THOMPSON COBURN LLP

insights

TYPES NOT MAPPED YET August 07, 2023 | TTR not mapped yet | Matt I. Hafter

Refresher on Cybersecurity Resources for Health Care Entities

Recently, the U.S. Department of Health and Human Services published new cybersecurity resources describing best practices for health care organizations. In its Hospital Cyber Resiliency Analysis Initiative: Landscape Analysis, HHS noted that "[t]he National Security Council (NSC) considers the [healthcare and public health] sector to be one of the top three sectors prioritized for additional cybersecurity attention" with the FBI now considering the patient and public safety risk that "cyber-attacks are posing on hospitals as 'threat to life' crimes."

With this background, HHS made ten "key observations" about the state of play. Here is a refresher on those observations and what they mean.

1. **Directly targeted ransomware attacks aimed to disrupt clinical operations are an outsized and growing cyber threat to hospitals.**

- HHS characterizes ransomware as the largest threat to the healthcare sector that has a major impact on patient care and safety.
- As an example, the report describes one case of a ransomware attack on a practice where the physicians elected to retire from the practice rather than pay to retrieve the data.

2. **Variable adoption of critical security features and processes, coupled with a continually evolving threat landscape, can expose hospitals to more cyber-attacks.**

- Multi-factor authentication may not be used consistently across key systems and critical entry points.
- Barely over 50% of surveyed hospitals reported having a documented plan to address vulnerabilities; and many rely on regular scanning for vulnerability management which by itself is not sufficient without (among other things) processes to priority and address identified issues.
- The scope of training of hospital staffs varies, and there is little data on the efficacy of such outreach.
- With the increase of in-home care, medical devices and technologies are increasingly important to communicate, monitor and report information; however, this leads to challenges in standardizing and protecting those devices and the information that flows across them.

3. **Hospitals report measurable success in implementing email protections, which is a key attack vector.**

- Virtually all hospitals surveyed had basic spam and phishing protections in place. But these protections do not definitively prevent the current generation of social engineering and phishing attacks.
- New types of attacks, for example, can penetrate these protections by becoming malicious only after they are delivered.

4. **Supply chain risk is pervasive for hospitals.**

- Like many other enterprises, hospitals find it challenging to manage risks arising from their supply chain, with third-party and supply chain risk being the third most important threat among a sampled group of chief information security officers.

© 2025 Thompson Coburn LLP Attorney Advertising

5. **Medical devices have not typically been exploited to disrupt clinical operations in hospitals.**

- Although not a significant attack vector for cyber attacks, medical devices warrant attention as a vulnerability for hospital operations.
- Unsupported, legacy medical devices may be difficult to scan and especially vulnerable to advanced forms of attack; which, in turn, may require additional segmentation and thereby limit their usefulness.

6. **There is significant variation in cybersecurity resiliency among hospitals.**

- Especially with smaller hospitals, knowledge of resiliency coverage was limited. These hospitals found it challenging to stay current on threats and – with limited budgets – invest in cybersecurity resources.

7. **The use of antiquated hardware, systems and software by hospitals is concerning.**

- A very significant majority of reporting hospitals of all sizes reported that they operate with end-of-life operating systems or software with known vulnerabilities, presenting greater challenges to implement patches and other security protections.
- Even larger hospitals that may enjoy more robust protections expressed concerns about connecting and sharing data with affiliates or with small rural hospitals where the use of legacy systems is more prevalent.

8. **Cybersecurity insurance premiums continue to rise.**

- Premiums for cyber insurance have increased significantly, resulting in some hospitals not securing insurance or self-insuring.
- Coverage exclusions for not meeting minimum security standards also reduce the adequacy of coverage.

9. **Securing cyber talent with requisite skills and expertise is challenging.**

- Talent gaps in meeting the need for trained personnel to fill jobs in cyber security is a challenge generally, and especially in the health care sector where qualified individuals are more attracted to higher-paying industries.
- Hospitals with smaller budgets are nonetheless subject to the same compliance standards and resource needs as larger hospitals but have more difficulty staffing their cyber functions.

10. **Adopting HICP improves cyber resiliency.**

- HHS's analysis illuminated a correlation between HICP (health industry cybersecurity practices) and the benefits of implementing the NIST cybersecurity framework (National Institute of Standards and Technology standards and guidelines of best practices).

After this comprehensive description of the landscape, HHS suggests some steps to mitigate risks. These include:

- Identify mission-critical suppliers and require contractual protections for cyber risks, and mitigate those supplier risks through internal controls and remediation.
- Develop and continually update an IR (incident response) playbook to monitor, identify, mitigate and respond to threats.
- Conduct "red team" and table top exercises involving a large scale system down event with executives and key clinical leaders to test preparedness and responses.
- Conduct training simulating a "whaling" attack (a form of phishing in which the bad actor impersonates a senior executive in the organization – the "whale" – and targets those in less powerful positions to reveal sensitive data or performing other harmful actions).

Thompson Coburn attorneys are closely monitoring the progress of these developments and would be pleased to help clients with the steps to mitigate risks. Contact the authors for additional information.

© 2025 Thompson Coburn LLP Attorney Advertising

authorsTest

matt

Matt I. Hafter

© 2025 Thompson Coburn LLP Attorney Advertising