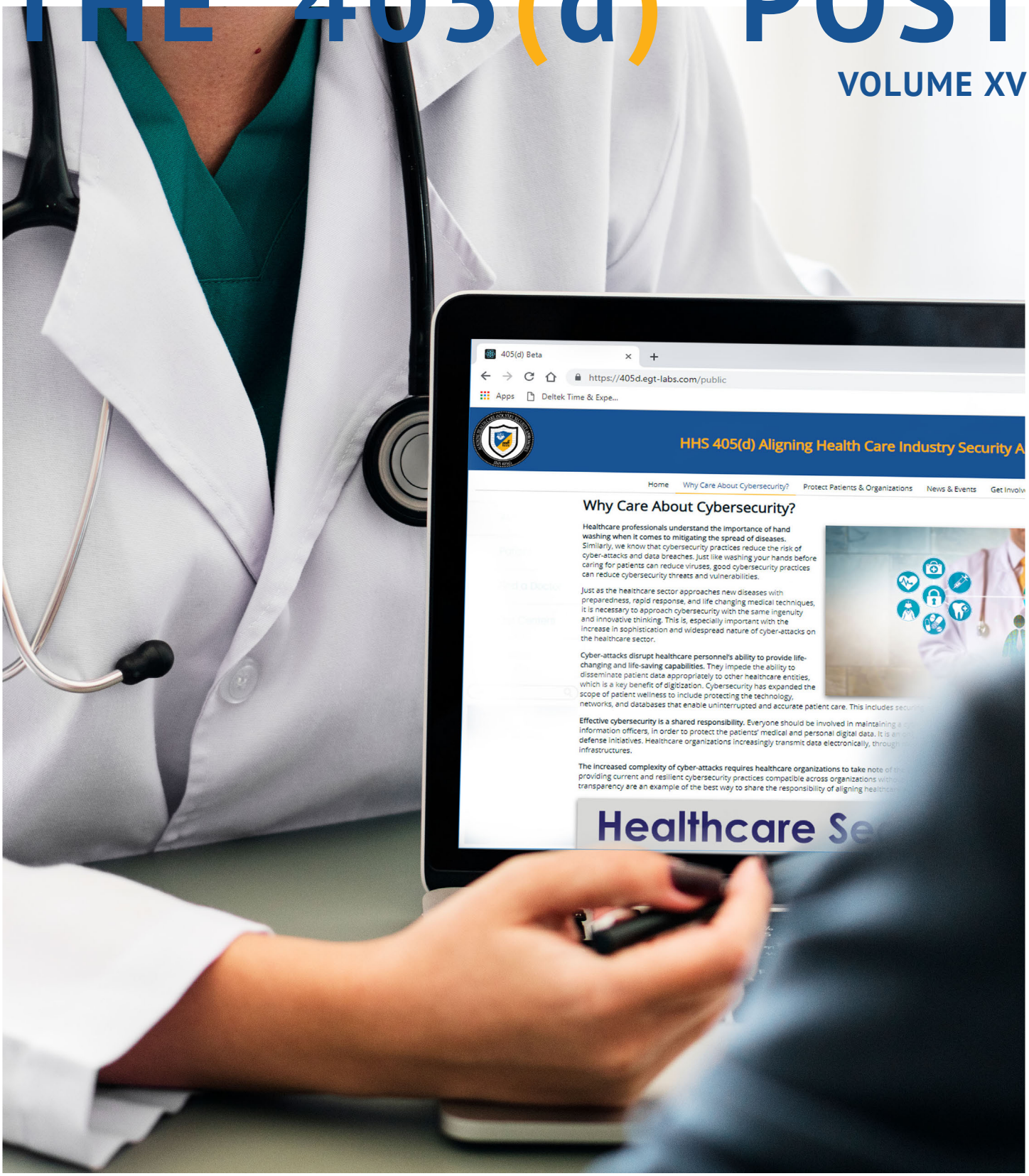
THE 405(d) POST

VOLUME XV



HHS 405(d)
Aligning Health Care Industry Security Approaches

A Word from the Task Group

The Impact of Ransomware on Healthcare

By Ed Gaudet, 405(d) Task Group member

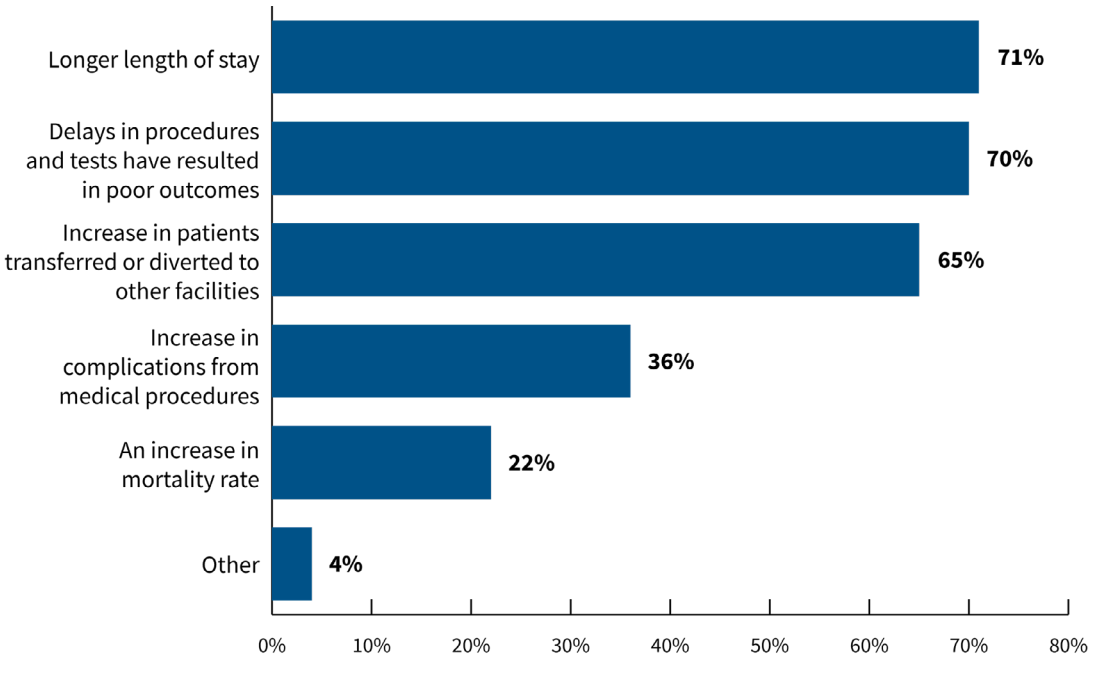
There's no denying that 2021 was a devastating year for cybersecurity attacks in healthcare. Not only did data breaches continue to increase, but ransomware attacks also upped the ante for patient safety, care delivery, and supply chain resiliency. In the last two years, we've experienced more ransomware attacks as an industry with devastating impacts. Many believe this past year has been the worst on record. In a recent article, Joshua Corman, former chief strategist of the Cybersecurity and Infrastructure Security Agency's (CISA) COVID task force, stated, "The silver lining here is sometimes you have to hit rock bottom. If we're still talking about this as fines or records and not as human life and adverse patient outcomes, then we won't bring the right tools to fix this." Like with every problem, the first step is admitting there is one. And Houston, we have a big one.

COVID-19 increased and broadened traditional cyber-attacks and introduced new risk factors to Health Delivery Organizations (HDOs), including fraudulent suppliers and equipment, remote work, new technologies, staffing challenges, and elevated patient care requirements. It is no surprise that cyber risk was announced as the top business risk in the Allianz Risk Barometer 2022 report. Experts predict that cyber-attacks and supply chain disruption will continue to increase in 2022. At the WEDI Spotlight Conference in January 2022, Corman said that "things are on fire, and we're going to need a resilient workforce to deal with these shocks on all fronts."

