Clearwater

How to Mitigate Gaps in Your Front-Line of Cyber Defense

Clearwater's Steve Akers on Unique Issues for Small to Midsize Health Entities

ISMG
INFORMATION SECURITY
MEDIA GROUP

Steve Akers

Akers has over 25 years of experience in cybersecurity and compliance and more than 15 years of experience in security and consulting services. He is the founder and former CTO of Change Dynamix, a security and behavioral analytics platform, and he has served in leadership roles for Alert Logic, TruArx Inc. and Netex Inc.

The threat landscape has evolved significantly in the past year or so – particularly for small to midsize healthcare entities. **Steve Akers** of Clearwater said these organizations are particularly vulnerable because their first-line cyber defenders are their highest risk variable.

In this video interview with Information Security Media Group, Akers discussed:

- Unique security risks for small and midsize healthcare organizations;
- Why "interesting enough" is now a huge staffing factor;
- Alternative security models offered by managed security service providers.

Healthcare: A Target-Rich Environment

TOM FIELD: How has the threat landscape evolved most in the past year or so, particularly for small to midsize healthcare entities?

STEVE AKERS: In cybersecurity, many things change in a year. There is a focus on sophistication and AI-influenced thought. Two years ago, most people could spot a malicious email. But today they're so good, well-written

and contextual that it's harder and harder to tell the difference. Sometimes, a bad actor's content is better and more believable than content that somebody would subscribe to.

Cyberthreats are not slowing down, and healthcare is one of the most target-rich environments – tens of millions of records this year. Clearwater is tracking over 110 threat actors specifically targeting healthcare with no discrimination for size or sector of the healthcare industry or third party or supply chain supporting the industry. This is not just a problem for big health systems. As in every industry, more technological advancements can mean better service and patient outcomes, but they also mean you have more exposure and risk.

Cyber Defense: A Critical Function

FIELD: Why do you believe that cyber defenders are the highest-risk variable in a security and compliance program?

AKERS: We've all heard the David and Goliath story. What about David versus 100 or 1,000 Goliaths that never sleep and are powered by advanced AIs and backed by nation-states? Many believe the challenge is: Who in your organization is David?

But we need to grow beyond thinking of this as a person and think of it more as a critical function that's staffed and equipped appropriately.

That story is what all organizations are facing, but it's particularly impactful for small to midsize health entities. They don't have the resources to do this themselves, and often they struggle to attract resources while being forced to pay A-list compensation for not-A-list talent. And for those that are fortunate enough to find the top talent, can those people work 24/7, weekends, holidays? What if they get sick? Of course, they can't, right? That's just not feasible.

Cybersecurity is one of the largest gaps in the jobs available relative to the small number of resources there are to fill them. It's hyper-competitive, which makes cyber defenders one of the high-risk variables in any program. One of our clients recently told us that they found it difficult to attract the right talent because they simply were "not interesting enough."

'Not Interesting Enough'

FIELD: Why is "not interesting enough" such a huge staffing factor now?

"We need to grow beyond thinking of cyber defense as a person and think of it more as a critical function that's staffed and equipped appropriately."

AKERS: Cybersecurity resources are in high demand. For that reason, people want what they feel are the best jobs relative to growth and exposure to technologies. They want something that they feel excited about every day. Unfortunately, that often yields high turnover. What once seemed like the best job for somebody has grown static, and they feel like maybe they've stagnated in the role. Or maybe it's the other extreme, where there are so many things happening that the employee can't handle what's going on, which means that they can't grow or progress in the things that they find most interesting about their career. So, they leave, which then leaves the organization without a critical resource.

Partnering With an MSSP

FIELD: What alternative models should small to midsize health systems and hospitals consider to address this risk and overcome the challenges of finding and funding the correct resources?

AKERS: For most small to midsize entities, the two biggest risks are staff and the technical stack that they use or invest in to address the modern threat that they're facing. Unfortunately, one is not a substitute for the other. Lots of technology without a team to properly manage and engage it is going to be ineffective. A large team without the proper tools will leave that team in a constant state of reactivity. Furthermore, both scenarios also can mean those same resources are not helping the organization achieve its goals and mission, and that's what you're really striving toward.

