Five Ways Security Operations is Ending Cyber Risk for Medical and Biopharmaceutical Organizations

ARCTIC WOLF | BIOPHARMA DIVE

Custom content for Arctic Wolf by studioID

INTRODUCTION

Healthcare organizations are under constant attack from cybercriminals. The situation has only worsened during COVID-19, as healthcare professionals contend with the dual stresses of dealing with a worldwide pandemic while simultaneously transitioning to the new WFH world.

Over the past year, cyberattacks against the healthcare and biopharma industries have been launched by a variety of bad actors, from Russian hackers trying to steal coronavirus research from American, British and Canadian biopharmaceutical companies,[1] to cyber-criminals using ransomware attacks to extort millions from hospitals and university medical centers.[2]

With many of the most egregious attacks making national and international headlines, healthcare organizations are cognizant of the dangers they face. Recent surveys point to a heightened awareness throughout the industry, as companies pour increasing amounts of money and resources into the latest cybersecurity tools. At its current rate of growth — around 7% every year — the global security market is projected to climb to $270 billion by 2026.[3] According to a recent Deloitte survey, more than half of surveyed organizations plan to increase their security spend in the face of the ongoing pandemic.[4]

But despite a heightened awareness within the healthcare industry and a proliferation of security tools, hackers still manage to inflict damage. The financial impact of these attacks is devastating, with the average total cost of a data breach in the U.S. growing from $3.54 million in 2006 to $8.19 million in 2019.[5]

How do healthcare organizations protect themselves from these attacks, especially at a time when COVID-19 is already placing additional stresses on workers and their companies? The answer: security operations — a combination of cybersecurity tools and professionals that ensures broad visibility into every aspect of a company's data and devices.

Here are five challenges facing the healthcare industry during the pandemic — and how security operations helps companies meet them head-on.

01

AN EVER-EXPANDING ATTACK SURFACE BROUGHT ON BY THE SHIFT TO REMOTE WORK

The abrupt shift to remote work brought on by COVID-19 has drastically expanded the attack surface at every healthcare organization. Instead of merely concerning themselves with what happens on the work computers within the four walls of their hospital or lab, companies must now contend with staffers using employee-owned laptops, phones, tablets and home computers in every conceivable location. The move to remote work has also blurred lines between office and home, expanding the online "work day" to an all-day, all-night affair.

The expanded attack surface means more opportunities for hackers to install malware and infiltrate a company's network, as well as the ability to steal steal patient records and raid a company's IP. Many hackers already have. According to Microsoft, by April 2020, coronavirus-themed cyberattacks had been confirmed in every country in the world.[6] With these factors in mind, how do healthcare workers — and the IT professionals responsible for monitoring them — stay vigilant about cybersecurity 24/7?

THE SECURITY OPERATIONS SOLUTION:

The fact is, few hospital security teams can monitor these sorts of threats around the clock, or even have the visibility necessary to catch cyberattacks the moment they happen. Only security operations — the right combination of tools and security professionals — can monitor today's companies around the clock, working with your own technology to look at billions of daily security events to eliminate blind spots.

02

A FASCINATION WITH THE LATEST TOOLS — WITHOUT THE EXPERTISE TO MANAGE THEM

CEOs and IT professionals alike are always looking for the next big thing in cybersecurity tools. But purchasing the latest gadget is rarely a be-all and end-all solution. "I can buy the latest and greatest firewall or an add-on to my Cisco platform and they demo really well," says Sam McLane, chief technology services officer of Arctic Wolf. "It's not until you've got them implemented where you're like, 'I've gotta hire two more people and send them to training.'"

