Information Protection: A People-Centric Approach to Safeguarding Healthcare Data

How cybersecurity leaders utilize context and the threat landscape to accelerate incident management

Cybersecurity has become one of the most complex and urgent issues facing the healthcare industry. The number of cyber attacks continues to grow, and attackers are getting even more sophisticated at compromising systems. For healthcare, the stakes couldn't be higher. Left unchecked, data breaches can expose patient data, disrupt business, damage trust and even harm patients.

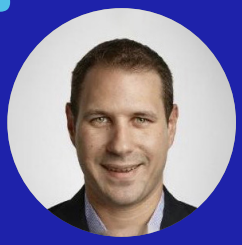
As cyber criminals evolve both their objectives and methods, safeguarding healthcare data and preventing data loss has only grown more challenging. A decade ago, the threats faced by healthcare organizations usually consisted of brute-force attempts to penetrate a hospital's on-premises network. Some might exploit newly discovered or well-known vulnerabilities in hardware and software. Others might take advantage of lax security measures. In either case, the outcome was largely certain: exposed data, payment card theft, espionage and compliance issues.

"There was always something within the internal design of a hospital's information network that bad actors wanted to exploit," said Proofpoint Industries Solutions and Strategy Leader Ryan Witt. "And they usually found it pretty easy to exploit."

That's changing. While many attacks still compromise infrastructure, most hinge on the attacker's skill at manipulating human nature. According to the *2021 HIMSS Healthcare Cybersecurity Survey*, only about 1 in 7 respondents cited legacy software as the origin of their biggest security incidents. People-related factors were a far bigger cause, including:

- Phishing (71%)
- Human error (19%)
- Social engineering (15%)[1]

Organizations have gotten better at hardening their infrastructure, and many have migrated to the cloud. The distinct network perimeter of old no longer exists – people are the new perimeter. These trends have shifted attention from traditional data loss prevention (DLP) solutions to a more people-centric approach to safeguarding sensitive data. That's especially true in widely distributed healthcare networks. The COVID-19 pandemic, which greatly increased remote work and telehealth use, has only accelerated the dynamic.



Malicious actors, whether they are internal or external threats, are no longer focused on networks or devices."

MIKE STACY | Senior Director of Enterprise Security Strategy | Proofpoint

"Every data breach study says the same thing – between 85% and 95% of all attacks are human centered," said Proofpoint Senior Director of Enterprise Security Strategy Mike Stacy. "There's no question about it. Malicious actors, whether they are internal or external threats, are no longer focused on networks or devices."

Instead, they are drawing a bead on your organization's most valuable asset – your people. And only a security strategy based on protecting those people will get to the root of the problem.

Context is king

Healthcare organizations clearly need more modern information protection. Despite increases in spending, 67% of respondents to the HIMSS survey reported experiencing "significant security incidents" in the preceding 12 months.[1] During that same period, 600 breach incidents were reported to the U.S. Department of Health and Human Services. The 10 largest of these breaches impacted the health or financial information of more than 1 million patients each.[2]

Traditional data loss prevention follows the data – data in use, data in motion and data at rest. The challenge has been to understand the contexts in which data is being accessed. Under what conditions is remote access to a database legitimate or suspicious? When is transferring files through email acceptable collaboration? When is it an unacceptable risk? Context counts.

"The philosophy we need to adopt is protecting people and defending our data," said Proofpoint Senior Director for Cybersecurity Strategy Brian Reed. "And what I mean by 'defending our data' cannot include shutting down the conversion of data as a raw material and contextualizing it and making it useful as information. Instead, it requires understanding the process of converting data to information and protecting it every step along the way."

In other words, those charged with healthcare information security must move beyond the binary decision of allowing or blocking based solely upon the contents of data. According to Reed, moving from this technology-centric control to a people-centric approach is "the biggest mind shift" in information security today.

"It's about making sure that you understand all the decisions people are making with data," he said. "What's the normal business or organizational context that somebody has for opening this file, sharing this information or utilizing the specific application? Once you understand the interactions that people have with data, you can then focus on understanding advanced use cases."

Know your 'Very Attacked People'

Contextual decision-making of the kind Reed envisions depends on better intel about the entire cast of characters involved in cyber attacks. It's knowing the perpetrators, the defenders and the victims. For example, a people-centric approach requires making distinctions not merely between external actors and internal actors, but *within* those categories as well. Are the majority of your organization's external threats nation-states, terrorists, criminal syndicates or lone-wolf threat actors? Are your organization's targets high-profile leaders or lower-level workers? And with insider incidents up 44% in 2022,[3] do you know whether your insider threats are malicious, careless or compromised?

These distinctions need to be as granular as possible. Knowing who is trying to gain access to your data helps reveal their intentions. A Proofpoint analysis of a leading teaching hospital's email traffic showed that two-thirds of malicious activity was aimed at its research institutions. And within that activity, scientists in the genomics division were targeted two-thirds of the time. In this case, the cyber criminals weren't after financial or patient data. They wanted to steal intellectual property (IP).

In another case study, a children's hospital found that attackers focused on two distinct areas: accounts payable and users with clinical research titles. The first area was targeted for straightforward financial reasons such as invoice fraud. The second group of users was targeted to steal IP and research. The attackers were also interested in records for minor patients – since most children have yet to establish a credit history – making identity theft more likely to go unnoticed and increasing its value on the dark web.

