proofpoint.

REPORT

2022 Healthcare Cyber Crime Update

A department-level analysis of email-based attacks on healthcare systems

proofpoint.com

Executive Summary

Amid a growing array of threats, the healthcare industry is pummeled by hundreds of successful cyber attacks each year. Ransomware, business email compromise (BEC) and state-sponsored attacks are just a few of the threats that keep security teams awake at night. Overwhelmed staff have a long list of things they should do to reduce risk—but lack sufficient bandwidth and budget to see them through.

In this context, Proofpoint presents the "2022 Healthcare Cyber Crime Update." This report is designed to help healthcare organizations prioritize efforts that will improve their security posture the most.

This report is based on new enhancements in data analysis deployed by our engineers for the healthcare sector using aggregate telemetry through Proofpoint Targeted Attack Protection (TAP). We analyzed data from six of the largest U.S. healthcare organizations gathered from January 2021 through December 2021.

We analyze:

- The overall volume of malicious emails
- Click rates on malicious messages by department
- The raw number of clicks by group
- The volume of incidents for ransomware and fraud

While all these metrics fluctuated up and down across the board, we saw a few general trends. First, the volume of attacks and click rates trended upward. And while ransomware settled to more stable levels after the first quarter, tactics used for business email compromise (BEC) and other types of fraud spiked again in the fall.

The findings of the report reinforce what healthcare organizations already know—that threats are increasing and growing more complex. In this environment, a people-centric approach to cybersecurity is critical. Rather than focusing on networks and devices, organizations should understand that bad actors target people. Only a security strategy based on protecting people gets to the root of the problem.

Over the past several years, cyber criminals have increasingly targeted the healthcare industry. In 2021, 600 breach incidents were reported to the U.S. Department of Health and Human Services. Alarmingly, at least 10 of these incidents affected the personal health or financial information of *more than one million patients each.*[1] As a result, "the year has seen some of the largest cybersecurity impacts in healthcare's history."[2]

Ransomware is a growing threat that has hit healthcare especially hard. Recent attacks have shut down IT systems at major hospital systems for as long as several weeks,[3] hurting patient care in the middle of a pandemic. One doctor flatly told a U.S. House committee that "healthcare is not prepared to defend or respond to ransomware threats."[4]

Cybersecurity risks from devices and software

Awareness has also grown about some of the sector's unique vulnerabilities. For example, the security of medical devices has drawn intense attention over the past year.[5] Researchers have discovered vulnerabilities in infusion pumps,[6] insulin pump controllers[7] and other lifesaving devices. One issue is the sheer complexity of a typical hospital's inventory—thousands of different device types, each with its own software and hardware to maintain. To make matters worse, many of these devices lack security-by-design features and must be patched individually.[8]

The software supply chain also presents a risk to healthcare organizations. The worlds of application security and software development were rocked in December 2021 by news of a severe remote code execution vulnerability in a widely used Java logging library called Apache Log4j.[9] The Department of Health and Human Services' (HHS) Health Sector Cybersecurity Coordination Center (HC3) issued an alert in December. It warned healthcare organizations to ensure that none of their software is running vulnerable versions of Log4j. This is a tall order. Many institutions have a huge number of unique devices.[10]

[1] Jessica Davis *(SC Media)*. "10 biggest healthcare data breaches of 2021 impact over 22.6M patients." December 2021.

[2] Ibid.

[3] Stacy Weiner *(AAMC)*. "The growing threat of ransomware attacks on hospitals." July 2021.

[4] Jessica Davis *(SC Media)*. "'Health care is not prepared': Physician details deficiencies in market's ability to combat ransomware threats." July 2021.

[5] Jessica Davis *(SC Media)*. "'Nothing is a standalone device': How a complex ecosystem leaves medical security in flux." August 2021.

[6] Jill McKeon *(Health IT Security)*. "Infusion Pump Vulnerabilities Point to Gaps in Medical Device Security." August 2021.

[7] Jill McKeon *(Health IT Security)*. "FDA Recalls Medtronic Insulin Pump Controller, Cites Cybersecurity Risks." October 2021.

