Stop Fraudulent Emails Before the Damage Is Done

How Seattle Children's Hospital utilized Proofpoint's email fraud defense solution to fend off BEC attacks

When Chief Technology and Security Officer Gary Gooden joined Seattle Children's Hospital in March 2019, he knew that if he wanted to improve the organization's cybersecurity posture, he'd have to start with its biggest blind spot: email.

"Email fraud defense [EFD] was a critical need," Gooden recalled. "The primary vector for breaches was—and remains—email: fraud, business email compromise [BEC], ransomware—everything to do with other types of phishing campaigns. All those attacks were evident, obvious and ongoing."

Those problems weren't unique to Seattle Children's. Over the last few years, cybercriminals have shifted their focus away from networks and machinery and set their sights on vulnerable human targets. According to the 2020 HIMSS Cybersecurity Survey, roughly 90% of targeted cyberattacks today originate over email.[1]

The most costly of these are BEC attacks. Relying on social engineering rather than technical exploits, they're practically invisible to traditional security tools. Recipients—thinking that they're interacting with someone they know and trust—are tricked into doing the attacker's bidding.

In an all-too-common scenario, BEC victims have induced members of accounting teams to send tens of thousands of dollars (and in some cases, much more) to bank accounts controlled by fraudsters posing as vendors and suppliers. The FBI estimates that companies incurred $26.2 billion in losses from 166,349 incidents globally between June 2016 and July 2019.[2]

"As these attacks become more sophisticated—via identity spoofing or credential-stealing—traditional security tools won't cut it," said Ryan Witt, Managing Director, Healthcare Industry Practice at Proofpoint. "Organizations will need next-

> *"Email fraud defense was a critical need. The primary vector for breaches was—and remains—email: fraud, business email compromise, ransomware—everything to do with other types of phishing campaigns. All those attacks were evident, obvious and ongoing."*

Gary Gooden | Chief Technology and Security Officer | Seattle Children's Hospital

> *"As these attacks become more sophisticated—via identity spoofing or credential-stealing—traditional security tools won't cut it. Organizations will need next-generation controls and an integrated email fraud defense solution to keep patient records safe, secure the supply chain and protect their brands."*
>
> **Ryan Witt** | Managing Director, Healthcare Industry Practice | Proofpoint

generation controls and an integrated email fraud defense solution to keep patient records safe, secure the supply chain and protect their brands."

Gooden, who previously logged more than two decades of work as a security executive before assuming his new post, heartily agreed with that view. The problem he faced at Seattle Children's wasn't that the healthcare system lacked a toolkit, he said, "but we didn't necessarily have the right tools in it. And when we did have the right technology, it wasn't fully implemented."

While Seattle Children's Hospital did have some mixed-generation firewalls in place, "we weren't monitoring the environment correctly to ascertain our threat level," Gooden explained. The system didn't have any real visibility into east-west traffic within its environment and lacked intrusion prevention detection along its network perimeter.

And when most staff shifted to remote work during the COVID-19 pandemic, "it exponentially increased our threat surface," he said.

There couldn't have been a better time to embrace a dynamic EFD solution.

Implementation tiers: Technology, people and policies

In partnering with Proofpoint, Gooden's priority was to prevent Seattle Children's domain from being spoofed in attacks against its patients, partners and staff. "And by extension, we would help protect the organization's brand," he added.

The implementation methodology involved a three-pronged approach that ensured they'd connect the right technology with the right people and policies at the health system.

- **Technology.** When it comes to technology, Witt said, Proofpoint advises "clients to do everything they can to stop these threats before they reach the people they're trying to attack." Seattle Children's has deployed Targeted Attack Protection (TAP) to monitor incoming emails and block advanced threats that used malicious attachments and URLs and data loss prevention (DLP) to filter outbound email containing sensitive data. Gooden has also layered on threat response auto-pull (TRAP) to reduce the labor required to respond when TAP detected malicious email across the health system and EFD to protect against imposter attacks by authenticating email traffic.

> *"Everyone in communication must agree upon the security protocols. It's an operational tale, where we're constantly trying to mature our ability to manage the EFD stack."*
>
> **Gary Gooden**

- **People**. In tandem with Proofpoint's Security Awareness Training program, Seattle Children's began testing its users through simulated phishing campaigns—with just-in-time training when their staff failed to recognize fraudulent email. Gooden's team also began publishing security awareness notifications across the multi-state organization, focusing on safe computing practices and raising awareness of security threats among staff.

  It's essential, Witt said, for staff to understand how deeply cybercriminals will dig into your organization, your role hierarchy and each staff member's responsibilities in order "to design a compelling email that will lure the end user to take the criminals' desired action, no malware required." In this way, Gooden said, Seattle Children's gave particular attention and training to what Proofpoint calls Very Attacked People™ (VAP) to mitigate their higher levels of risk.

- **Process**. Policies that remain an ongoing process comprise the final pillar, according to Gooden. Seattle Children's recently implemented new procedures for users who either send or receive payments, requiring them to verbally confirm any requests to redirect payments before making the requested changes. Additionally, Gooden's team placed branded "warning" notifications above externally sourced messages to inform users to proceed with caution. Users are still allowed to click external links as they see fit; the company uses TAP to rewrite the URL to inspect unknown or suspicious links.