Indeed, having too many tools, particularly without the professionals to manage them, can be even worse than not having enough tools. According to IBM's annual Cyber Resilient Organization Report, companies that use more than 50 cybersecurity tools scored 8% lower in their ability to mitigate threats and 7% lower in their defensive capabilities, compared to enterprises employing fewer toolsets.[7]

Even if your system is running optimally now, companies — and the people who work there — constantly change. Consider the irreplaceable IT expert who set up your cybersecurity system two years ago. "If that person were to leave, do you have the personnel and plan to deal with that?" says McLane. "There's such a shortage of talented personnel, people are saying, 'hey, I bought this tool, but I really don't know how to use it effectively.'" And cybersecurity professionals agree: No tool is perfect. "If you could find a magic bullet out there that was one hundred percent effective," says McLane, "we'd all be out of business except for that company."

THE SECURITY OPERATIONS SOLUTION:
No matter what it promises, no single cybersecurity tool can do it all. Security operations melds a combination of tools with a Concierge Security Team (CST) able to provide 24/7 coverage. Working alongside a company's internal team, the CST oversees every aspect of monitoring, detection and response, while reducing or eliminating the alert fatigue many healthcare IT experts are currently experiencing.

THE SHORTAGE OF QUALIFIED SECURITY PROFESSIONALS

Most companies simply can't afford to hire a dedicated security team capable of providing 24/7 cybersecurity. According to the Ponemon Institute, a typical company spends nearly $3 million a year on an in-house security team, a sum out of reach for most organizations in the healthcare industry.[8] Even if they could afford it, a worldwide shortage of qualified security professionals makes this difficult at best.

Unfortunately, there's no end to the deficit in sight. According to the most recent Cybersecurity Workforce Study, more than four million new cybersecurity workers are currently needed to meet global demand; in the U.S. alone, the cybersecurity workforce gap is nearly 500,000.[9]

Given the overwhelming need for workers and the sensitive nature of the field, turnover is a major issue with in-house security teams, particularly the ones with the most talented and technologically savvy specialists. As McClane explains, "They get everything up and running, and then suddenly they're like, 'OK, what's next? I'm just answering compliance questionnaires and babysitting a system.' And they get bored."

THE SECURITY OPERATIONS SOLUTION:

With security operations, there's no longer the need for companies to try to hire and retain qualified cybersecurity professionals. They work in challenging and innovative environments, where they're given access to the latest research on threats and intel feeds and constant opportunities for training and professional development. The result: teams that are inspired, motivated and up to date on the latest cybersecurity challenges.

THE WEAK CYBERSECURITY LINK IN ANY HEALTHCARE ORGANIZATION: PEOPLE

When it comes to cyberattacks, people are the weak link. Healthcare companies are no different. And with the rise in telehealth and the ongoing shift to remote work, human error continues to be a major security concern. Whether the attacks are opportunistic or targeted, phishing scams or massive data breaches, human beings remain the weak link in any company's cybersecurity chain.

At the most recent CyberMed Summit, experts discussed various reasons why doctors are particularly susceptible to cyberattacks, including a tendency to prioritize patient care over cybersecurity and the huge difference in how doctors and cybersecurity experts assess "risk".[10] "Doctors are highly trained medical professionals and when they're trying to remember passwords and deal with phishing scams, typically they're like, 'someone else does that for me'," says McLane. "And so they make great targets."

THE SECURITY OPERATIONS SOLUTION:

Even the most capable in-house IT team can't keep its people from making simple human mistakes. Managed Detection and Response ensures that when mistakes happen or cyberattacks occur, systems are in place to react, respond and recover 24/7.

Look for a security operations partner who can detect and respond to threats within minutes of infection. The key? Total visibility and an ability to filter out all that cyber noise. "We know what to look for and we know what's important," says McLane. "So we're able to say that within five minutes, we're going to give you a call. And we live up to that standard."