[8] Jessica Davis *(SC Media)*. "'Nothing is a standalone device': How a complex ecosystem leaves medical security in flux." August 2021.

[9] Lily Hay Newman *(Wired)*. "'The Internet Is on Fire.'" December 2021.

[10] Marianne Kolbasum McGee (H-ISAC). "Log4j Flaw: Healthcare Sector Warned to Take Action." December 2021.

Advanced persistent threats

To make matters worse, state-sponsored actors seem to be stepping up their attacks as geopolitical tensions increase. Several federal agencies released a joint advisory in January 2022 that warned Russian-backed advanced persistent threat (APT) actors are targeting critical infrastructure.[11] On the same day, HC3 confirmed that healthcare may be on the radar of these attackers.[12] When Russian troops invaded Ukraine in late February, the Cybersecurity and Infrastructure Security Agency (CISA) reported a surge of distributed denial-of-service (DDoS) attacks and wiper malware. While they mainly targeting organizations in Ukraine,[13] spillover effects have been reported around the world.

Even before these events, one presenter at the World Economic Forum's Annual Meeting on Cybersecurity in November 2021 issued a stark warning: cyber attacks are threatening the integrity of the healthcare system itself.[14] This reality may jeopardize the sector's ability to provide lifesaving care.

"We can, and should, be doing better," the presenter said.[15] Events since then have only made matters worse.

Methodology

To a large degree, "doing better" means having accurate and timely information. Every day on average, Proofpoint analyzes more than 35 billion URLs, 2.2 billion emails and 200 million attachments. We also monitor more than 22 million cloud accounts per day using advanced artificial intelligence and machine learning. This broad and diverse set of data offers insights into customers' security posture—especially about the risks that stem from people.

Our people-centric approach, along with the data from our far-reaching installed base, provides unique insights that no other company can provide. Our Very Attacked People™ (VAP) analyses are the most visible, public-facing examples of how this information can be applied. VAP analyses identify the job titles within an organization (or groups of them) that face a higher-than-normal risk of attack.

Delivering more granular data

In 2021, our engineers embarked on a project to build out even more detailed metrics for the healthcare sector. The initiative enables data analysts to focus not only on job titles, but on departments as well. It also provides more granular data about attack frequency, how users respond to them and attackers' objectives.

[11] HHS Cybersecurity Program. "Understanding and Mitigating Russian State Sponsored Cyber Threats to U.S. Critical Infrastructure." January 2022.

[12] Marianne Kolbasuk McGee *(Healthcare Info Security)*. "Russian APTs: Why Stakes Are So High for Healthcare Sector. January 2022.

[13] Cybersecurity and Infrastructure Security Agency. "Destructive Malware Targeting Organizations in Ukraine." February 2022.

[14] Stephanie Duguin *(World Economic Forum)*. "If healthcare doesn't strengthen its cybersecurity, it could soon be in critical condition." November 2021.

[15] Ibid.

This study is based on the enhanced data made possible by this project. It uses aggregate telemetry data from six large U.S. healthcare organizations, normalized into a single entity, for January through December 2021. The institutions included in the data set are large health systems with at least 10 hospitals, numerous clinics and employee counts in the thousands. The geographic distribution of these hospital networks makes it relevant to the broader North American market.

Malicious Message Volume: Rising for Much of the Year

Even in organizations that have low click rates for malicious email, the raw number of clicks goes up as the volume of attacks increases. Unfortunately, much of 2021 saw sharp increases in the volume of malicious emails sent by threat actors of all types (Figure 1). At the same time, stress on the healthcare industry has remained high as the COVID-19 pandemic continued for the entire year. This toxic mix of factors increases the odds that healthcare workers might click on a malicious message.

It takes only one click to trigger a damaging breach, so the risk to an organization increases with the number of clicks. As a result, these surges in volume have increased the odds that an attack will succeed.