Last year The Ponemon Institute, the pre-eminent research center dedicated to privacy, data protection, and information security policy, researched the impacts of ransomware attacks on healthcare. The research study, The Impact of Ransomware on Healthcare During Covid-19 and Beyond, was published in September 2021 and surveyed 597 IT and IT security professionals in HDOs across the U.S. They used qualitative methodology to understand the impact of the COVID-19 pandemic on delivering patient care, and the impact cyber-attacks, like ransomware, had on protecting patient safety, data, and overall quality of care.

Unlike a data breach that exposes protected health information (PHI), ransomware locks down critical electronic systems and data within an HDO until the "ransom" is paid, rendering the ability to deliver care electronically useless. More than 40 percent of Ponemon's survey respondents said they experienced a ransomware attack within the last two years, and these attacks disrupted the ability to care for patients. As shown in Figure 1, ransomware can impact patient care in many ways.

Figure 1. What impact does ransomware have on patient care?
More than one response from the 43 percent of respondents in HDOs that had a ransomware attack.



Dr. Larry Ponemon, chairman and founder of The Ponemon Institute, said that their "findings correlated increasing cyber-attacks, especially ransomware, with negative effects on patient care, exacerbated by the impact of COVID on healthcare providers." The key findings from this study found that ransomware impacts patient care in numerous ways:

- More complications from medical procedures
- Delayed procedures and tests that resulted in poor outcomes
- Additional patients transferred or diverted to other facilities
- Longer lengths of stay

By analyzing the steps that HDOs are taking to protect patient safety, data, and care operations, we were able to distinguish what is working and what is not working. What is most concerning is that more than half of the HDOs that responded to this survey disclosed a lack of confidence surrounding risk management and cyber-attacks before and after the onset of COVID-19, as shown in Figure 2.

COVID-19 has directly impacted HDOs' ability to manage third-party risk. To mitigate patient care risks, HDOs must continue to make significant changes, such as increasing staff and routine risk assessments. In Figure 3, 63% of respondents hired additional staff, 60% demanded more risk assessments, and 50% outsourced their third-party risk management program. More than one in four admitted that remote work impacted their vendor risk management programs' effectiveness.

Figure 2. How less confident was your organization in its ability to mitigate the risks of ransomware before COVID-19, vs today?
Not confident and no confidence combined.

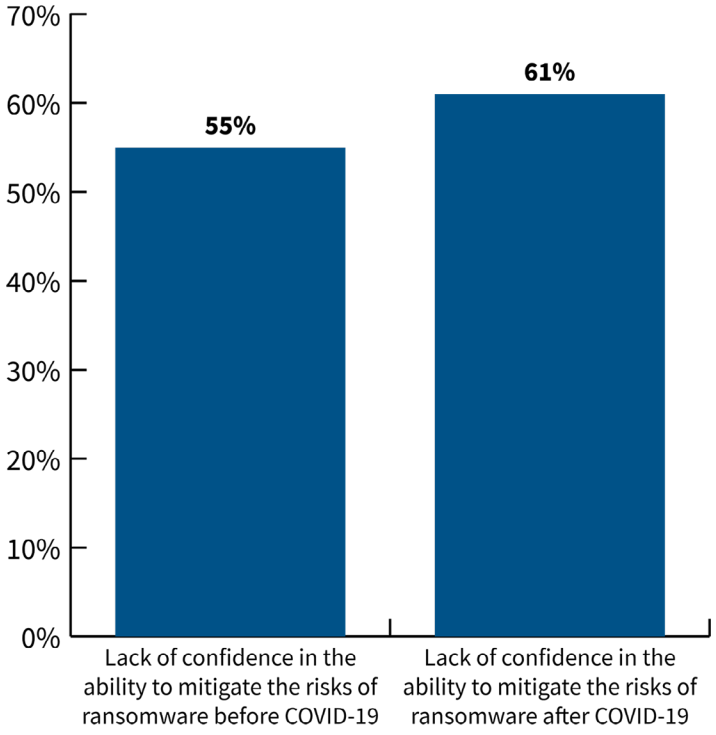


Figure 3. How organizations responded to COVID-19 and the third-party risk
More than one response permitted

