SPOTLIGHT

Sponsored by: Proofpoint

With employees and business associates at the center of most data loss incidents, defending data starts with protecting people.

Protecting Healthcare Organizations with Human-Centric Email Security

June 2024

Written by: Lynne A. Dunbrack, Group Vice President, Public Sector

Introduction

Three out of four cyberattacks start with an exploitation of a human element. These attacks often start with bad actors sending emails using spoofed identities to target people. Threat actors also leverage generative AI (GenAI) to speed up the creation of authentic-looking and sounding email messages. These messages lure unsuspecting users into clicking on a link, opening an attachment that contains malware or ransomware, or revealing more information about themselves to enable identity and credentials theft. Human error can also cause data loss when an email is misdirected to an unintended recipient.

Healthcare organizations need to take a human-centric approach to security to protect themselves. This involves addressing two fundamental challenges: protecting people and defending data. Healthcare organizations must focus on:

- Protecting information coming in from email
- Preventing misdirected email because of human error
- Protecting transactional emails, such as mass emails that a third-party sender sends

IDC's March 2024 *U.S. Healthcare Provider IT Survey* confirms that healthcare organizations are investing in various security technologies to protect vulnerable IT and data assets. Of the 37.5% of respondents who expect their security budgets to increase over the next 12 months, 29.6% say that increased funding will be allocated to data loss prevention (DLP). DLP ranked second in investment priority after identity management (32.2%).

AT A GLANCE

KEY STATS

- Three out of four cyberattacks start with an exploitation of people (source: 2023 Data Breach Investigations Report: Frequency and Cost of Social Engineering Attacks Skyrocket, Verizon, June 2023)
- Of the 37.5% of respondents who expect their security budgets to increase over the next 12 months, 29.6% say that increased funding will be allocated to data loss prevention (source: IDC's *U.S. Healthcare Provider IT Survey,* March 2024).

KEY TAKEAWAY

Healthcare organizations need to take a human-centric approach to cloud email security to protect against accidental and deliberate data loss. Additional security training will help improve employee resiliency.

Four Dimensions of Human Risk

To create an effective human-centered security strategy, it is important to understand the four distinct dimensions of human risk:

- **Threat risk:** Email is still the number 1 attack vector, and in 2024, it remains an unauthenticated communication channel. Threat actors have long discovered that it is easier to lure people into clicking a link or file to launch their attack through social engineering than to breach well-established network security technology.
- **Identity risk:** Vulnerabilities such as weak access controls, excessive user permissions, and other poorly defined identity and access management processes result in identity risk. Once identities are compromised, threat actors can launch business email compromise (BEC) and account takeover (ATO) attacks, which are prevalent in Microsoft 365.
- **Impersonation risk:** Multistage threats start with deception to obtain end users' credentials. This enables the threat actor to take over an account and impersonate the victim to conduct fraudulent business transactions or compromise key suppliers.
- **Data loss:** Often, data loss occurs when a careless user inadvertently sends a sensitive email to the wrong recipient. It also happens when a malicious user has nefarious motives, such as stealing intellectual property before resigning from (or being terminated by) their employer.

Benefits of an End-to-End Email Security Solution

A comprehensive, end-to-end email security solution addresses every type of threat in the email delivery chain and provides the following benefits to healthcare organizations:

- **Detect and prevent social engineering attacks and malicious URLs in the predelivery stage:** The predelivery stage is defined as scanning emails before they enter the cloud email environment. In this stage, an organization must be highly efficient in stopping threats. Considering the large volume of threats that are sent to the enterprise, organizations need to maximize their detection of threats such as spam, phishing, business email compromise, and malware. Advanced threat detection techniques — such as machine learning (ML), threat intelligence, behavioral analysis, and semantic analysis — can ensure suspicious emails are identified and blocked. Attachments and links may be executed in a sandbox environment. This allows one to observe their behavior in a controlled setting and detect threats that may not be apparent through static analysis alone.
- **Stop targeted threats such as lateral internal phishing and advanced email fraud in the postdelivery stage:** The postdelivery stage is defined as scanning and remediating emails after they are inside the cloud email environment. In this stage, AI-based detection provides an extra layer of protection against advanced threats such as BEC. This additional protection can be applied to all users within the company. Or it can be specifically used with high-risk individuals, such as employees who are often targeted by threat actors, VIP employees like executives, or employees with special privileges. Additional postdelivery controls include user reporting of suspicious messages, automated abuse mailbox management, and in-the-moment email warning tags to help users make more informed decisions.

- **Ensure real-time URL protection in the click-time stage:** The click-time stage refers to the point where the user is engaging with the email, in particular clicking on URLs. One risk here is threat actors weaponizing URLs after delivery. In this stage, click-time protections can help stop these threats. They include URL rewriting with click-time sandboxing and browser isolation.