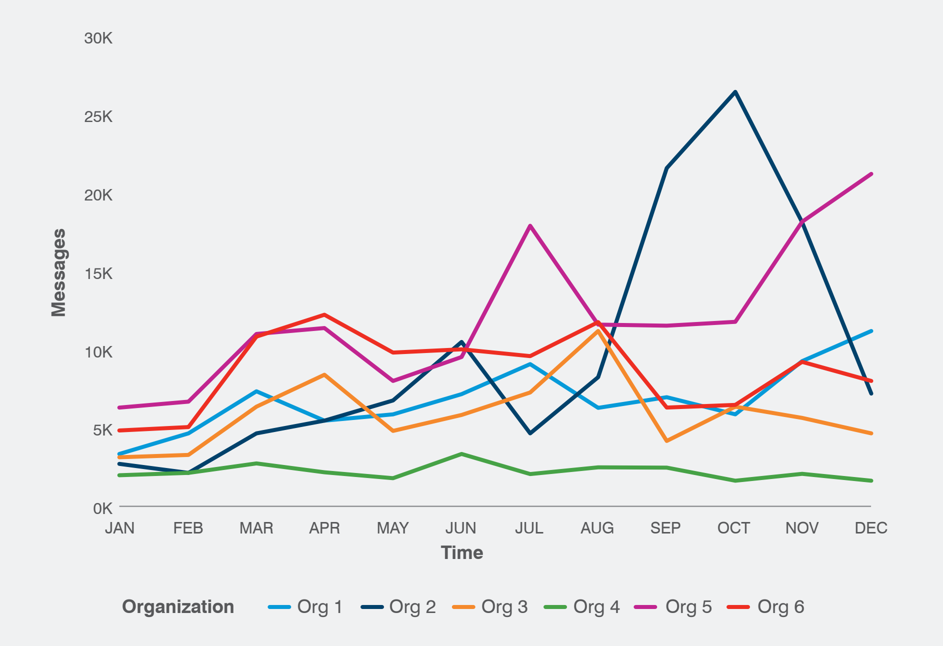

Figure 1. Overall malicious message volume across anonymized organization, January–December 2021.

By department

We can learn much by comparing and contrasting the volume of malicious emails by department. Behavioral health, for instance, saw major increases in the third and fourth quarters (Figure 2). One institution in our sample saw a huge spike in volume in that department in September and October. Most of the other institutions saw more gradual increases within that timeframe.

Overall volume by department — behavioral health

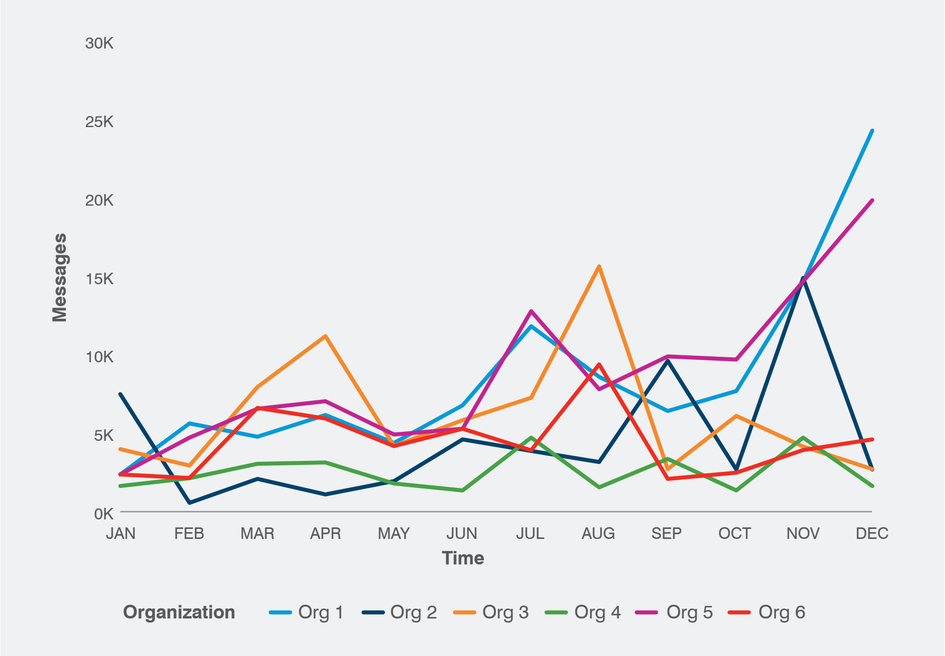

Figure 2. Malicious attack volumes in behavioral health departments, January–December 2021.

