Booz | Allen | Hamilton

Commercial Solutions

BUSINESS INSIGHTS

5 Facts about Cyber Security for Pharmaceutical Companies

An overview of cyber security issues impacting the pharmaceutical industry, and what you can do to prepare and protect your company.

Most pharmaceutical companies agree that the losses from a cyber attack could be staggering. Consequences ranging from stolen IP, repeating clinical trials, litigation, and lost revenue resonate throughout an organization. Although the pharmaceutical industry is lagging behind other industries when it comes to cyber security implementation, there's a new sense of urgency. Because of the impact to share prices and brand image, boards of directors have taken note. As data sharing becomes more prevalent across the industry, companies are starting to grasp that a breach in their network—that subsequently spreads to others—could have significant reputational impact.

Pharmaceutical companies must understand the risks and vulnerabilities within their firms as well as third party exposure. In this Business Insight, Booz Allen Hamilton Senior Lead Technologist Lou Klubenspies discusses today's most important cyber security issues facing the pharmaceutical industry and how to address them.

1. Cyber Attacks Are Already Here

The history of cyber attacks is clear: if individuals or companies have anything of value, they will be targeted by malicious parties. Pharmaceutical companies are a prime target given the importance and prevalence of the intellectual property they possess. In fact, healthcare companies are now a greater target for cyber attacks than companies in the retail industry.[1] In the pharmaceutical space, the reality is that the attacks have already occurred, resulting in the exfiltration of sensitive data, including compound information and clinical trial data. Companies engaged in merger and acquisition activities have experienced attacks in which insider information was misused to trade their stock for profit in advance of a merger being announced publicly. Waiting for warning signs to prompt your development of a comprehensive cyber security program? You're already behind.

2. Attack Vectors are Different

Knowing how attackers operate within your industry is an important step to strengthening your cyber security posture. In pharma, foreign state actors' pursuit of intellectual property remains a significant threat to these companies. These adversaries are attempting to exfiltrate sensitive data, often times by seeking to "turn" an insider, or sometimes planting an individual within the company, in hopes that the individual will aid in locating valuable data. Disgruntled employees and those facing layoffs are also a substantial threat. The way the crown jewels will be stolen from a pharma company is much different than for a retailer or a bank. In the pharma industry, adversaries are in it for the long haul. They continuously attempt to take data out of companies, mining for IP that can help them identify compounds to develop drugs and give them an edge in their respective countries.

3. Start with Data Classification

You know that adversaries are looking for your most valuable and sensitive data like formulas and compounds. To protect it, you must first be able to identify it, both at rest and in transit. Data classification is a foundational protection capability for pharmaceutical companies that enables you to enumerate and label what is marked sensitive so that you are alerted to who's accessing it and where it's being sent. Undertaking the work to implement data classification provides immediate benefits, because protection is then automated. But classification is more than simply a data labeling task; it requires an understanding of critical applications that are associated with the data, so that layered protection can be provided at both the application and the data levels. This is particularly important with unstructured data, which often finds its way onto sharing and collaboration sites – a likely conduit for insiders to exfiltrate data without being tracked.

1. Hannah Kuchler. "Cyber attackers 'target healthcare and pharma companies'," Financial Times, May 28 2014. (http://www.ft.com/intl/cms/s/0/a6b09006-e5c9-11e3-aeef-00144feabdc0.html#axzz3phYoQH87)

Understand the risks, and stay ahead of the game.

4. Mitigate Insider Threats with Privileged Account Management

The likelihood of insider attacks to pharmaceutical companies is real. The challenge is in detecting and mitigating the risks posed by an insider attack. External attackers know that if they can compromise privileged account credentials, they can traverse your network while appearing as insiders, potentially bypassing existing detection and monitoring solutions. In response, privileged account management solutions provide the necessary control and oversight so that "superuser" accounts are not misused or abused. Unmanaged superuser accounts can lead to loss or theft of sensitive corporate information, or serve as an entry point for malware that can quickly compromise a network. Privileged account management can also aid in closing back doors for administrators and superusers as well as providing robust audit trails. In the past, superusers could erase their own tracks to remove the evidence of wrongdoing, but the implementation of a privileged account management solution can provide a solid first level of defense against insider threats.

5. Unite Your Cyber Protection

Lines of business in pharmaceutical companies are vastly different, but cyber protection shouldn't be. It may be the job of a CISO to develop security processes and protocols to protect the firm from cyber attacks, but threat awareness is everyone's job. Designating security ambassadors for each line of business can help deliver your company's risk management message throughout the business. One way of looking at this approach is as a shift of the security awareness paradigm from centralized to decentralized. This effectively moves organizations from a state of hoping policies and procedures get followed, to a state of making security a part of daily work processes. These types of "peer catalyst" programs also help the ambassadors serve as the eyes and ears of corporate to help them improve change management, provide bi-directional communication, refine messaging, identify targeted training needs, and overcome organizational inefficiency, without having to reorganize the company.

In summary

The future state of cyber security for pharmaceutical companies is having an integrated security operations center where company data is classified, enriched with physical access controls, and the company is alerted to anomalous behavior through the use of analytics. Companies will also have an incident response plan that is made more effective by these improved detection efforts.

Today, however, pharma's first challenge is understanding all its threat vectors. Once understood, privileged account management, data classification, and anomalous behavior detection will help companies prevent data exfiltration. Building from this foundation will enable pharma companies to reach a more secure and mature future state. Adopting a strong frontline defensive posture, with an understanding and classification of your critical assets, strong credential management, and baseline behavior profiles for detecting anomalous network behavior, will put your future-state security operations center that much farther ahead of the game.

To learn how Booz Allen Hamilton can help your business thrive, contact:

Lou Klubenspies
Senior Lead Technologist
klubenspiesIII_louis@bah.com
Tel +1 609-578-7281

Heath Stockton
Global Account Development
stockton_heath@bah.com
Tel +1 571-420-0187

www.boozallen.com/commercial

Booz | Allen | Hamilton