OPTUM™

Healthcare Cybersecurity: The New Strategy

Optum's Aaron Rinehart on Why It's Time for a New Approach

ISMG
INFORMATION SECURITY
MEDIA GROUP


Aaron Rinehart

Rinehart currently serves Chief Enterprise Security Architect at UnitedHealth Group and has worked and consulted in the field of Information Security and Risk Management for organizations such as the Department of Homeland Security, National Aeronautics and Space Administration and the Department of Defense. He has been a featured speaker at several media outlets and conferences, most notably the National Press Club in Washington DC, ABC News and the Huffington Post.

From ransomware to targeted social engineering attacks, the threats to healthcare entities have changed enormously. Isn't it time for healthcare's cybersecurity strategy to change, too? That's the premise of Optum's **Aaron Rinehart**.

Rinehart, the Chief Enterprise Security Architect at Optum, comes from a distinguished background in government, aerospace and defense. But he's never seen an industry with quite the urgent cybersecurity needs as healthcare.

"[I]f your credit card information is breached and disclosed publicly, you can change it. The financial institution can generate new cardholder information, disclose the breach, and you're back in business," Rinehart says. "But health information is persistent. It's out there. You can't change physical things about you that easily."

In an interview about the urgency of improving healthcare cybersecurity, Rinehart discusses:

- The industry's unique challenges;
- How to manage emerging technology risks;
- Key elements of the new healthcare security agenda.

The Healthcare Threat Landscape

TOM FIELD: First off, Aaron, how is healthcare transforming in this digital age?

AARON RINEHART: We're seeing a lot of things happen across the landscape. We're seeing customers and patients driving the patient experience. When I go to the doctor, I want to be in the driver's seat of my own healthcare. Patients and consumerization of healthcare are driving changes to technology.

FIELD: Talk to me now about the threat landscape. How do you see it evolving around healthcare's changes?

RINEHART: The more we introduce technology solutions to bring innovation around healthcare, whether it be the electronic medical records, innovations around making the hospital nurse experience more efficient, or big data platforms, the more we are expanding the reach in the attack surface possible for threat actors.

> "The more we introduce technology solutions to bring innovation around healthcare ... the more we are expanding the reach in the attack surface possible for threat actors."

The attack surface is growing and becoming more dispersed. As we disperse it out to the patient themselves, we are responsible for having to manage that from a security perspective effectively to ensure we are responsible with that patient's healthcare data.

How Healthcare Security Is Different

FIELD: Talk to me about how healthcare security is different. What do you find to be unique about the security challenges that face healthcare entities?

RINEHART: I come from a long background in government, aerospace and defense, and when I came to Optum/UnitedHealth Group, I had never encountered such a complex set of requirements and regulations to deliver secure solutions. In healthcare, PHI (Personal Health Information) data is not indicative of other types of industries and data.

In other words, if your credit card information is breached and disclosed publicly, you can change it. The financial institution can generate new cardholder information, disclose the breach, and you're back in business. But health information is persistent. It's out there. You can't change physical things about you that easily.

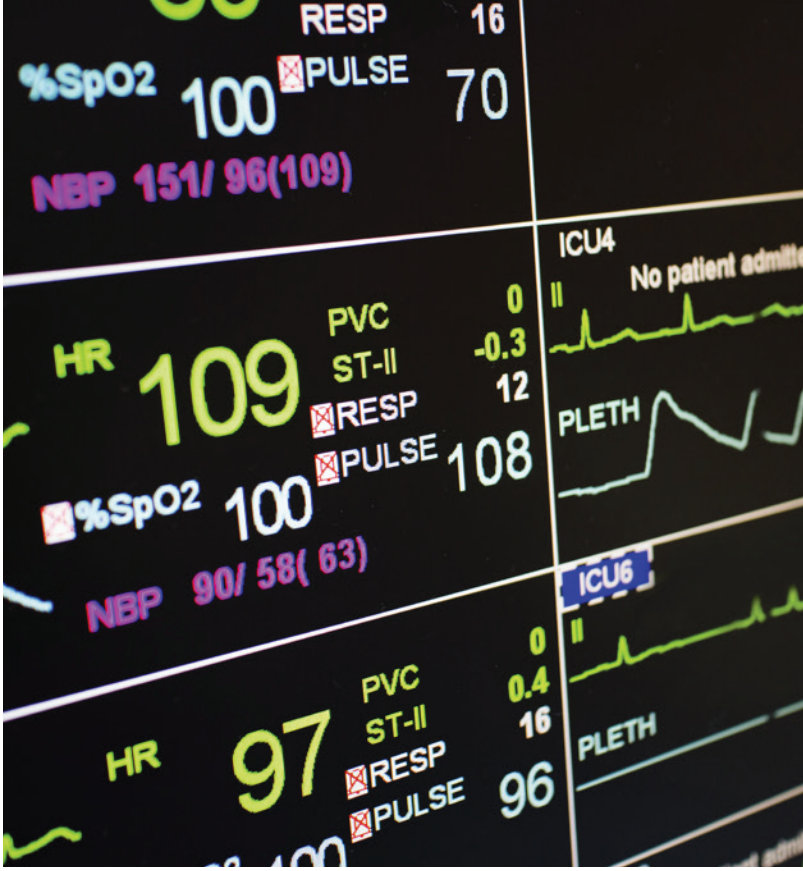
In my opinion, there's a heavier weight because of that and a greater responsibility. That's what drives us here at Optum to deliver good solutions.