This trend is alarming. The ongoing global pandemic and resulting economic recession has impaired many people's mental health, which may increase their vulnerability to cyber crime. People in these departments regularly face stressful interactions with their patients and their families. The pressure and fatigue they face can cause some to click on things that they normally would not.

Three key departments whose work involves matters of life and death also faced a growing volume of attacks in the second, third and fourth quarters (Figure 3).

They include:

- Accident and emergency (A&E)
- Critical and intensive care (CCU/ICU)
- The operating theater, where surgery takes place

For these three departments, attacks more than tripled from February to April and rose further by June. Volumes leveled off after that, but at a much higher level than at the beginning of the year. Then they spiked again in November.

Spikes in these departments are especially troubling because patient safety is most at risk if these departments' systems are disrupted. These attacks hit at the very heart of a healthcare's central mission—saving lives. And while institutions could well suffer compliance penalties, remediation costs and brand erosion from such an event, the effects go far beyond these financial concerns.

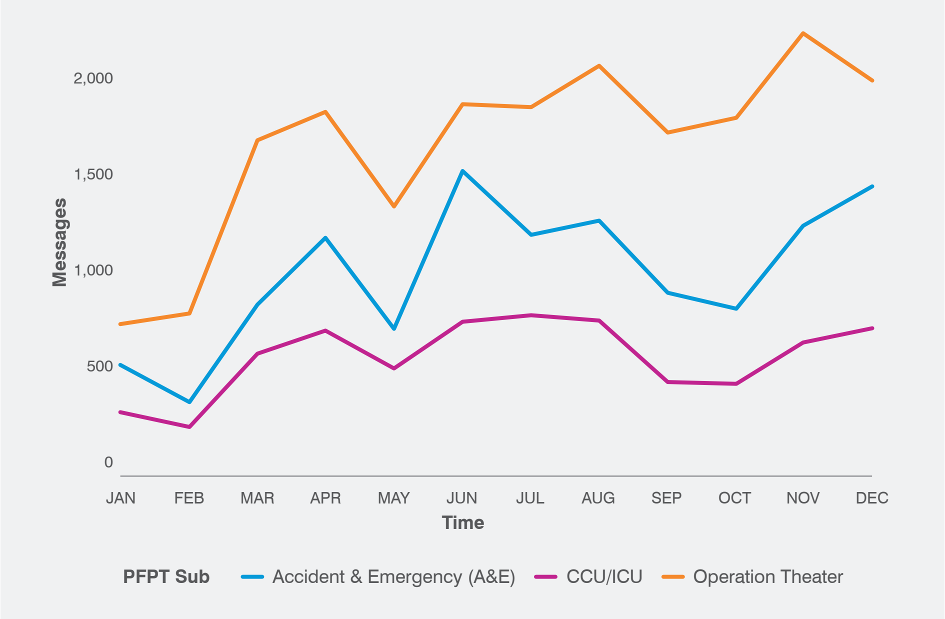

Figure 3. Malicious attack volume for three "life risk" departments, January–December 2021.

Click Rates: Risks to Life, PHI and the Bottom Line

Thankfully, users do not click on most malicious messages. Several factors may contribute to this rare bright spot in our findings:

- Security awareness efforts by employers
- Media coverage of cybersecurity best practices for consumers (which can translate to a work setting)
- Simple common sense by employees

But again, any click rate above zero represents risk to an organization—especially in an environment of elevated volume. It's a classic numbers game: more clicks represent more opportunities for a successful attack. For our customers, these clicks are almost always remediated. But for institutions that lack people-centric protection, the risks add up quickly.

Attackers target departments within healthcare institutions that advance their objectives. Some users may be more likely to fall for an attack, face a higher-than-normal volume of attacks or have elevated access privileges that would make a successful attack especially harmful. Understanding which departments could benefit most from more cybersecurity awareness training can help organizations make the best use of the bandwidth they have.