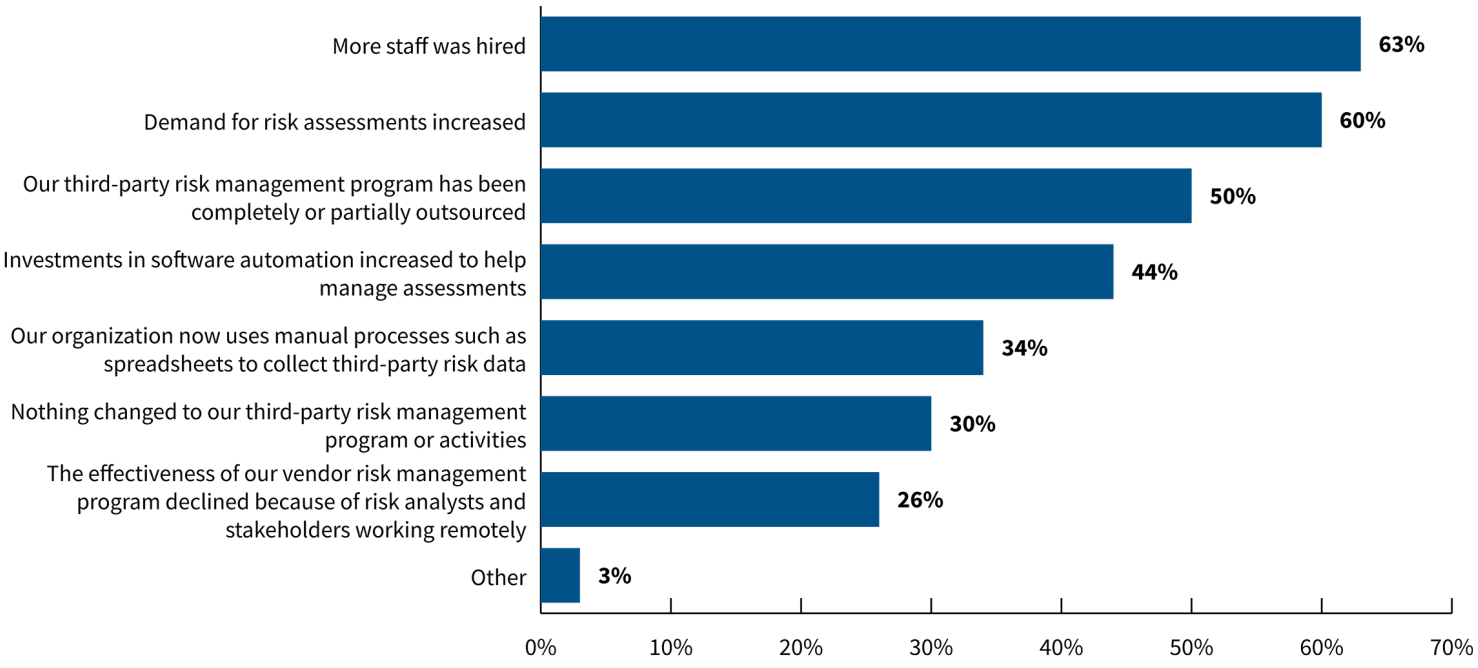