Since kicking off the project in April 2019, Gooden said the primary challenge was tracking down "owners" of various email streams and workflows to confirm who was sending what and why.

"After identifying the players involved in an email stream or workflow, we then had to safelist domains in such a way that we would not stop them from communicating once we went into enforcement," he said. "That kind of sleuthing work was a sizable workload, but it's necessary if you are trying to do things like EFD."

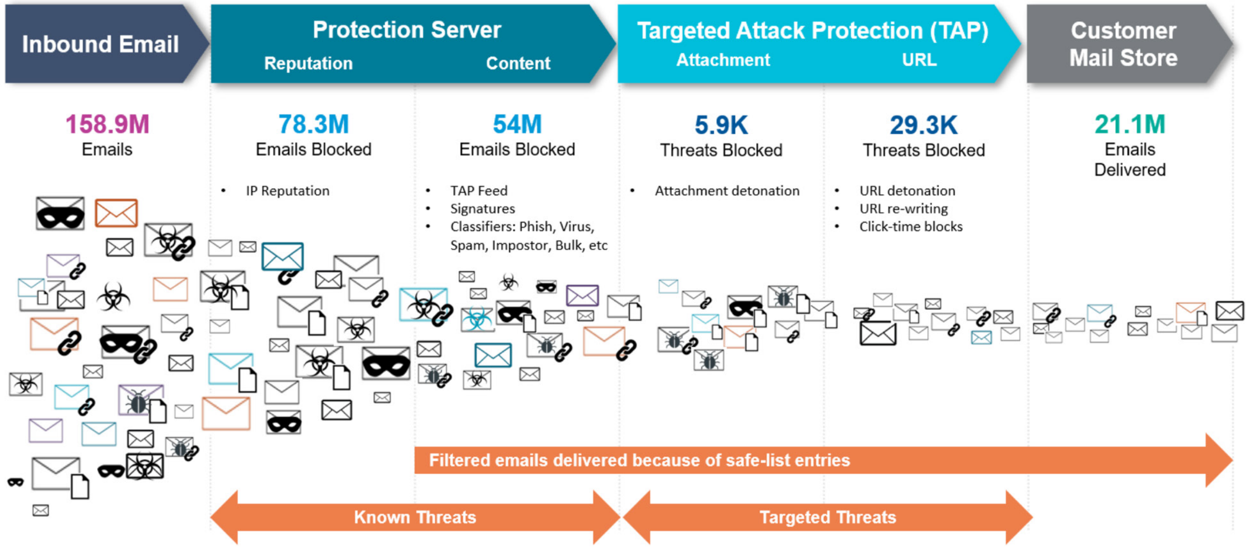
An ongoing project

Seattle Children's EFD solution went live in June of 2020. Gooden said he is happy with the results. But he added email security is very much a living project, not just a simple implementation.

"These tools are helpful and customizable, but that means that more than ever, everyone in communication must agree upon the security protocols," he said. "It's an operational tale, where we're constantly trying to mature our ability to manage the EFD stack."

The highest value, he reports, exists in general awareness of email-related threats, regardless of project, department or location. As Gooden pointed out, this step has also prevented shadow IT from arising because the domain cannot be used without permission.

Figure 1. Email threat protection summary statistics—July 2019 through April 2020



Source: Seattle Children's Hospital. 2020. Stop fraudulent emails before reaching your clinical staff, patients and associates [webinar]. https://www.himsslearn.org/stop-fraudulent-emails-reaching-your-clinical-staff-patients-and-associates

"Proofpoint helped improve our posture and hardening for BEC attacks as previously we did not have a Domain-based Message Authentication, Reporting and Conformance [DMARC] setting," he said. "BEC attacks targeting our brand are significantly more visible now."

For other organizations considering an EFD solution, Gooden and Witt recommend prioritizing how technology and people come together to act as a first line of defense. Technically, think about specific needs and capabilities:

- TAP helps detect, mitigate and isolate advanced threats that target people through email by detecting known and unknown threats involving malicious attachments and URLs.
- TRAP provides security teams with orchestration and automation capabilities to retract malicious emails delivered to user inboxes.
- DMARC authentication detects and prevents email spoofing techniques used in phishing, BEC and other email-based attacks.

Above all, it's crucial to conduct continuous security awareness training for every employee with access to the system. "They're being attacked, but they're also your front line," said Witt. "Run simulations and training with staff to understand where to best place your adaptive controls."

> *"Proofpoint helped improve our posture and hardening for BEC attacks as previously we did not have a DMARC setting. BEC attacks targeting our brand are significantly more visible now."*
>
> **Gary Gooden**

"Understand that the technology is one thing, but your patience around discovering what the process is concerning the people who are involved will be your long pole," said Gooden. "If you're not willing to roll up your sleeves and do that type of work, then you will have a problem implementing any solution."

It's more reasonable, Gooden added, to make sure your health system works with a partner that can offer insights from the field with a willingness to teach and demonstrate exemplary practices: "Implementation of EFD requires a thoughtful, holistic and partnered approach."

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

References

1. Healthcare Information and Management Systems Society. 2020. 2020 HIMSS cybersecurity survey. Nov. 16. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf.

2. U.S. 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.

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