KEY TAKEAWAYS
CHIME PUBLIC POLICY
CONGRESSIONAL BRIEFING

CHIME PUBLIC POLICY
WORKING FOR YOU IN WASHINGTON

Unmasking the Cyber Threats in Healthcare

CHIME's Public Policy team held a briefing on Capitol Hill on November 7, 2023, titled "Unmasking the Cyber Threats in Healthcare." Mari Savickis, CHIME's VP of Public Policy, moderated the session.

Panelists:

Nate Couture
Network AVP, Chief Information Security Officer
UVM Health Network

Erik Decker
VP/Chief Information Security Officer
Intermountain Health

Nate Lesser
VP & Chief Information Security Officer
Children's National Hospital

•

Please contact policy@chimecentral.org with any questions.

You can watch the full briefing here:
Congressional Briefing

INTRODUCTION

CHIME is a membership organization for chief information officers (CIOs) in hospitals, health systems and other healthcare settings across the country. Within CHIME is the Association for Executives in Healthcare Information Security (AEHIS), the membership arm of CHIME made up of chief information security officers (CISOs) and other healthcare security leaders.

Together our members are charged with overseeing the purchase, deployment and use of technology in a safe and secure manner. They are among the nation's foremost health IT experts on cybersecurity, privacy and the security of patient and provider data and devices connecting to their networks. Three of our members came to Washington, D.C., to share insights and educate Congressional staff on the current cybersecurity landscape in the healthcare sector. Below you will find some of the key takeaways from the briefing.

CYBER SAFETY IS PATIENT SAFETY

Threat actors have figured out that they can make money a lot quicker by disrupting business operations rather than just stealing data to resell. Disrupting business operations in the healthcare sector means disrupting patient care and the ability to save lives. There has been at least one confirmed death in the U.S. that has been attributed to ransomware and the FBI and Department of Justice (DOJ) are now calling ransomware attacks "public safety incidents." The message that the sector is trying to drive is "cyber safety is patient safety."

IN ORDER TO BEAT ONE OF US, YOU MUST BEAT ALL OF US

The Healthcare and Public Health (HPH) Sector is an incredibly complex ecosystem. Typically, when a ransomware attack occurs, it's not just a single organization that gets hit. For example, a hospital is often interconnected with other care organizations, affiliates, and vendors and any one of them can get affected and cause problems. Not one institution stands alone in this, and the only way to combat these types of threats that are facing the sector is to come together as a team. Erik Decker recalled former National Cyber Director Chris Ingils stating that "we have to establish this critical infrastructure partnership construct (i.e., The Health Sector Coordinating Council) in such a way that you have to beat all of us to beat one of us."

MORE RESOURCES ARE NEEDED AS CYBERSECURITY IS NOT CHEAP

Healthcare, more than any other sector, has an incredible disparity in terms of financial abilities which translates to information security. We need to think about how to provide better resources to raise the bar and ensure we provide some level of baseline security across the entire system.

Small, rural and under resourced health systems are scraping by on small budgets. They are focused on care delivery and not having to close their doors and force patients to now travel even further to get care. Cybersecurity is not cheap.

CHIME did a survey and 40% of the respondents said they would need help in the form of grants and other financial assistance to be able to implement a cybersecurity program to try and do their part in this equation.

THE VALUE OF HEALTHCARE RECORDS

Healthcare records are more valuable than almost any other data because they will often include personal information that is unalterable. When your credit card is stolen you can easily call the company, cancel the card, and get a new one. When your healthcare record is stolen, you can't revoke your medical history, not if you want to continue to receive care. A child's record may be even more valuable than an adult's because the theft of a child's identity is often not detected until they are 18 when they begin to do things like open a credit card or buy a car.