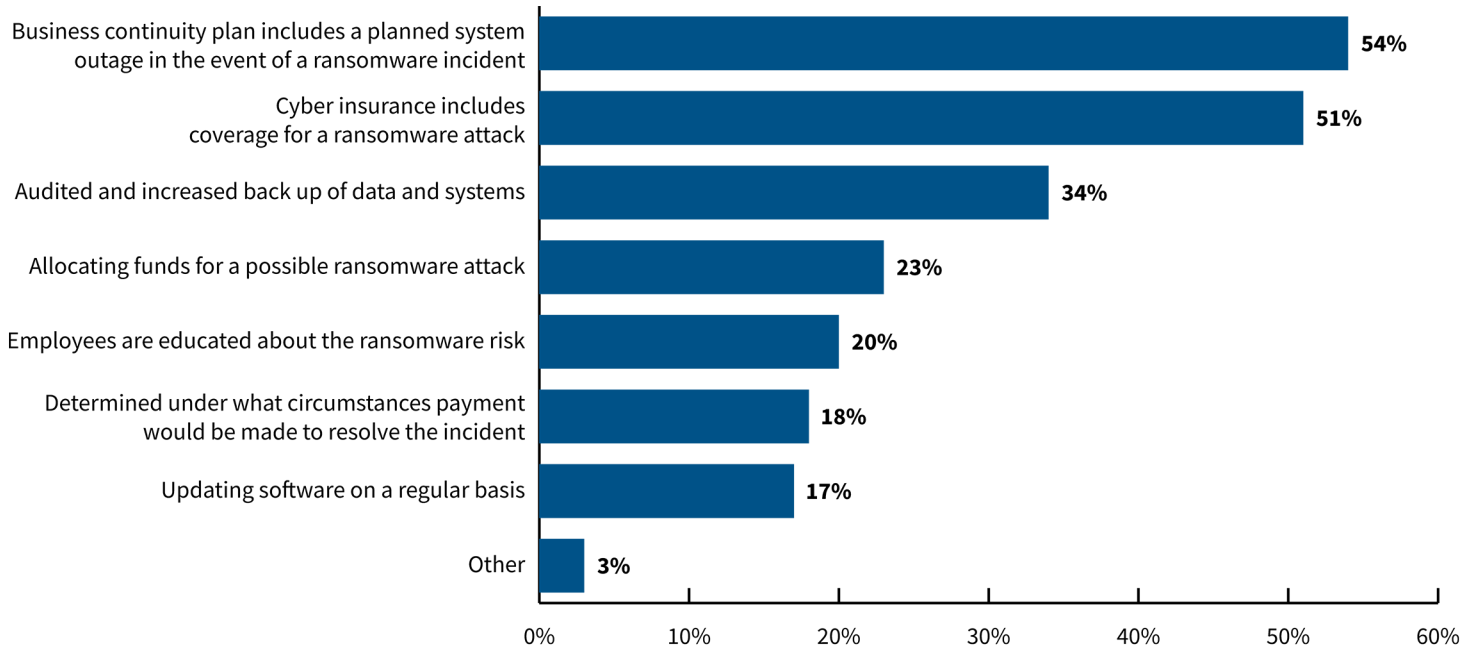


