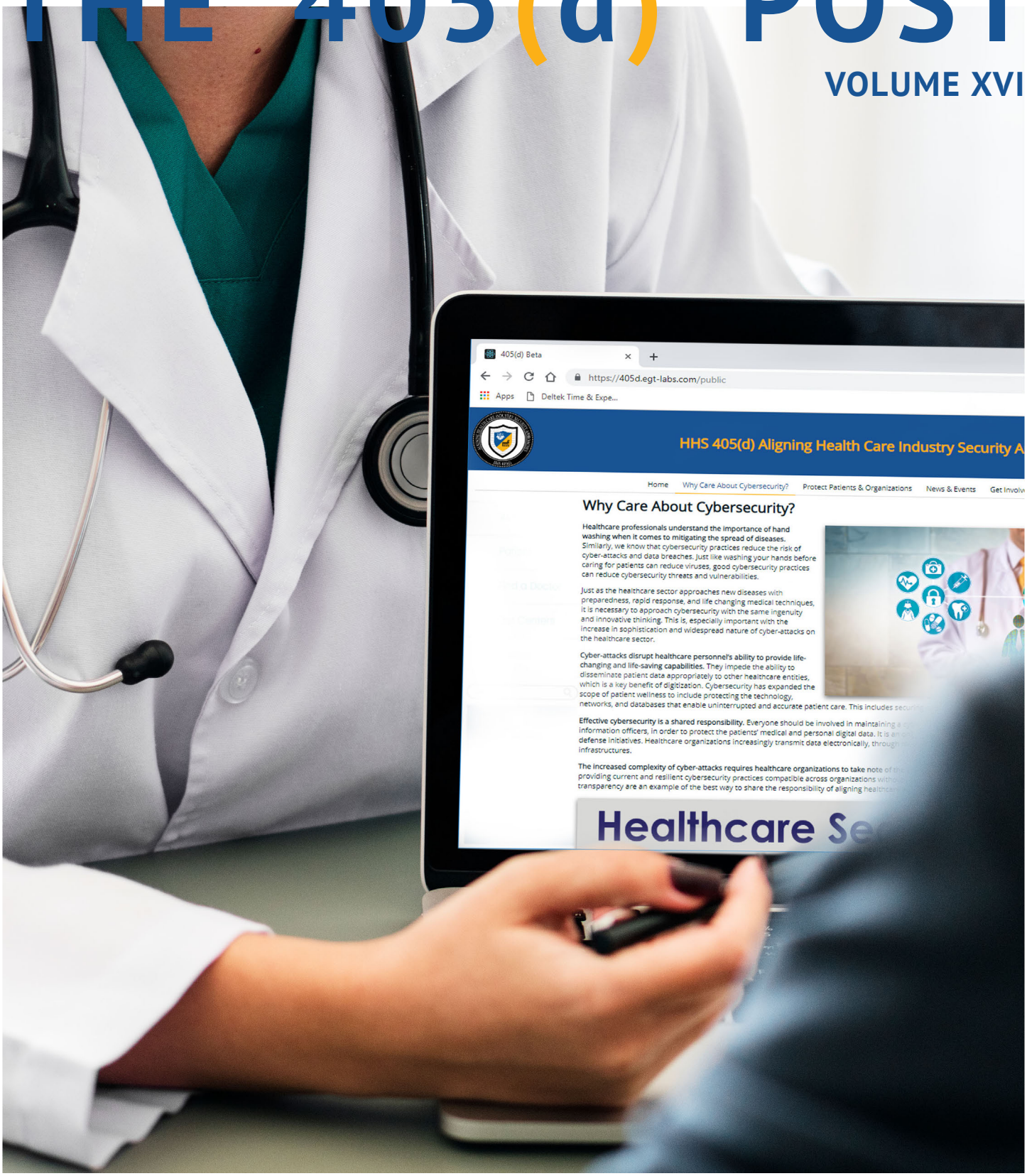
THE 405(d) POST

VOLUME XVI



HHS 405(d)
Aligning Health Care Industry Security Approaches

A Word from the Task Group

Cyber Insurance—From Risk Transference to Organizational Assurance

By Traci Lamb and Mitch Parker, 405(d) Task Group Members

Cyber is one of the most significant risks facing the HPH Sector and the insurance market. Every type of Healthcare Delivery Organization (HDO) has cyber risk. Whether it's ransomware, phishing emails or other cyberattacks, it's becoming more prevalent every day. Accordingly, cyber insurance policies appear to hold more value than in times past. One size doesn't fit all. Due to different risks and exposures, each HDO's need is unique to its business. When looking for a good cyber insurance policy, HDOs should consider coverage in several areas, and weigh that with the associated premium and retention amounts which are increasing significantly. Additionally, insurers are requiring more proactive measures to help mitigate the overall risk to both the insurer and insured. It's helpful to engage an insurance broker to assist with the many facets of cyber risk. They can assist in providing benchmarking data and other information that's challenging for HDOs to obtain on their own in a volatile market.

