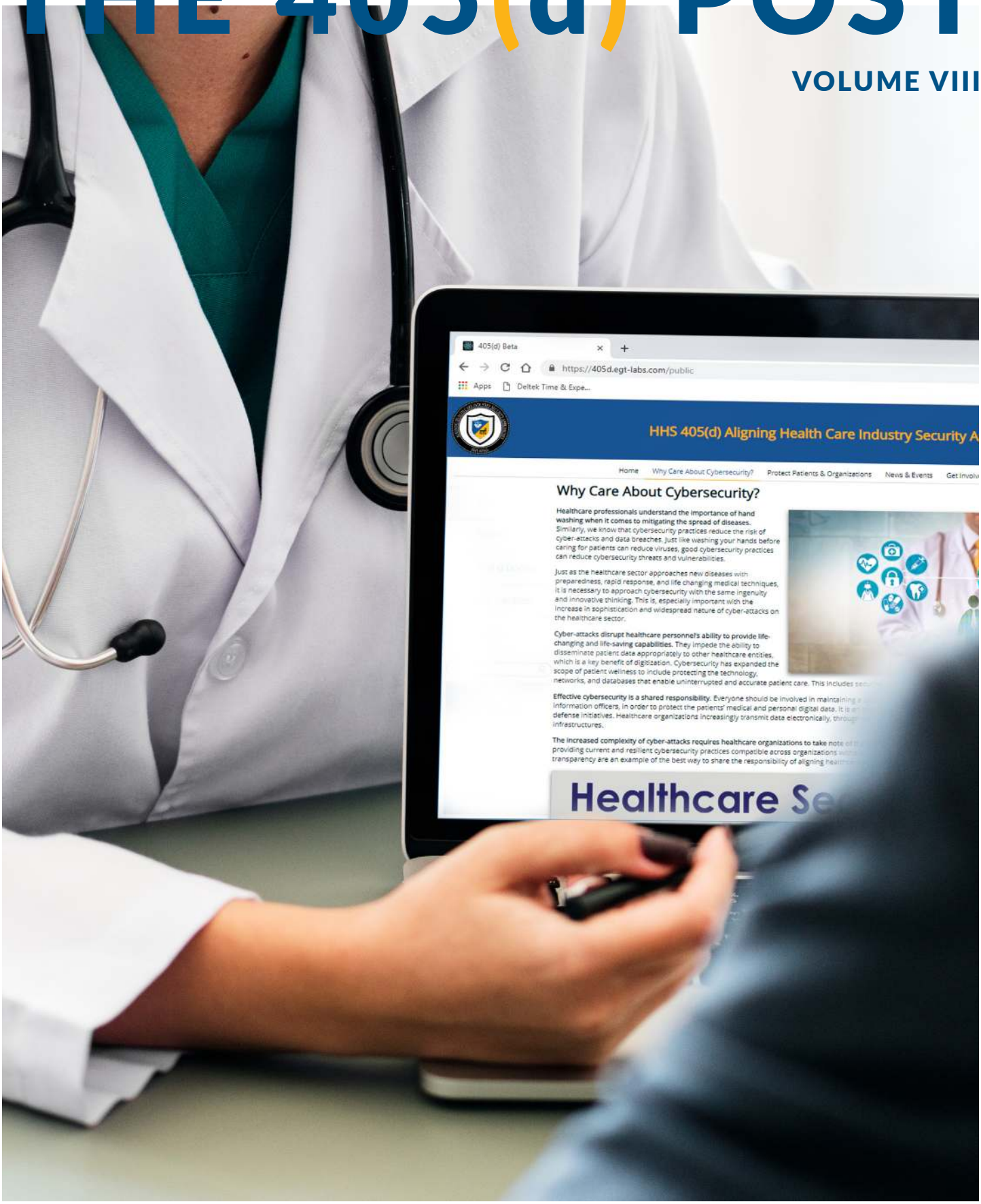
THE 405(d) POST

VOLUME VIII



HHS 405(d)
Aligning Health Care
Industry Security Approaches

Effective Cybersecurity Training and Awareness Programs

Lenny Levy, CISSP, CISA, MBA 405(d) Task Group Member

Have you ever been forced to sit through a boring security training session? Or have you ever taken an online course and want to click the “next” button as quickly as possible to make it end? As a cybersecurity leader, even I find those sessions unbearable.