Overall click rates

Our sample of large healthcare organizations had an overall click rate of 0.62%. That's typical in our experience. But differences in department-level data are revealing. That's because attacks against some departments threaten patient safety. Others may expose protected health information (PHI). Still others may jeopardize an institution's perpetually tight finances.

Of the three "life risk" departments outlined above, two have higher-than-average click rates of 0.70% (Figure 4). The rising volume of attacks on those departments amplifies the raw number of clicks from these departments—and risk to the institution—even more.

But other departments have even higher click rates. Education and administrative departments have click rates of 0.74% and 0.81%, respectively. Social services is even higher at 1.13%. These departments hold confidential data that, if breached, could violate the Health Insurance Portability and Accountability Act (HIPAA) and other regulations.

Facilities and maintenance departments saw an astounding 1.55% click rate. This points to a higher risk to financial records involving supply procurement, construction and services contracts.

Total Click Rate 2021, Top Departments
Click Rates by Department: Risks to Life, PHI and the Bottom Line

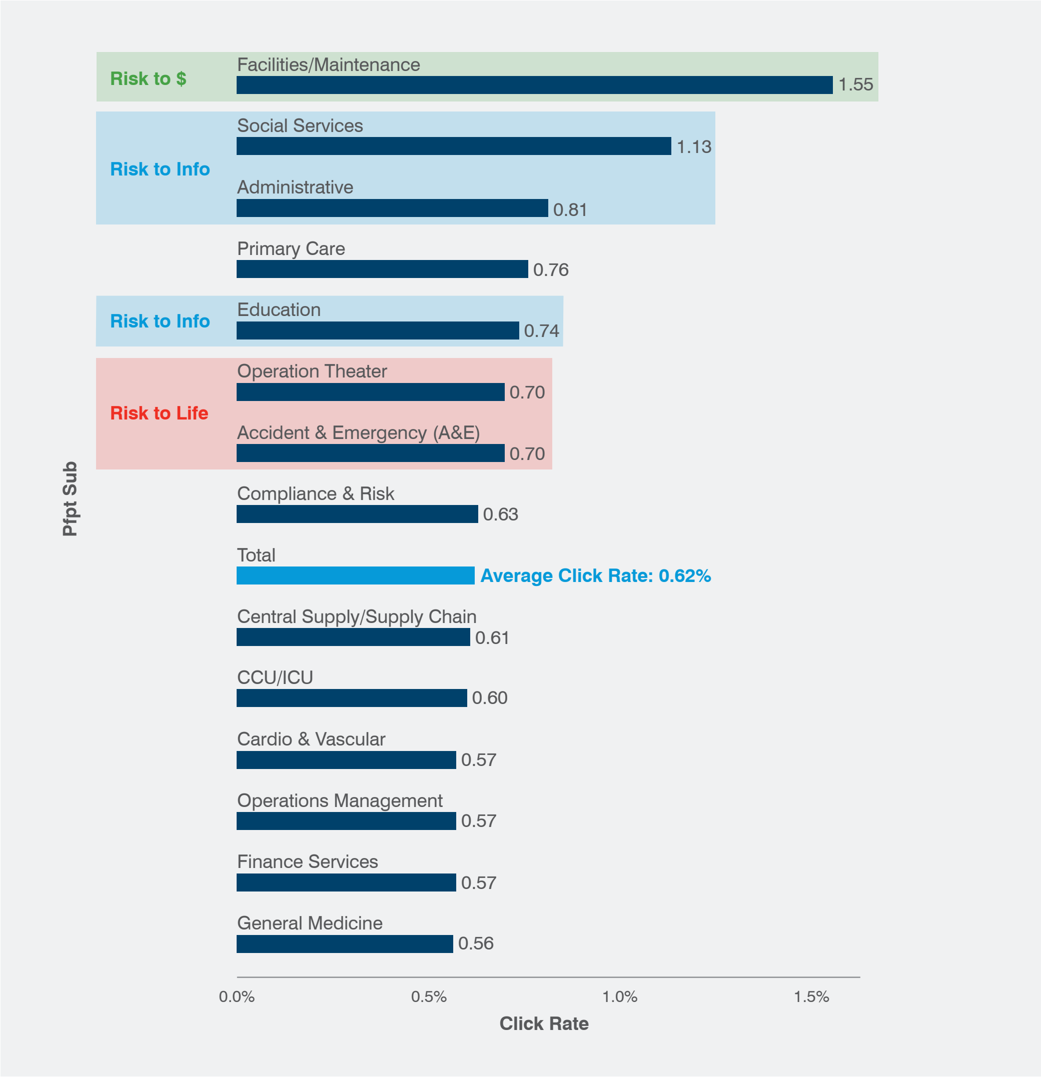

Figure 4. Departments with highest click rates, January–December 2021.