Two of the major changes that ransomware has brought about have been the significant cost increases and increased scrutiny that policyholders now face. According to the Corporate Finance Institute, purchasing insurance is a common example of transferring risk from an individual or entity to an insurance company.[1] Tom Johansmeyer, in his Harvard Business Review article, The Cyber Insurance Market Needs More Money, indicated that the average ransom payment increased 82 percent from 2020 to 2021.[2] He also indicated that the number of ransomware attacks in the first half of 2021 was more than the entirety of 2020. Marsh indicated in their Cyber Insurance Market Overview: Fourth Quarter 2021 that Cyber Insurance pricing in the US increased an average of

1 Corporate Finance Institute. "Risk Transfer." https://corporatefinanceinstitute.com/resources/knowledge/strategy/risk-transfer/.

2 Tom Johansmeyer. "The Cyber Insurance Market Needs More Money." Harvard Business Review. March 10, 2022. https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money.

96 percent year-over-year, with the third quarter increase being 40 percent higher than the previous one, and the largest since 2015, when ransomware started becoming a major concern.[3] Marsh identified four factors for this increase, which are:

- **Loss environment:** Numerous insurers have incurred significant loss ratio increases due to the increase in ransomware attacks and severity.
- **Systemic Risk Concerns:** Insurers are paying attention to the risk that a single event like the NotPetya attack could have a wide-ranging effect. Merck's recent legal victory over coverage for $1.4 billion in losses to Merck from its insurers over this attack likely adds to this.[4] With the current situation in Eastern Europe, the probability of a systemic attack has increased.
- **Reinsurance:** Reinsurance, which is insurance for insurance companies, and a way to transfer risk so that they can write more and larger policies, has become significantly more expensive.[5]
- **Available Capital:** The amount of capital available to clients from insurers is decreasing. This means that the premiums that the insurers are collecting has the potential to not be sufficient for a catastrophic loss such as another NotPetya attack.

It is this last concern over available capital that is driving both the artificial scarcity of insurance products and correspondingly higher prices. Insurance companies, given the significant upward trend in attacks and frequency, are not going to act in the capacity of risk transference for companies that are at risk for incurring a ransomware attack that will cost them multiples of premium costs. The reinsurance industry still has memories of what happened to AIG in 2008, when they lost $30 billion on insuring real-estate-backed multi-sector Collateralized Debt Obligations (CDOs).[6] These were the toxic assets that were a major factor in the 2008 financial crisis. The increasing costs and frequency of ransomware attacks bring concern that instead of toxic financial assets, a large-scale ransomware attack could bring our financial system to a halt this time.

What can Healthcare do about this?

Healthcare organizations need to work in partnership with their insurance brokers to build plans to address cyber insurance coverage. While some larger universities, such as Indiana University and the University of Nebraska are self-insuring against cyberattacks, most healthcare organizations do not have the financial resources, capital, or credit to do the same.[7] Healthcare has risk management plans for other adverse events. Cyber events need to be at the same level as other enterprise risks.

The first step is to call or meet with the insurance broker and understand what their security requirements are for retaining the cyber insurance policy. Get a list from the broker in writing of what specific security requirements they are looking for. Also make sure to notify your CFO, Controller, or Treasurer of this.

Conduct a risk assessment of your organization against the HIPAA Security Rule using the ONC Security Risk Assessment tool, available here. If possible, have an outside firm complete this.

3 Marsh. "Cyber Insurance Market Overview: Fourth Quarter 2021." https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html.

4 Marsh. "Cyber Insurance Market Overview: Fourth Quarter 2021." https://www.marsh.com/us/services/cyber-risk/insights/cyber-insurance-market-overview-q4-2021.html.

5 "Insurance Handbook: Reinsurance." Insurance Information Institute. https://www.iii.org/publications/insurance-handbook/regulatory-and-financial-environment/reinsurance.

6 Robert McDonald and Anna Paulson. "AIG in Hindsight." Federal Reserve Bank of Chicago. October 2014. https://www.chicagofed.org/~/media/publications/working-papers/2014/wp2014-07-pdf.pdf.