Why deliver training at all? Compliance is often cited, but the reality is cybersecurity is not just a technical issue. The human element plays a key role in keeping healthcare organizations secure. End users can impact the security posture in a variety of ways, such as :

- Clicking on a malicious link in a phishing message that launches a ransomware attack
- Copying data to an unencrypted flash drive which is subsequently misplaced
- Using an insecure password that an attacker guesses to obtain access to Protected Health Information

An effective training and awareness program is needed since everyone plays a role in the security of an organization. So why isn’t droning on about the latest cyberattacks for an hour effective? Some common attributes of an ineffective program include:

- Content is not targeted to the attendee’s role
- Too much content in one session
- Material is not engaging
- Training concepts are not relatable

Ultimately, organizations need a strong culture of security so all users understand their role in keeping it secure.

Targeted training material

It would not make sense to have a training with nurses to discuss the importance of patching servers, nor would it be a good use of time to discuss secure coding practices with executives. However, there are

topics like social engineering that apply to all users, and teaching users how to recognize the signs (e.g., emotional pull, urgency) and mechanisms (e.g., phishing) are important for a broad audience. Other topics may be more relevant to specific populations, and should be addressed accordingly. See Table 1 for an example on how this concept can be customized for your organization.

Group	Timing	Key activities	Delivery *
Entire Workforce			
New members	*Orientation*	• HIPAA security and privacy • Secure password practices • Phishing (and where to report)	*In-person*
All members	*Annual*	• Data protection • Staying safe online • Social engineering • Emerging topics (e.g., work from home)	*LMS*
	Monthly	Leverage video "snippets" / short training sessions on topics including: • Data security • Physical security • Online scams • Working from home • Identifying suspected security incidents	*LMS*
	As required	• Topical awareness campaigns based on current events Newsletters / emails with tips / tricks • Focused activities for cybersecurity awareness month (October)	*Email* *In-person* *Ambassadors*
Specific populations			
Help desk	*As required*	Training on common phone-based scams including fraudulent credential resets, link / file access, etc.	*In-person* *Ambassadors*
Clinical staff	*As required*	• Topics based on population need / risks • Securing protected health information • Potential clinical impact of cybersecurity	*Email* *In-person* *Ambassadors*
Corporate Finance	*Biannually*	Business Email Compromise (BEC) scams	*In-person*
Incident Response Team	*Twice a year*	Training and tabletop exercise for the incident response plan	*In-person*

Table 1 – Example training plan

It is important to note that one delivery mechanism is not necessarily the best for all groups / topics. While email can be easily ignored, in-person or virtual training sessions are not always logistically feasible. Given many small and moderately sized organizations do not have anyone dedicated to security awareness and training (or even security), leveraging champions or ambassadors is an effective way of reaching different populations. These are security aware individuals cultivated across the organization to help deliver awareness activities to their teams.

Frequency

Annual training sessions are great for a compliance "checkmark" but are not effective for long-term retention or culture change. Instead of trying to cram as much content into a session, content should be delivered in smaller more manageable segments. This helps increase retention and demonstrates the priorities users should focus on. As shown in Table 1, frequency should be tied to the audience and topics being conveyed.

Interesting and Fun

Training is one of the only interactions most users have with the information security function. Boring sessions can give the perception that the material is not important, or the organization does not care. No need to dress up as a clown for impact, but be thoughtful about how the content can be engaging. For example, during cybersecurity awareness month my teams have leveraged escape rooms, crossword puzzles, scavenger hunts and more to reach people in different ways. Activities like a coloring contest can be valuable since they can engage the workforce member and their family. In addition, there are a variety of humorous security awareness videos that make light of common issues in a way that grabs attention.

Relatable

If the recipient does not see the value of the information, they are less likely to retain and apply it. One of the best ways to demonstrate value is to show how the material applies to their day to day life. Talking about the importance of multi-factor authentication for personal bank accounts, makes it easier for people to understand why it's needed for electronic medical records.