Figure 4. What steps were taken to prepare for a ransomware attack?
More than one response permitted



Cybersecurity experts strongly believe that nothing will change if the healthcare industry continues to deny the impact that cyber-attacks and IT failures have on patient care and safety. The good news is that healthcare leaders are beginning to change how they manage cybersecurity risk and build overall resilience. Respondents stated that they believe the most critical action to take when facing ransomware threats is a business continuity plan that includes system outage tests and cyber insurance coverage validation. In Figure 4, survey respondents itemized all steps taken to prepare for a ransomware attack.

The data from this study suggests a correlation between cyber-attacks and impacts to patient safety and care delivery. Fortunately, there is a silver lining. The pandemic has put a spotlight on what needs to happen. We've learned that we need to do more with less, collaborate more for leverage, and be better prepared in our recovery and continuity operations. Simply put, our industry has miles to go before we can sleep. So, six months after publishing the Ponemon Research, where exactly are we as an industry?

The good news is that there has never been more collaboration between the public and private sectors across the healthcare industry. For example, the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) includes more than 300 health providers entities, medical device manufacturers, health IT companies, plans and payers, labs, blood and pharmaceutical companies, public health entities, and several government partners. They are working together to develop cybersecurity practices, processes, and educational material to help practitioners:

- Align cyber threats to best practices
- Build risk management programs to protect our healthcare supply chain
- Manage cybersecurity threats that can occur during an emergency, such as the COVID-19 pandemic
- Reduce cost, complexity, and time in the contracting process while improving patient safety

Unfortunately, cyber-attacks continue to impact HDOs with no end in sight. It's not a matter of if you'll experience a cyber incident; it's a matter of when and to what end and overall cost. Healthcare leaders must make cybersecurity and risk management a top strategic priority, investing in programs that "digitally transform" how they manage risk and cybersecurity with the same sense of urgency and focus applied to initiatives such as patient engagement. The Ponemon Institute study is not only a wake-up call for the healthcare industry to transform its cybersecurity and risk management programs, but also a call for community advocacy to take action and deliver more robust protection of our data and the assurance of the availability of life-saving care whenever and wherever we need it.

HICP in the Spotlight

March 13-19 was Patient Safety Awareness Week

The Institute for Healthcare Improvement created the Patient Safety Awareness Week (PSAW) campaign to inspire action to improve healthcare safety. This annual event serves as a dedicated time and platform to build awareness about patient safety and recognize the work already being done. As the HHS 405(d) Program says, "Cyber Safety is Patient Safety," and cybersecurity plays an important role in keeping patients safe.

This year, the 405(d) Program was excited to release a PSAW toolkit for healthcare and public health organizations to communicate with their employees directly as well as awareness products for our own platforms. We wanted to show that cybersecurity can be a priority for every member of a healthcare organization, no matter the member's role or the organization's size.

The toolkit included a poster and video with tips to protect patients through cybersecurity, as well as draft emails for management based on organizational sizes (small and medium/large). The content can be used in internal communications such as email distros, newsletters, and social media platforms like Yammer. Based on the reception of these products, we hope to provide even more robust toolkits for next year.

You can find the toolkit here. If you missed PSAW, don't worry! The content is designed to be relevant year-round because patient safety should always be a priority.

HIMSSCast: What is HHS 405(d), and how can it help build cybersecurity readiness?

Leaders from the U.S. Department of Health and Human Services, Intermountain and HIMSS discuss the top threats to information security – and describe how this key public-private partnership can enable more collaborative and consistent risk mitigation.

Listen to the podcast here.

Bust Cybersecurity Myths with Education and Training

By Bijan Anvar, 405(d) Task Group Member

The 405(d) Chronicles is a platform for sharing firsthand insight, lessons learned, and perspectives from cybersecurity professionals in the field today.

I have seen and heard a lot as someone who frequently gives trainings extensively to medical, dental, and legal groups. What really surprises me are the cybersecurity myths so many people believe. After one of my presentations, someone told me that my presentation was useless to them because their office used "Macs" and, "FYI, Macs don't get malware." This was a relatively small group, but the gentleman assured me that he confirmed it with the person who handles their IT. I politely mentioned that it is never a bad idea to get a second or third opinion, and he might want to consider speaking with someone else. This was on a Sunday. The following day, he called me to say that he was hit with ransomware and needed help.

Another time, I was in my doctor's office and saw what looked like a hard drive in a bucket of water. I asked what they were doing, and they responded, "We replaced the hard drive, and our IT person told us to clean the drive by leaving it under water for 24 hours." When I told them that they needed soap to clean it well, they were surprised, but took my advice seriously. I have been a patient there for MANY years, so thought I could have a little fun. The issue, however, is serious. Clearly, that is not the way to wipe a hard drive, but this is what they were told by people they paid for IT expertise.

These are just two real life examples of people trusting IT professionals without verifying the information and that information being wrong. Cybersecurity education and training are critical to any small, medium, and large business. Training should include creating best practice protocols. This is important not only to be proactive, but also for vetting a vendor who promises to help you with your security needs. What good is buying a firewall if it is not configured properly? You don't have to know about IT to ask about IT. You owe it to your patients who trust you with their data to be informed about cybersecurity.