ATTACKS ARE BECOMING MORE FREQUENT — AND MORE SOPHISTICATED

According to a recent FBI report, phishing scams were the most common internet crime reported by victims in 2019.[11] As tools on the Dark Web become increasingly sophisticated, hackers are able to create everything from credential pages and corporate branding to company emails that are indistinguishable from the real thing. The rise in the number and complexity of attacks has led to more false-positive alerts — and correspondingly high levels of alert fatigue. According to a study by the Cloud Security Alliance, 31.9% of respondents ignore alerts due to false positives.[12]

The result of this rise in attacks? Compromised patient records, lost work days, lawsuits and hospitals held for ransom. In worst-case scenarios, doctors lose access to vital patient records, and are unable to safely administer drugs or care. In September 2020, a female patient in Germany died after a ransomware attack disrupted emergency care at a university hospital, the first time a patient's death has been directly linked to a cyberattack.[13]

THE SECURITY OPERATIONS SOLUTION:

As cybercriminals become increasingly sophisticated, security operations provides awareness training for employees that is effective and ongoing. "In place of hour-long PowerPoint presentations," says McLane, "there's been a shift towards microlearning, 'in-the-moment' training that immediately responds to what the user is doing. A user clicks on a bad link, for example, and gets a quick note about what they've done and how to avoid making the same mistake in the future."

The goal for security operations is continuous improvement, where it's not just what a company and its people are doing now, but what they need to be doing six months down the road.

To that end, quarterly reviews are key. "Do we have visibility into all of the company's tools and programs?," McLane says. "Is everything configured properly? How can we get better control of administrative accounts or tighten security of Office 365?"

With security operations, every aspect of a company's security is examined, from people to processes. Over time, a company's cybersecurity becomes stronger and more resilient and better able to detect and withstand future attacks.

CONCLUSION

/// Healthcare and biopharmaceutical organizations are under increasing attack because of COVID-19 and the ongoing shift to remote work — and there's no end in sight.

Security operations, with its 24/7 coverage and emphasis on both tools and technical expertise, is the most effective and cost-efficient way for those in the healthcare space to meet today's cybersecurity challenges head-on.

SOURCES

1 "Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say," *The New York Times*, August 11, 2020. www.nytimes.com

2 "Ransomware Attack on Colorado Hospital Highlights Fears of More Healthcare Hostage Situations," *TechRepublic*, May 4, 2020. www.techrepublic.com

3 "2020 Roundup of Cybersecurity Forecasts and Market Estimates," *Forbes*, April 5, 2020. www.forbes.com

4 "Attack Worries Increase as Pandemic Continues," *Security Boulevard*, June 25, 2020. securityboulevard.com

5 "2020 Roundup of Cybersecurity Forecasts and Market Estimates," *Forbes*, April 5, 2020. www.forbes.com

6 "Hackers Have Hit Every Country on Earth with Coronavirus-themed Cyberattacks," *Business Insider*, April 8, 2020. www.businessinsider.com

7 "IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue," *IBM News Room*, June 30, 2020. newsroom.ibm.com

8 "How Effective are Security Operations Centers?," *Security Boulevard*, April 14, 2020. securityboulevard.com

9 "Cybersecurity Workforce Shortage Continues to Grow," *CPO Magazine*, November 15, 2019. www.cpomagazine.com/

10 "Why is the Healthcare Industry Still So Bad at Cybersecurity?," *Ars Technica*, February 9, 2020. arstechnica.com/

11 "Hackers are Getting Better at Tricking People into Handing Over Passwords — Here's What to Look out For, According to Experts," *Business Insider*, July 18, 2020. www.businessinsider.com

12 "How to Avoid Cyber Alert Fatigue: Tips From Infosec Pros," *Digital Guardian*, July 17, 2020. digitalguardian.com

13 "A Patient Has Died After Ransomware Hackers Hit a German Hospital," *MIT Technology Review*, September 18, 2020. www.technologyreview.com

ARCTIC WOLF

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we provide security operations as a concierge service. Highly-trained Concierge Security® experts work as an extension of your team to provide 24x7 monitoring, detection and response, as well as ongoing risk management to proactively protect systems and data while continually strengthening your security posture. Learn more at arcticwolf.com.

LEARN MORE

studio / ID

BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

LEARN MORE