Click rates over time

Click rates fluctuated from department to department. But generally, they rose over the course of the year—a trend so consistent that we looked further into why. One possibility: the organizations in our sample conducted security awareness training early in the year. But as the year progressed, employees grew less careful.

Figure 5 highlights these trends for selected departments. Click rates in ear, nose and throat (ENT) care swung from near zero through Q2 to nearly 1.5% in Q4. Neurology departments' click rates also jumped from near zero through Q3 to nearly 1.5% in Q4. And legal departments clicked on more than 1% of all malicious emails during the first three quarters of the year.

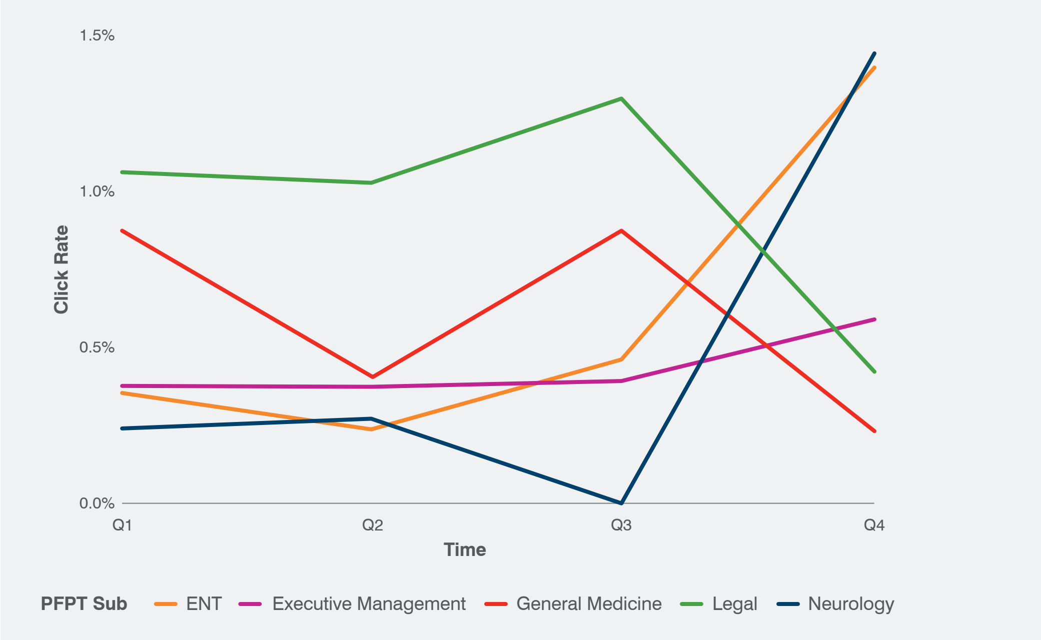

Figure 5. Departmental click rates for selected departments, January–December 2021.

Attacks by Objective: Ransomware Stabilizes, BEC Spikes

Proofpoint Targeted Attack Protection (TAP) helps reveal attackers' intent. This study looks at trends related to two specific objectives: ransomware and fraud that results in business email compromise (BEC).

Ransomware

After several years of breakneck growth, our data shows ransomware volumes stabilizing after April. Still, the healthcare enterprises in our study saw high volumes of ransomware attacks in the first quarter (Figure 7). Ransomware spiked somewhat in December, a stark reminder that this threat is by no means a thing of the past.

