Clean Bill of Health

Securing Pharmaceutical and Life Science Firms with Proofpoint

Pharmaceutical companies are facing a deluge of targeted attacks that threaten their intellectual property, data and brand. Proofpoint's people-centric approach helps protect your data, operations, and IP from today's biggest threats.

PROTECTING PEOPLE, PROCESSES AND INTELLECTUAL PROPERTY

Pharmaceutical companies have a two-pronged mission. They exist to develop safe, effective drugs that enhance the lives of people. And at the same time, they must protect their operations and intellectual property to continue that work. Succeeding on both counts can be a matter of life and death for the patients they serve—and for their own business.

For drug makers, safeguarding drug and clinical trial data, drug formularies and production processes, and intellectual property (IP) is mission-critical. But in an era of digital, global collaboration, that challenge is more complex than ever.

To bring innovations to market, companies share troves of data internally and with outside partners. That openness is an opportunity for cyber attackers to gain access to valuable information and cash in on stolen IP. Beyond the financial harm, these attacks can hurt customers and undermine their brand promise.

At the same time, drug makers are under pressure to prove that their products are effective when used as prescribed. In some cases, this leads to direct interaction with patients—the companies must ensure people are using the medications how and when they're supposed to. Safeguarding these contacts is yet another security must.

Recent targeted attacks on pharmaceutical and life sciences companies are telling. In our analysis of attacks against Fortune 500 companies, drug makers saw a 150% jump in impostor emails—one of the largest increases in any industry.[1] In 2018, attackers targeted pharmaceutical companies an average of 71 times per organization. Healthcare organizations as a whole received an average of 43 impostor emails in the first quarter of 2019.

Like organizations across a variety of industries, drug makers have invested in traditional security tools. But these tools defend only the traditional network perimeter—one that is dissolving.

"Borderless" drug research and development networks have become the norm. The old perimeter-based security model leaves people both behind and outside of those networks vulnerable. Researchers, production managers, quality control managers, patients and others are exposed to this new breed of people-focused attacks.

1 Proofpoint. "Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks." November 2018.

AN INDUSTRY UNDER ATTACK

Bringing a new prescription medicine to market is a lengthy and expensive process. According to the Tufts Center for the Study of Drug Development, developing a new prescription medicine and getting it approved costs drug makers $2.6 billion and takes at least 10 years.[2] The first company that brings a new drug to market is supposed to have exclusive rights to it. It's easy to see why the right IP would be so valuable to an attacker.

Stolen patient data is also valuable. It can be used in identity theft schemes or sold directly to cyber criminals.

It's no wonder pharmaceutical companies face such a wide range of threats.

IP theft

Stolen IP can benefit rivals—especially those beyond the reach of domestic patent laws. An unscrupulous company that steals drug-related trade secrets can rush to market with a cheaper version, undercutting the true maker. Cyber criminals can also command big sums for stolen IP on the black market.

State-sponsored attacks

Hostile governments use corporate espionage tactics to steal sensitive information, such as drug formulas, research, and strategic plans. They may bribe an insider to hand over key data. Or they may plant a spy, hired as a legitimate employee, to carry out the deed.

Insider attacks

Insider attacks are another danger. Disgruntled workers may steal IP and other confidential data. The challenge for pharmaceutical companies is how to detect and lessen the risks posed by insider attacks.

Prescription fraud scams

Scammers can obtain prescription drugs for their own use or to resell. Opioids and other highly addictive drugs are typically targets—the so-called "Oxycontin threat vector."

Social media threats

Drug makers are quickly growing their social media presence to engage and gather feedback about their products and monitor for adverse drug reactions.

This new channel also opens the door to bad actors to steal protected health information (PHI) and sensitive drug data. These attacks could result in lost revenue, a damaged brand, and stiff fines for violating the Health Insurance Portability and Accountability Act (HIPAA) and other mandates.

Account compromise

One of the most common ways attackers gain access to IP and other sensitive data is by taking over privileged accounts. This enables the attacker to traverse victims' network disguised as an insider. The technique allows them to bypass detection and monitoring tools.

Unmanaged superuser accounts can lead to loss or theft of sensitive corporate information and serve as an entry point for malware.

Hurting the Healers: The Impact of Cyber Threats on Pharmaceutical Companies

Stolen IP and patient data can have many harmful effects. These include:

- Loss of competitive advantage and market position
- HIPAA noncompliance and potential fines resulting from breaches of clinical trial results and patient data
- Damage to critical systems and business disruptions, such halting drug production
- Brand damage, which means consumers lose trust in a company's ability to protect their personal health information or keep drugs safe
- Reduced shareholder value from bad press and fines attributed to a breach
- Financial impact due to lawsuits and lost revenue

2 Thomas Sullivan (*Policy & Medicine*). "A Tough Road: Cost To Develop One New Drug Is $2.6 Billion; Approval Rate for Drugs Entering Clinical Development is Less Than 12%." March 2019.

TAKE A PEOPLE-CENTRIC APPROACH

Today's cyber attacks target people, not technology. That's why drug makers must take a people-centered approach to securing their stakeholders, users, and consumers and the data they use and share.

The pharmaceutical industry is collaborative. Its workers are duty-bound to "cure." These factors make the industry especially vulnerable to attacks that exploit human nature. And the potential payoff of successful attacks is high.