The Healthcare Security Challenge

FIELD: Those are the security challenges. What do you find to be unique about healthcare's vulnerabilities?

RINEHART: From my perspective, the healthcare industry has not invested well in best practices when it comes to deploying and configuring technologies. From my experience, the vast number of vulnerabilities introduced into an organization come out of poor design, not following best practices, and poor configuration. I see this whenever I'm involved with a healthcare institution. These areas need improvement industrywide.

FIELD: Aaron, what unique challenges do technologies such as BYOD and the internet of things pose to healthcare organizations?



RINEHART: It's a growing area of focus as the proliferation of IoT devices become more connected, and more interoperable.

The organizations, institutions and corporations that are required to responsibly manage and protect health data have to be sure that they can protect that data using a distributed model. If healthcare information data is being extended out to a personal device or an employee in a healthcare institution, that institution's security controls need to extend along with it to ensure it can properly and responsibly manage that data.

Managing User Expectations

FIELD: Following up on that, how should healthcare organizations manage and respond to user expectations about these technologies? Everybody goes to work with their phone and their data and their expectations of privacy. That has to pose a challenge.

RINEHART: It does. Everybody wants it, and they want it their way now. We deliver on that by focusing on the patient and the customer value. In my opinion, spending trends should be focused on delivering on that value for the customer and being able to deliver it to their mobile, because that's where they want it. It's about the customer, the patient. It's about the value in healthcare that should be first and foremost, and we have the responsibility to deliver on that.

Emerging Threats

FIELD: What are some of the emerging threats to healthcare organizations that can have a significant impact, such as ransomware?

> "[T]he healthcare industry has not invested well in best practices when it comes to deploying and configuring technologies."

RINEHART: Ransomware is top of mind. It's been around for a long time, but threat actors have only recently started using it on healthcare organizations. That makes it more and more at the center of where we need to be focusing.

I see a couple of different trends. First, the more we extend our management ecosphere with IoT devices, we have a responsibility to protect the data being accessed. But that makes the environment more complex, and complexity is the enemy of security. We have to drive a simple model because the more complex it gets, the costlier and the less effective it gets.

I also see new threats coming from the endpoint and from the actual users themselves, whether it be the corporate folks managing the infrastructure or the patient attack surface as well.

Approaching Management About Cybersecurity

FIELD: Aaron, we hear about a lot of security leaders these days being called before management and the board to discuss cybersecurity. How do healthcare security leaders now need to approach management and the board to discuss these new vulnerabilities and get the resources they really need?

RINEHART: The best approach when approaching the board is to focus on the business value, the value that customers will derive from security as a functional quality. There should be a comprehensive risk-based assessment, but that is the kind of discussion that helps drive the organization and their customers towards a successful paradigm.

> "If you maintain the idea that you've already been breached and you're hunting and looking for attackers in your network, it causes you to take a more practical approach."

Assume You've Been Breached

FIELD: Where do you see healthcare entities struggle the most to detect intruders in their networks?

RINEHART: I like to operate under the assumption that I've already been breached. If you maintain the idea that you've already been breached and you're hunting and looking for attackers in your network, it causes you to take a more practical approach. You have to keep the model simple.

Visibility is very important because you cannot protect what you cannot see. So, there needs to be a focus on spending around visibility because it is important to know your attack surface well.

The Need for Visibility

FIELD: Aaron, let's go to the flip side now and talk about response. Where do you see healthcare entities struggle once a breach has been discovered, and it's time to respond?

RINEHART: Usually it's due to a lack of visibility into their own infrastructure; incomplete or inaccurate documentation of networks; out-of-date configurations; poor incident handling practices; and untested disaster recovery scenarios.

It's also very important that when responding, you have to be resilient to keep the business moving. You have to be able to recover. Often it's forgotten because we focus so much time and money on the actual security controls for the apparatus, but we have to remember that if we're breached, we've still got to keep the business moving, even though there may be fines or lawsuits or anything else bad that happens as a result of the breach.

Helping Healthcare Manage Security

FIELD: What key elements of the new strategic approach do healthcare organizations really need to take to proactively manage security across the entire enterprise?

RINEHART: Automation is a key element; automate all things that are possible. I see security solutions becoming more automated, decreasing the likelihood of human error and configuration changes.

Big data and machine learning are also huge trends. We have done some innovation here as a company around that, focusing on large data sets of attack information to correlate and find patterns where we couldn't before.

FIELD: That's where they need to go. How are we going to get them there? What do you find to be the core technologies and practices that are going to help healthcare organizations get to this next level of managing security across the enterprise?

RINEHART: It's funny you say that. I do believe in the tried and true, which are the industry best practices. Best practices often are not practiced across all industries, not just healthcare. Areas like management of secure configuration and good design practices.

I also see the need for continuous assessment and for building a sound risk management program. It's fun to focus on hype about new technologies and capabilities, but it's also important to make sure you have good solid fundamentals in your program because that also will help drive value for your company. ■

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 28 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.

Contact

(800) 944-0401 • sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification.

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com