I-091019-PSA). Sept. 10. https://www.ic3.gov/Media/Y2019/PSA190910.

2. HIMSS. 2020 HIMSS cybersecurity survey. Nov. 16. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf.

3. Ibid.

proofpoint.

**About Proofpoint**

Proofpoint is a leading cybersecurity company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, we help companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on us for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

Produced by HIMSS™ | www.himss.org | ©2021