7 Chris Dunker. "Regents approve adding cyberattack losses to self-insurance policy." Lincoln Journal Star. April 8, 2022. https://journalstar.com/news/local/education/regents-approve-adding-cyberattack-losses-to-self-insurance-policy/article_24c6be3b-1843-5df2-a9e2-9673edbad678.html.

Perform a gap analysis of the Risk Assessment results to determine areas for improvement. Develop a plan to address the discovered issues, starting with the highest ones. Ensure that issues are assigned to projects, tracked, and monitored for progress and completion.

Align the projects against the 405(d) Health Industry Cybersecurity Practices (HICP). These resources, which are available at 405d.hhs.gov, discuss ten types of practices that organizations can tailor to their needs:

1. Email Protection Systems/Security to avoid phishing, malware, and social engineering attacks
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device/Internet of Things Security
10. Cybersecurity Policies

What is most important here is that organizations align their projects against these practices with a goal of demonstrating improvement in one or more of each area.

In addition to those areas, organizations need to address the following:

- **Tabletop Exercises:** Conduct tabletop exercises at least annually to determine readiness and gaps in it in case of a cyber-attack.
- **Downtime Procedures:** Work with clinical and administrative departments, especially Health Information Management (HIM), Revenue Cycle, Laboratory Services, and Radiology, to understand process flows and what to do in case computer systems no longer work. Update this at least annually if not more. For more information, see Cybersecurity Practice 10: Cybersecurity Policies in the HICP Technical Volumes.
- **Physical Security:** Conduct a physical security risk assessment and address findings and concerns. For more information, see Cybersecurity Practice 2: Endpoint Protection Systems in the HICP Technical Volumes.
- **Contract Language:** The Health Sector Coordinating Council (HSCC) has published Model Contract Language for Medtech Cybersecurity (MC2). This is available here.
- **PCI-DSS Compliance:** This is required to process credit cards by the credit card brands. If resources allow, get an Attestation of Compliance done by a Qualified Service Assessor (QSA).
- **Privileged Access Management:** No user needs administrative access by default. Require two-factor authentication to access these critical credentials and cycle the passwords when complete. For more information, see Cybersecurity Practice 3: Access Management in the HICP Technical Volumes.
- **Email Protection Systems:** Email security measures to avoid phishing, malware and social engineering attacks. For more information, see Cybersecurity Practice 1: Email Management in the HICP Technical Volumes.

The ransomware epidemic means that the insurance underwriters are going to do whatever they can to avoid becoming the next AIG due to it. This means that instead of just writing a check, companies need to proactively demonstrate compliance with best practices and requirements. The 405(d) Program, ONC, and HSCC have provided excellent resources. Leverage them as part of a plan to show the insurance companies that issuing a policy to your company presents less risk than a CDO did in 2008.

HICP in the Spotlight

Incident Response for Small Healthcare Organizations

Incident response is the ability to discover cyberattacks on the network and prevent them from causing data breach or loss. Incident response is often referred to as the standard "blocking and tackling" of information security. Many types of security incidents occur on a regular basis across organizations of all sizes. Two common security incidents that affect organizations of all sizes are 1) the installation and detection of malware, and 2) phishing attacks that include malicious payloads (via attachments and links). Though neither of these incidents directly results in a data breach or loss, each event enables breach or loss to occur through subsequent events. Small organizations are often challenged by incident response management, in part because incident response procedures may not be established. Employees who rarely encounter cyberattacks may not remember what to do in the case of an incident. Members of the management team may not know whom to contact to obtain or provide information about the incident. In many cases, there are no dedicated information security professionals in small organizations, resulting in increased reliance on the IT department. A common concern is the fear of penalties from regulators if the organization contact authorities to rectify a security incident.

To address these concerns, establish and implement an incident response plan: Before an incident occurs, make sure you understand who will lead your incident investigation. Additionally, make sure you understand which personnel will support the leader during each phase of the investigation. At minimum, you should identify the top security expert who will provide direction to the supporting personnel. Ensure that the leader is fully authorized to execute all tasks required to complete the investigation. Once your incident response plan is implemented, ensure compliance with the plan's elements. At minimum, your plan should describe steps to be followed, for example, in the event of malware downloaded on a computer or upon receipt of a phishing attack. See below examples of actions to take to respond to incidents.