This leaves organizations with some choices. But ultimately, the best course of action – particularly for small to midsize healthcare entities – is to partner with an MSSP that can scale up or down to meet your unique needs, has broad offerings to cover more attack services, understands the healthcare space intimately, and is versed not only in cybersecurity but compliance, because on many levels the two are intertwined. A Ponemon report this year said that when partnering with an MSSP, organizations were able to identify and contain a breach in 80% of the time it took those without an MSSP. An identification reduced the window by 16 days – so we found it 16 days sooner if an MSSP was involved. Those are material differences in the battle against cyberthreats.

"Getting help is effective, and the potential cost of not getting help from experts who do this every day – who dig to find bad actors – could be far too high."

Benefits of an MSSP

FIELD: What are some of the specific benefits that a specialized managed security service provider can bring to a midsize entity?

AKERS: Having the right MSSP can vault a healthcare entity's cybersecurity detection and protection capabilities to those of a much larger organization without the need for adding a headcount. The entity can gain much-needed visibility across their entire technical footprint, whether that be on-premises, remote, cloud, SaaS or third parties. A quality MSSP should provide services at the endpoint, servers, native cloud services and SaaS applications. And within each of those, there should be a different level of visibility.

For example, some MSSPs only focus on logs. But logs are reactionary, which means that you're missing a big footprint. Some organizations and MSSPs focus on EDR, which is great when you can install an agent, but if you can't, then you have gaps. What about things like vulnerability management, which often can be a linchpin in evaluating your overall risk or the potential impact when an attack takes place? An MSSP should be able to provide all of those services and others on a 24x7 basis and work with the healthcare entity on a response model that works for them.

Not everybody's the same. Yes, they're trying to deliver an outcome: They want to provide good patient care. But exactly what's best for them should be customized and meet their needs. No one has unlimited budgets, but ideally you want to put us in the best position to respond to you, whether it's 8:00 a.m. to 5:00 p.m. Monday through Friday or 3:00 a.m. Christmas morning. To do that, we need the best visibility and data points for context so we understand what's happening across the organization. Not all MSSPs have the same model and not all of the outcomes are the same, so make sure you do your research.

Financial Business Case for MSSPs

FIELD: Let's talk about limited budgets. Given the resources, what recommendations do you have for building the financial business case to move toward with a managed security service provider for front-line cyber defense?

AKERS: These questions can be hard because you don't want to sound alarmist, but healthcare is in a unique position in their communities – particularly regional and critical access facilities – to provide much-needed services. First and foremost, patient care is the cornerstone. A malicious actor using ransomware to shut down clinical systems or critical

services can impact the quality and availability of patient care. Nobody wants to see that. Patient care is the most important case.

The second case is that healthcare is complex. It's evolving. It's unpredictable. It's not "if," it's "when" something is going to happen. The data we discussed earlier suggests getting help is effective, and the potential cost of not getting help from experts who do this every day – who dig to find bad actors – could be far too high.

The Clearwater Approach

FIELD: How is Clearwater helping its customers mitigate their cyber defense gaps?

AKERS: Managed security services is a key part of fulfilling our commitment to be the healthcare industry's premier partner for cybersecurity, privacy and compliance. Our suite of services was designed from the ground up to provide the foundation and capabilities needed to cost-effectively detect and protect against today's modern threats and adapt to tomorrow's unknown challenges. And we want to deliver these services in alignment with compliance and regulatory standards because that's always a moving target for organizations. So, understanding both is important, and we do that really well.

Our orchestration of those services brings together contextual data, threat hunting, risk and vulnerability management, and incident response by experts in both security and healthcare on a 24/7 basis. Clearwater believes we are uniquely positioned to provide highly detailed security operations and insights for the resource-constrained healthcare industry, enabling our clients to deliver on their mission of providing safe and effective care and world-class innovation across the healthcare ecosystem.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® · CU INFO SECURITY® (Just for Credit Unions) · GOV INFO SECURITY® · HEALTHCARE INFO SECURITY®

infoRisk TODAY · CAREERS INFO SECURITY® · Data Breach TODAY (Prevention. Response. Notification.) · CyberEd.io

CIO.inc · DeviceSecurity.io · PaymentSecurity.io · FraudToday.io

CYBER THEORY · CyberEdBoard · Xtra mile LIFECYCLE MARKETING · GREYHEAD

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io