"Whether you look at it from a cost perspective or a per-incident basis, the most expensive insider threat is when an account gets compromised."

BRIAN REED | Senior Director for Cybersecurity Strategy | Proofpoint

"These threat actors will work out who is likely to be most valuable and of interest to them," Witt said. "Make no mistake about their ability to draw these conclusions and how much time they will put into figuring these things out."

For that reason, knowing your own people is just as vital as knowing your enemies. That task is more complicated today because legitimate access to healthcare IT systems is no longer limited to your employees. With digital transformation, cloud expansion and the "Great Reshuffling" of the COVID-19 era workforce, many outsiders may also be authorized users. These include contract workers, clinicians working from remote facilities, patients accessing records from devices and vendors using OAuth-enabled applications in the cloud. Each user represents a first step into your systems.

These shifts have made account compromise and credential theft the Holy Grail of malicious actors. According to the Ponemon Institute, credential theft rose from 14% of all cyber incidents in 2020 to 18% in 2022. Meanwhile, the cost of credential theft to victims jumped 65% from $2.79 million to $4.6 million over the same time.[4]

"Whether you look at it from a cost perspective or a per-incident basis, the most expensive insider threat is when an account gets compromised," Reed said.

Anyone can be a target of a phishing expedition. But as Witt points out, "people are not treated equally by bad actors." Witt said. That's why measuring attack volume alone is not enough to identify your Very Attacked People (VAPs.) Here are three attributes that determine how users are being targeted and by whom:

- **Actor Type**. Considers the criminal's level of sophistication. For example, a state-sponsored attacker represents higher risk than a small-time cyber criminal.
- **Targeting Type.** Targeted threats usually pose a higher risk than those that cast a wider net. Did the threat hit only one user on the entire planet? Was it focused on a particular user, company, vertical or geography? Or was it a spray-and-pray campaign seen by half the globe?
- **Threat Type.** This aspect considers how dangerous the threat is and how much effort went into it. It takes into account the tools, techniques and procedures involved in the attack. For example, a remote access Trojan (RAT) or stealer is going to have a higher score than a generic consumer credential phishing email.

These VAPs represent "fewer than 10% of an organization's users," Witt said. "And there's now a lot of data that can show which departments and which job functions are most likely to be heavily attacked. Understanding who is being attacked should be a strong guide when determining where and how to put your defenses in place."

The best defense is a targeted defense

So what can healthcare organizations do to best protect people and defend data using a people-centric approach?

"I've never met with healthcare CIOs who said they were flush with money, staff, capability and technology," Witt said. "They can't apply the gold standard against every threat, so they need data to help them drive their choices and understand where it makes sense to layer in protection."

Stacy recommends starting with assessments of threat and risk vectors for your organization, and then drilling down more deeply into specific "people risks." These assessments should not be limited to the applications that people access and the sensitive data they use. They should also include users' typical behaviors in email, in cloud services and on the Web.

With these models in place – and continuously updated through an operational program – CIOs and CISOs can position their resources where they will be most effective, and pivot as needed. Necessary-but-risky behaviors can be identified and contained on demand, for example, without hurting the user experience or placing draconian restrictions on data access.

Keep safeguards in place so that you don't put users in a position where they have to make judgments."

RYAN WITT | Industries Solutions and Strategy Leader | Proofpoint

People can also be among your most valuable defenses against cyber attacks, Reed said. Ongoing security awareness training, education and testing can help employees make better decisions about whom to trust. Armed with this knowledge, they'll know how to identify suspicious email and impersonators who ask for credentials.

Finally, Stacy stressed that a people-centric approach does not replace the fundamentals of information protection but enhances it. The basic "blocking and tackling" of an effective cyber defense posture still includes tactics such as:

- Using isolation technology to keep risky web content out of your environment
- Securing Microsoft 365 and other cloud platforms with a cloud access security broker (CASB)
- Deploying an information protection and cloud security platform on a prioritization of organizational risk
- Building a robust business email compromise defense using Domain-Based Message Authentication, Reporting and Conformance (DMARC) authentication to stop spoofed email

"Ideally, you want to keep as much malicious traffic away from users as possible," Witt concluded. "Keep safeguards in place so that you don't put users in a position where they have to make judgments."

To learn more about how Proofpoint can help healthcare organizations combat advanced threats, safeguard patient data, and modernize compliance, visit proofpoint.com/healthcare.

References

1. Healthcare Information and Management Systems Society. 2021 HIMSS Healthcare Cybersecurity Survey. www.himss.org/resources/himss-healthcare-cybersecurity-survey.
2. Proofpoint. *2022 Healthcare Cyber Crime Update*. www.proofpoint.com/us/resources/white-papers/healthcare-cyber-crime-update.
3. Brian Reed, "Insider Threats Are (Still) on the Rise: 2022 Ponemon Report," *Proofpoint Blog*, January 25, 2022. www.proofpoint.com/us/blog/insider-threat-management/insider-threats-are-still-rise-2022-ponemon-report.
4. Ponemon Institute. 2022 Ponemon Institute Cost of Insider Threats Global Report. www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats.

proofpoint.

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 75 percent of the Fortune 100, 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.