Our integrated, people-centric approach helps reduce the risk of ransomware attacks by layering controls by helping to:

- Prevent the initial attack
- Identifying users that are most susceptible to phishing emails
- Automating detection and response processes
- Training users to be more resilient to phishing

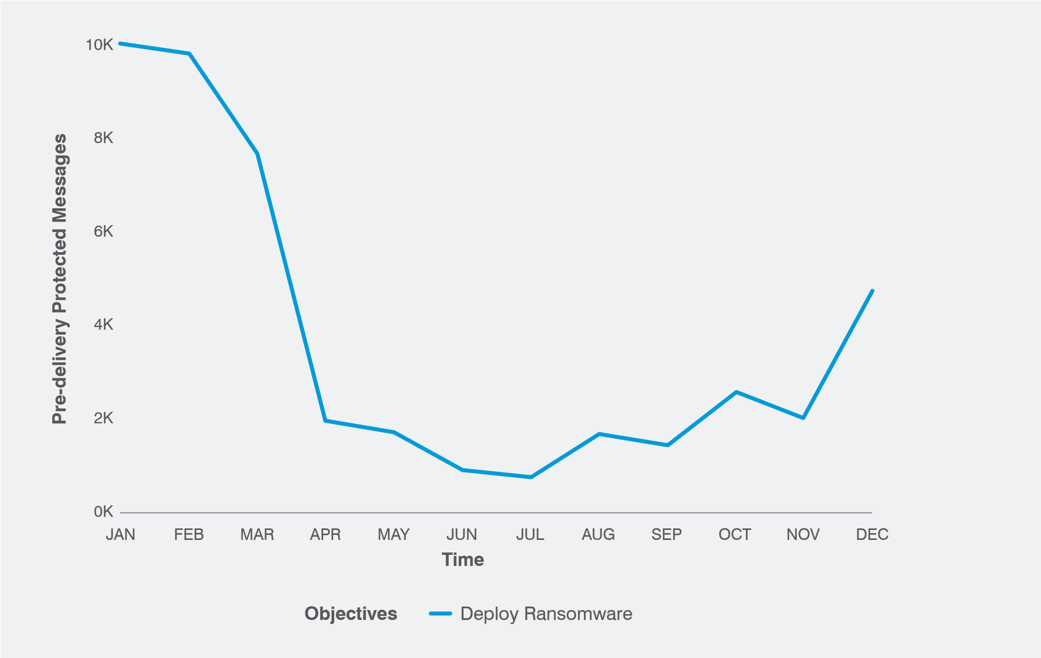

Figure 6. Pre-delivery protected messages by month, ransomware execution.

Executive fraud, BEC and social engineering

Email fraud, including BEC, is one of today's biggest and costliest cyber threats. According to the FBI, U.S. businesses paid out $2.4 billion in 2021 to resolve BEC issues, with another $278 million for similar types of fraud.[16]

Email fraud preys on human nature—fear, trust and the desire to please—to steal money and valuable information. It has hit organizations of every size, across every industry and in every geography. They're socially engineered and highly targeted. And they are especially effective at impersonation, using tactics such as spoofing to pose as trusted partners and business associates.

For healthcare, email fraud is especially harmful. It hurts the most vulnerable segment of the populace and the people dedicated to helping them. At the healthcare institutions in our sample, attempts at fraud spiked early in the year. They came roaring back in the last half of the year before returning to low levels in December (Figure 7). All signs point to email fraud persisting as a cyclical threat.