LESSONS LEARNED FROM A RANSOMWARE ATTACK

"On this day three years ago, we were in the middle of our recovery. At 10:44 am on October 28, 2020, applications started disappearing. It took about 15 minutes for over 1,300 servers to disappear, that's over 600 applications that our hospital depended on. I then spent 18-20 hours a day 7 days a week for the next 5 weeks to help get the hospital back. That was nothing compared to what our clinicians and their support staff were trying to do. And none of that holds a candle to the stress of the patients and families who were trying to get care at that time." - Nate Couture

UVM Health Network chose to be transparent about their 2020 ransomware attack which is not the norm. In fact, there are few incentives to do so.

One important lesson that was learned is the need to break down the silos internally and within the industries and groups. Hospitals will have emergency management practices, but they are worried about floods, hurricanes, and tornados but are not thinking about cyber. The IT staff are worried about disaster recovery and how they are going to recover systems in these types of situations. Cybersecurity folks worry about stopping and responding to threat actors. However, there is very little communication between these groups, and it's crucial that they work together in the recovery.

In addition, you have to make it about patient impact. A lot of the guidance out there isn't based on healthcare and is based on other industries and is focused on business impact assessment. That's not appropriate for the healthcare sector. "You can lose your electronic health record system. Doctors can chart on paper. You can figure out how to do the billing later, but you can't mix a chemo cocktail by eye. The priority order that you have can be totally wrong." -Nate Couture

HAVING AN ADVERSARIAL MINDSET IS KEY

We must have an adversarial mindset when thinking about protecting our critical infrastructure. Having an adversarial mindset means thinking about:

Who are the primary people trying to break in?
What are they trying to do?
What is their motivation?
What are they trying to accomplish?

The three vectors primarily used in an initial intrusion are social engineering (i.e. phishing), known exploited vulnerabilities, and a back door through a third-party vendor.

> "We need to be able to have insurance. It's one of the only tools in the tool chest we have, and we have to be able to use it."
>
> **-Nate Lesser**

CYBER INSURANCE IS A NEEDED TOOL IN THE TOOL CHEST

Cyber insurance has become less affordable for some healthcare delivery organizations. According to the Hospital Cyber Resiliency Initiative Landscape Analysis, cybersecurity premiums increased by an average of 46% in 2021.

Some companies are unwilling to take on the risk associated with catastrophic failure.

There is the need for a federal mechanism that backstops the industry so that we don't have a hospital out there on an island where they can't get insured.

It's also important to note that after a cyber incident you become uninsurable.

MINIMUM STANDARDS

20 health systems were asked "Would you welcome minimum standards?" as a part of the Hospital Cyber Resiliency Initiative Landscape Analysis and they said yes it would help. However, an incentive program would be absolutely necessary in order to achieve it.

Standards should be tied to recognized security practices such as 405(d) and the NIST CSF.

The construct to do this is the HSCC Cybersecurity Working Group which CHIME and AEHIS are active members of.

RESPONSIBLE USE OF AI

The primary way that threat actors are using generative AI is to improve their social engineering with better and more convincing messaging. It may someday get to the point where it's writing malware, but that's not where we are today.

There is a lot of risk when it comes to privacy because you have to give them a lot of information to train these models.

> "The biggest risk right now is our own usage of [generative AI] and how responsible we are versus how the threat actors use it against us."
>
> **-Nate Couture**

WORKFORCE CHALLENGES

Cybersecurity workforce challenges are massive. There are three quarters of a million openings for cybersecurity positions today in the U.S. with 1.1 million cybersecurity professionals employed today. "We are massively understaffed for the threat we are facing."
- Nate Lesser

Intermountain Health has an apprenticeship program that focuses on bringing in people without traditional backgrounds that is supported by a state grant. This could be done on a national level.

The remote revolution has been devastating for cybersecurity staffing, especially in rural areas because locally based talent has been lured away by higher paying positions.

RESOURCES

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- Hospital Resiliency Landscape Analysis
- Coordinated Healthcare Incident Response Plan (CHIRP)
- P.L. 116-321