There are many resources to help all sizes of businesses. The 405(d) program is the best place to start if you're looking for a place to begin learning about cybersecurity for your healthcare organization. The *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP) publication lays out the top five threats facing healthcare and the ten practices to mitigate those threats. The 405(d) Program also helps with cyber hygiene for offices with posters, an active social media presence and campaigns such as Patient Safety Awareness Week and Cybersecurity Awareness Month. All their awareness products and resources can be found at 405d.hhs.gov.

Cybersecurity in the News

Russia-Ukraine War: Threats Facing the Healthcare Sector

HealthcareInfoSecurity.com reported that as Russia's military invasion and cyberattacks on Ukraine escalate, some experts warn that critical infrastructure entities, including those in the health and public health sector of the U.S. must also be on high alert for potentially disruptive cyber assaults. As the conflict in the Ukraine worsens, a top concern for healthcare sector entities is potential "collateral damage" related to cyberattacks and corresponding kinetic attacks, says Erik Decker, CISO at Intermountain Healthcare and 405(d) Program co-lead. He added, "Right now, there's no threat against the [U.S.] homeland directly that we're aware of due to that conflict, but the ability for malware and other types of attacks that bleed over and come into the homeland is a concern."

Read the full article here.

Learn how to keep your organization and patients from becoming "collateral damage" with HICP here.

Cybersecurity and Data Protection in Healthcare

Forbes published an article about the unique challenges to healthcare entities when protecting medical data. Damage from ransomware is growing fast as more and more attacks successfully attack medical infrastructure. This article looks at what healthcare providers should be wary of and how to protect patient data from cybercriminals.

Read the full article here.

Ready to take action? Start with HICP here.

How to Effectively Communicate Healthcare Cyber Risks to C-Suite Execs

Health IT Security reported that cybersecurity professionals must translate technical jargon into business deliverables in order to effectively communicate healthcare cyber risks to C-suite executives. Communicating the harsh realities of the current cyber threat landscape is essential to fostering a culture of cybersecurity and obtaining the crucial resources needed to combat these threats. On top of steep costs, cyberattacks and data breaches can lead to ambulance diversions, EHR downtime, appointment cancellations, and patient data exposure. The aftermath of a cybersecurity incident can cause reputational harm to the organization and risks to patient safety and privacy.

Read the full article here.

Learn how to mitigate these risks to your patients and organization with HICP here.

Recent Federal Resources

OCR

- Improving the Cybersecurity Posture of Healthcare in 2022

HC3

- Electronic Medical Records in Healthcare
- Lessons Learned from the HSE Cyber Attack
- The Russia-Ukraine Cyber Conflict and Potential Threats to the US Health Sector
- Destructive Malware Targeting Organizations in Ukraine
- Hermetic Wiper Malware
- CISA Issues 'Shields Up' Notice
- 2021 Trends Show Increased Globalized Threat of Ransomware
- Indicators of Compromise Associated with LockBit 2.0 Ransomware and Additional Mitigations
- January News Items of Interest to the Health Sector
- Cyber Threat Posed by BlackMatter RaaS Reduced to Guarded (Blue)

Spotlight Webinar April 13th at 1pm ET!

Join us to learn about the many available resources including free vulnerability scanning, web application scanning, ransomware readiness self-assessments from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. To register, visit our website at 405d.hhs.gov!

About The 405(d) Post

This newsletter is for information purposes only and aims to broaden awareness and align healthcare security approaches. The news articles represented in this newsletter are chosen at random to foster awareness and are not in promotion of any news organization. The "A Word from the Task Group" and the "405(d) Chronicles" is written by a different 405(d) Task Group Member each issue and does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute to this newsletter.

Need To Contact Us? Email us at cisa405d@hhs.gov

Follow us!

Facebook Twitter

Instagram LinkedIn

Visit our website at 405d.hhs.gov!