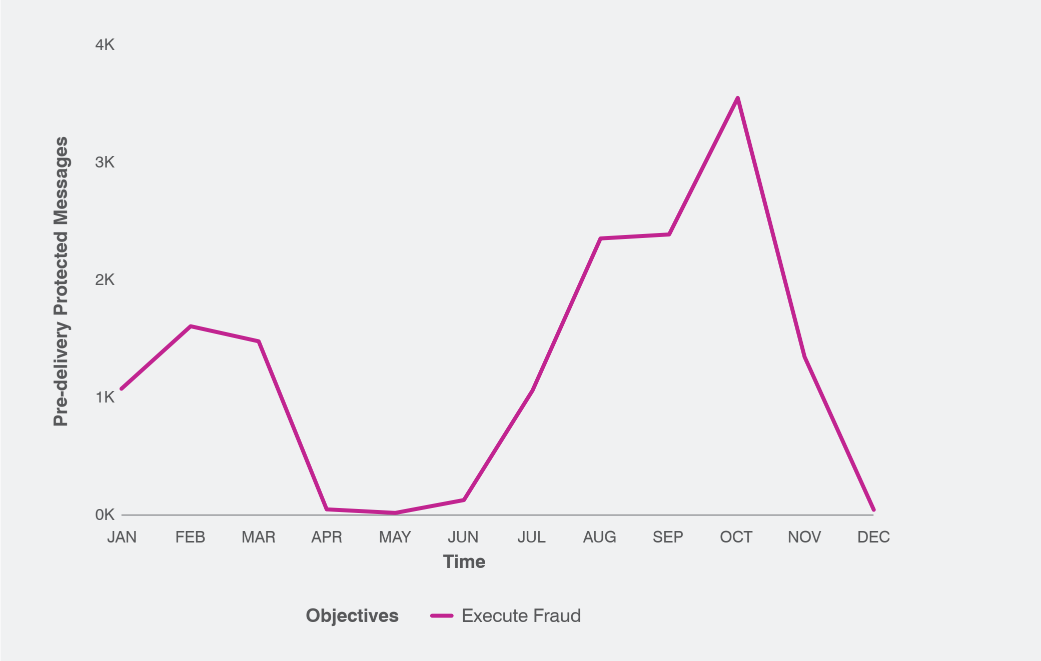

Figure 7. Pre-delivery protected messages by month, fraud execution.

[16] Federal Bureau of Investigation. "Internet Crime Report 2021." April 2022.

Conclusion

This report is designed to help you prioritize cybersecurity efforts.

The metrics in this report can fluctuate widely from one quarter to the next. But the general trend is clear: attack volumes are growing, click rates are rising and the raw number of clicks is unacceptably high. Given that a single click can result in a major breach, we must get these numbers down.

That's why 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.

No matter what type of healthcare organization you work for, Proofpoint can help. Here's what we recommend to support your security and compliance efforts:

- **Adopt a people-centered security posture.** Learn how your users are targeted, what data they have access to and whether they are prone to falling for attackers' tricks.
- **Use people-centric insight to improve your security posture.** Gain user-level visibility and insight, set strategic priorities and explain them to executives.
- **Train users to spot and report malicious email.** Help your people spot social engineering attacks such as phishing.
- **Assume that users will eventually click a link.** Spot and block inbound email threats that target users and outside threats that use your domain.
- **Use an effective email data loss prevention (DLP) solution to secure and access data.** Accurately classify sensitive and critical information. Then ensure it's accessed by the right people.
- **Build a robust business email compromise defense.** Use Domain-based Message Authentication, Reporting and Conformance (DMARC) email authentication to stop spoofed email—before it defrauds employees, clinical staff and outside business associates.
- **Protect remote staff and patients as delivery models evolve.** Use an information protection and cloud security platform to build a robust security service edge (SSE) or secure access service edge (SASE) architecture. Apply secure access and threat protection as you quickly and securely connect employees, outside business associates and patients to your data center and cloud.
- **Keep risky web content out of your environment.** Use isolation technology to assess unknown web pages and URLs in a protected container within a user's normal web browser.
- **Secure Microsoft 365 and other cloud platforms.** See cloud activity as it unfolds with a cloud access security broker (CASB). Scan and act quickly on potential cloud-based email policy violations across the continuum of care.
- **Reduce compliance risk.** Choose an archiving and compliance solution to quickly detect and mitigate insider data leaks—whether malicious or accidental—and identify and stop medical business fraud.
- **Partner with a threat intelligence vendor.** With our advanced threat intelligence, you get a solution with static and dynamic techniques to detect new attack tools, tactics and targets—and then learn from them.

The myriad of things that should and can be done to reduce cybersecurity risk is endless. But as CISOs know all too well, there is simply not enough money and bandwidth to do everything. We hope this report helps you prioritize your cybersecurity efforts to maximize the value of the investments your organization does make.

LEARN MORE

For more information, visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps 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 Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

proofpoint.