Incident	Response Recommendation
Malware	• Re-image, rebuild, or reset computer to a known good state. • Do not trust "malware cleaning" tools until they are verified to function as described.
Phishing	• Identify malicious e-mail messages and delete from mailboxes. • Proactively block websites (URLs) referenced in "click attacks." • Identify malware that might have been installed on computers, and remediate appropriately if present

For more information on Incident response plans check out the full Health Industry Cybersecurity Practices Publication (HICP) and HICP Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations at 405d.hhs.gov.

Happening Around Us

Solara Medical Supplies Faces $5M Proposed Settlement After Data Breach

A proposed settlement would require Solara Medical Supplies to pay $5 million and perform remedial security measures after a 2019 data breach that impacted 114,000 individuals. Judge Marilyn L. Huff from the US District Court for the Southern District of California preliminarily approved the deal, and the final hearing is set for September 12, 2022. In November 2019, the California-based medical supply vendor began notifying patients that their data was potentially compromised after some employee email accounts were breached for several months between April and June. The breach exposed names, Social Security numbers, birth dates, billing information, insurance information, driver's license numbers, and medical information. Solara Medical Supplies denied all wrongdoing, and the settlement does not qualify as an admission of guilt.

Read the full article here.

Learn more about how you can protect yourself from breaches with HICP here.

FDA releases medical device cybersecurity draft guidance

The U.S. Food and Drug Administration (FDA) published draft guidance in April, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," which seeks to emphasize the importance of safeguarding medical devices throughout a product's life cycle. The guidance released in 2018 was only draft guidance. This guidance when finalized will replace the current premarket guidance released in 2014. "These recommendations can facilitate an efficient premarket review process and help ensure that marketed medical devices are sufficiently resilient to cybersecurity threats," said FDA in the Federal Register notice about the guidance.

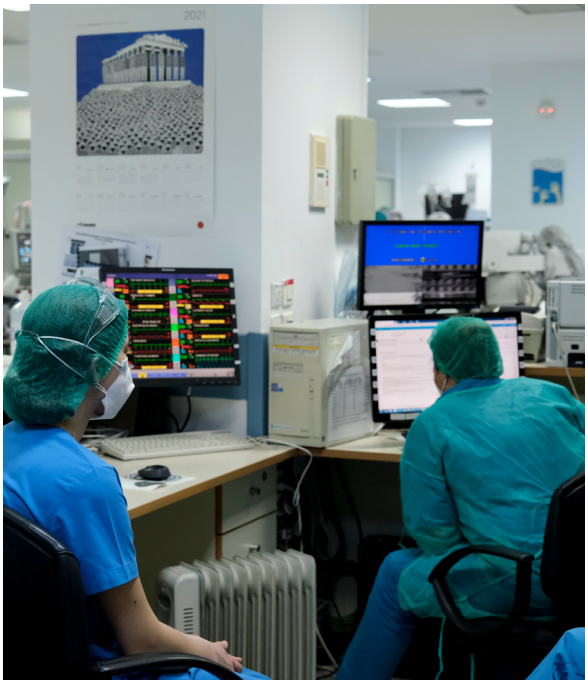
Read the full article here.

Alabama-based Healthcare Provider Impacted by PII Security Breach

Chief Healthcare Executive.com released a report regarding a breach at the Norwood Clinic in Alabama. The Alabama-based healthcare provider disclosed it had an incident affecting 228,000 patients. The health department said the incident was reported February 25. The Norwood Clinic said in a statement it discovered a cyber-attack had taken place in October. The clinic said the attacker gained access to servers that stored patient information, such as birthdates and Social Security numbers. The information did not include financial information or credit or debit card numbers, Norwood said. Norwood said it has employed cybersecurity experts to review its systems and has worked to improve its network security. Norwood also offered credit monitoring and identity theft protection services to patients.

Read the full article here.

Learn more mitigation practices with HICP here.



Recent Federal Resources

HC3

- Insider Threats in Healthcare
- Health Sector Cybersecurity 2021 and 2022 look ahead
- Lapsus$ and the Health Sector
- Mailchimp Sector Alert
- 2021 Top Routinely Exploited Vulnerabilities
- HIVE Ransomware Analyst Note
- March 2022 Vulnerabilities to the Health Sector
- Health-ISAC and HC3 Joint Bulletin: Potential Malicious Cyber Attacks from Russia - Credible Threats to US Critical Infrastructure Sectors

CISA

- 2021 Trends Show Increased Globalized Threat of Ransomware

OCR

- Four HIPAA enforcement actions hold healthcare providers accountable with compliance

June Spotlight Webinar Coming Soon!

Want to be the first to know the topic, date, and time of our upcoming June Spotlight webinar? Follow us on social media at @ask405d!

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!