Because threat actors have a broad arsenal, it's important to take a layered approach to defense. This helps counter all the different techniques that are used to target employees.

Both Threat Actors and Security Vendors Are Using AI to their Advantage

While email security is not "sexy" compared with other security strategies, it is essential for protecting a fundamental work process in every industry, including healthcare. Email is a significant attack vector since it is an unauthenticated communication channel. Cloud-based email is easy to spoof. And users reading email on their smartphones may not notice the visual cues of phishing emails, such as inconsistencies in email addresses or domains. Thus they unwittingly fall prey to phishing attacks despite taking numerous security training classes.

Corporations are not the only ones using GenAI to increase employee efficiency and productivity. Cybercriminals are using it to churn out more realistic emails by adopting more professional writing styles; eliminating spelling, typos, and grammatical errors; and translating fraudulent emails into other languages with minimal translation errors. Using ML tools to better understand user behavior allows bad actors to create more attractive socially engineered lures to which users will more likely respond.

In turn, security providers are embedding ML and natural language processing to better understand user behavior and detect anomalies that could indicate a data breach has occurred or will occur to mitigate the risk of an attack. Many of the mundane — but still important — tasks can be automated using AI, reducing the drudgery for security professionals while accelerating threat detection.

Considering Proofpoint

Founded in 2002, Proofpoint Inc. is a leading human-centric cybersecurity company serving more than 510,000 customers worldwide. On average, Proofpoint reports that it scans and analyzes 3.1 trillion emails, 21 trillion URLs, and 0.8 trillion attachments and monitors 45 million cloud accounts for takeover detection per year using advanced AI and ML. It uses these insights to improve its clients' security posture. Proofpoint's largest customer segments are financial services and healthcare.

Proofpoint offers end-to-end email protection across the entire predelivery, click time, and postdelivery email attack chain. Its core email security packages include advanced AI-based predelivery detection and comprehensive protection powered by NexusAI, Proofpoint's proprietary AI engine built on trillions of data points, capable of stopping various payloadless social engineering threats like advanced email fraud and malicious links. In addition, Proofpoint offers adaptive email security with behavioral AI defense postdelivery to counter targeted threats like internal phishing, specifically for high-risk employees, with seamless API integration with Microsoft 365. Proofpoint organizes its product portfolio into four families: people protection, information protection, human risk mitigation, and premium services. Under people protection, the focus of this Spotlight, are the product packages shown in Figure 1. Each package builds on the company's Core P0/P1 solution and subsequently each other to provide comprehensive protection:

- **Core P0/P1 delivers essential email threat protection:** There are multiple modules within Core P0/P1. Targeted Attack Protection (TAP) detects, analyzes, and blocks advanced email threats involving social engineering such as BEC, phishing emails, malware and ransomware, and spam. Threat Response Auto-Pull works with TAP to protect users from incoming malicious emails. Closed-Loop Email Analysis and Response streamlines the evaluation of emails users report as potentially malicious to an abuse mailbox. People Risk Explorer analyzes and segments the risks that internal and external users pose to identify the users most likely to pose a threat.
- **Core Plus provides impersonation protection:** Impersonation targets can be internal employees or third parties such as customers and suppliers with whom employees would typically communicate but who may have been compromised or spoofed. Email Fraud Defense secures email channels, mitigates email fraud, provides visibility into fraud risks posted by external parties, and simplifies domain-based message authentication, reporting, and conformance (DMARC) authentication. Secure Email Relay protects application-generated email and supports the migration of on-premises email relays to the cloud. Supplier Threat Protection looks for suspicious emails from suppliers and third-party accounts to detect potential phishing, malware, and business email account compromise attacks. Analysis of patterns across Proofpoint's customer base enables alert notification before threat actors launch their email attacks.
- **Advanced offers adaptive email data loss protection:** Building off the capabilities of Core and Core Plus, the Advanced package uses behavioral AI to detect anomalies, prevent email from being delivered to the wrong recipient or the right recipient but with the incorrect email attachment, and detect data infiltration in real time. Email Data Loss Prevention detects sensitive or confidential data within an email so that it can be further tracked and safeguarded. Email Encryption automatically encrypts emails and attachments, thus ensuring more secure email communications. The Advanced package mitigates the risk of data loss at the hands of the careless, compromised, or malicious user.
- **Complete ensures identity protection:** There are two modules in the Complete package. Identity Threat Defense and Response continuously scans for identity threats to stop privilege escalation and lateral movements of threat actors to their ultimate target of extremely sensitive — and lucrative on the dark market — data assets. TAP Account Takeover identifies the diverse types of threats targeting email accounts, including business email compromise, brute-force attacks, and data exfiltration. It automates alerts for them and accelerates email threat investigation and account remediation.