Our 2019 report, **"Protecting Patients, Providers, and Payers"** explores what we call Very Attacked People™ (VAPs) in healthcare, including life sciences/pharmaceuticals. We use the term to describe users within an organization who are the most heavily targeted by cyber threats. Figure 1 shows a real-life example.

Large pharmaceutical

In this example, public-facing email addresses and aliases are among the most targeted. They include the drugmaker's head of public relations and the PR alias, its investor relations alias, corporate marketing directors, and director of corporate giving. These emails are among the easiest to obtain, making them easy targets for attackers—even if they are not the ultimate targets.

Only one of the addresses, the company's vice president of research and development, is someone who fits the standard definition of a VIP.

HOW PROOFPOINT CAN HELP

Our people-centric approach is uniquely equipped to help you manage today's threats in all the digital channels that matter—email, the cloud, the web and social media. Our cloud-based suite protects against a wide range of attacks. We can help make users more resilient, stop attacks where they start, and block unsanctioned access to sensitive data and systems.

Proofpoint Email Protection

Proofpoint Email Protection is an easy-to-use, cloud-based solution for securing inbound and outbound email. It protects people, data, and brands from both common threats and new attacks while reducing inbox clutter. With Email Protection, you get granular control over impostor email, phishing, malware, spam, and bulk mail.

Proofpoint Information Protection

Identify, classify, and protect sensitive and regulated data at rest or in motion. Information Protection works across email and file storage both on premises and in the cloud. You can be sure that people who are authorized to use certain data types—and only those people—have access to it.

Encryption is automated, and policy enforcement is transparent. That means patients, researchers and anyone else can do what they need to do without security and compliance controls getting in the way. Information Protection also automates compliance by tracking electronic health records, IP, and other confidential data and files.

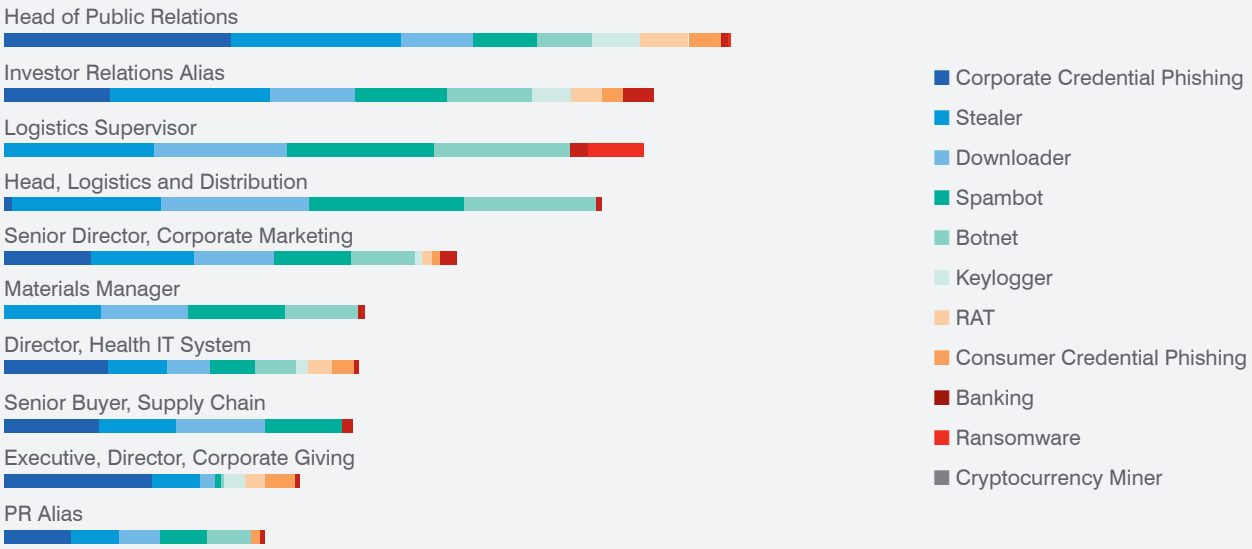

Figure 1: Breakdown of Very Attacked People at a large pharmaceutical company.

Proofpoint Security Awareness Training

Security education and awareness can turn even your most attacked people into a strong line of defense. Proofpoint Security Awareness Training provides up-to-date and relevant real-world phishing simulations to help assess which users are vulnerable, and how.

Education modules help people become better informed about emerging threats. You can monitor and track user progress over time to help them improve.

Proofpoint Digital Risk Protection

Proofpoint Digital Risk Protection monitors social media environments for posts and comments with high-risk content. It highlights adverse drug reactions (ADRs), deceptive advertising, off-label information, fake social media accounts, and more. Based on the content type, companies can decide whether to log, notify, hide, or delete it.

With Digital Risk Protection, you can protect your brand, prevent account takeovers, safeguard patients, and avoid costly social media phishing scams.

Proofpoint Cloud Account Defense

To prevent account compromise, you need a privileged account management solution. This provides the necessary control and oversight so superuser accounts are not misused or abused.

Cloud Account Defense protects Microsoft Office 365 users from account compromise and takeovers. With Cloud Account Defense, you can detect, investigate and defend against cyber criminals accessing your sensitive data and trusted accounts.

LEARN MORE

Learn more about how we can help you take a people-centric approach to protecting your data, operations, and IP at **proofpoint.com/us/solutions/healthcare-information-security.**

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity 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.

0201-006-01-01 01/20