FIGURE 1: ***Four Key Proofpoint Packages for Protecting People***

Source: Proofpoint, 2024

Cloud Email Security Use Cases

Deployed together, Proofpoint's extensive offerings address the following use cases:

- **Increased prevalence of human social engineering:** Threat actors are taking advantage of AI to launch more sophisticated attacks involving human social engineering. They use GenAI to quickly generate phishing emails that mirror the targeted organization's communication style or translate effective phishing emails into other languages to attack targets in other countries. The Core P0/P1 package protects against BEC, ATO, credential theft, and financial fraud attacks.
- **Increased reliance on third-party vendors:** Healthcare organizations are leaning on third-party email services to send emails on their behalf for marketing campaigns, customer support, and other administrative workflows. The Core Plus package protects against vendor email compromise through its Supplier Threat Detection module.
- **Data loss:** Misdirected email by careless users is as much a problem as data exfiltration, if not more so, because users have logged in with legitimate credentials and may be misdirecting email to validated recipients (e.g., wrong customer or colleague). Proofpoint's inaugural edition of its *2024 Data Loss Landscape Report* (January 2024) revealed that more than 70% of respondents across industries identified "careless users" as a cause of their data loss, while fewer than 50% cited technical issues. The Advanced package offers protection against both forms of data loss.

- **Identity compromise:** Active Directory (AD) identities are a common target for theft. Once AD has been compromised, threat actors can use legitimate credentials to move laterally through the network or escalate privileges to gain access to more sensitive information. The Complete package offers identity threat defense and detection and identifies potential account takeover events.

Challenges

These are some of the biggest security challenges faced by the healthcare industry and Proofpoint alike. They can also present opportunities for Proofpoint with its strong healthcare expertise and a broad product portfolio where its expertise can help. In detail:

- **Cybercriminals are constantly evolving their craft to exploit new vulnerabilities.** Threat actors are creative, and they are quick to adapt their strategies to exploit new vulnerabilities. This includes embracing AI, including GenAI, to accelerate their efforts to launch new attacks.
- **Email attacks are on the rise.** Given that most emails occur between parties known to each other (or at least they think they are), email senders and recipients trust that the email exchange has not been compromised. This unsuspecting nature makes end users more susceptible to attacks because they often show poor email hygiene. The more successful threat actors are at exploiting this channel, the more they will continue using it.
- **There's a heightened demand for security professionals.** Cyberattacks are increasing across all industries. It is difficult for healthcare organizations to attract and retain security professionals when they are competing for specialized talent against companies with better IT funding. As such, healthcare organizations are leaning on their security vendors to provide much-needed expertise.
- **There are complexities associated with acquisitions.** Integrating a new acquisition brings security challenges. Proofpoint is no stranger to acquisitions, having spent more than $1 billion to acquire 18 companies. Tessian, its latest acquisition, was completed in December 2023.

Conclusion

IDC recommends that healthcare organizations take a multipronged, human-centric approach to email security. This means:

- Moving beyond "good enough" solutions as threat actors are advancing faster than "good enough"
- Monitoring email threats to protect people and defend data
- Looking for innovative solutions that use AI and ML to detect threats within high volumes of email
- Reviewing processes for potential vulnerabilities and identifying where verification/authentication of suppliers and partners needs to increase
- Making employees resilient to these attacks

Behind every data loss incident is a person.

Threat actors and healthcare organizations are each racing to exploit AI and GenAI. Healthcare organizations will need data to train their models to understand relationships between recipients and senders and semantics to detect spurious emails. Behind every data loss incident is a person. Healthcare organizations require innovative educational approaches and teaching modules, such as brief training snippets, to instruct their employees on protecting themselves and their email. This is important because threat actors' exploits are rapidly evolving.

IDC believes the email security solutions market will continue to be important. To the extent that Proofpoint can address the challenges described in this paper, the company has a significant opportunity for success.

About the Analyst

Lynne A. Dunbrack, *Group Vice President, Public Sector*

Lynne Dunbrack is group vice president for Public Sector, which includes IDC Government Insights and IDC Health Insights. She manages a group of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads IDC Health Insights' Connected Health IT Strategies program.

MESSAGE FROM THE SPONSOR

About Proofpoint

Proofpoint, Inc is a leading cybersecurity and compliance company that provides health institutions protection and visibility for their greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps healthcare stop targeted threats, safeguard their patient data and intellectual property, and make their users more resilient against cyberattacks. Leading healthcare organizations of all sizes, including more than seventy-five percent of the Fortune 500 healthcare organizations, rely on Proofpoint for human-centric security solutions that mitigate their most critical risks across email, the cloud, social media, and the web before they cause lasting harm. More information is available at www.proofpoint.com/healthcare.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com