Conclusion

A successful cybersecurity awareness and training will positively impact culture and translate to behavioral change. Tying to a common goal, like patient safety, helps organizational acceptance for the time and effort spent on training activities. In addition, making sure the content is relevant to your workforce and engaging will also help drive cultural change.

Some people will take a look at this and nod their head in agreemen[1]t while others won't know where to start. For smaller organizations, take a look at the education topics in the Health Industry Cybersecurity Practices (HICP) Volume 1[1] from HHS' 405(d) Task Group. Complementing that are free training resources from HHS[2] , NIST[3] and DHS CISA[4] to get started. Rather than just picking random training sessions, think about the threats your organization faces and translate that into training program goals. For some it could be as simple as making sure your workforce knows who to call when they see something suspicious (e.g., report phishing message, computer acting strange).

Once you establish program goals, consider how you will measure success. While phishing tests can be an easy quantitative measure, think about other factors that demonstrate the impact of the training and awareness activities. Example metrics include:

- % of workforce members who click on phishing message
- % of workforce members who report phishing message (without clicking on it)
- % of workforce members who report phishing message (after clicking on it)
- % of workforce members who clicked on phishing message who took remedial training
- % of workforce members with malicious software detected on their workstation
- Periodic surveys on workforce member perception on information security

[1] https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf
[2] https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html
[3] https://www.nist.gov/itl/smallbusinesscyber/training
[4] https://www.cisa.gov/critical-infrastructure-training

405(d) HICP In the Spotlight:
Data Protection and Loss Prevention

A security breach is the loss or exposure of sensitive data, including information relevant to your organization's business and patient PHI. Impacts to your organization can be profound if data is corrupted, lost, or stolen. It's important to note that within the past few months, during the current pandemic, comes a significant spike in data breaches due to COVID-19 related scams and attacks, appearing as phishing, malware, ransomware, and more.

Security breaches may prevent users from completing work accurately or on time, and could result in potentially devastating consequences to patient treatment and well-being. Thus, good data protection and loss prevention practices in turn protect the organization and its patients.

The loss of sensitive data can be prevented in several ways. Data loss prevention is based on understanding where data resides, where it is accessed, and how it is shared. To protect your organization against data loss, consider the following tips:

- Set policies, guidelines, and/or expectations for how your workforce is expected to manage the sensitive data at their fingertips to ensure consistency and reduce errors. Most health care employees work with sensitive data on a daily basis, so it is easy to forget how important it is to remain vigilant about data protection.
- Establish a data classification policy that categorizes data as, for example, Sensitive, Internal Use, or Public Use.
- When e-mailing PHI, use a secure messaging application such as Direct Secure Messaging (DSM), which is a nationally adopted secure e-mail protocol and network for transmitting PHI.
- Train personnel to comply with organizational policies. At minimum, provide annual training on the most salient policy considerations, such as the use of encryption and PHI transmission restrictions.

Protecting our patients from cyber threats even during these uncertain times is paramount to keeping our healthcare systems running smoothly and securely. For more information on network segmentation and other ways to protect your organization from cyber threats, check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

Happening Around Us

Health Care Entities Continue to Get Hit by Ransomware: Universal Health Services Estimated to be Largest One in 2020

The National Law Review

As stated by the National Law Review, health care entities continue to face a barrage of attacks from cyber criminals, getting hit more frequently than any other industry. What is being publicized as one of the largest ransomware attacks against a health care entity in 2020, occurred in early October against Universal Health Services (UHS). It is believed that the ransomware attack involved the Ryuk strain, which is linked to Russian cybercriminals. Ransomware attacks are designed to be disruptive, and a disruption to patient care. To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

Physicians, nurses and support staff respond differently to data breach security policies

Becker's Hospital Review

In a study completed by Binghamton (N.Y.) University researchers and their team, the different subcultures of physicians, nurses and support staff will influence whether employees violate information security policies. Sumantra Sarkar, PhD, associate information systems management professor at Binghamton University said that, "Physicians, who are dealing with emergency situations constantly were more likely to leave a workstation unlocked. They were more worried about the immediate care of a patient than the possible risk of a data breach… On the opposite end, support staff rarely kept workstations unlocked when they were away, as they felt they were more likely to be punished or fired should a data breach occur." To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

4 Sophisticated Phishing Campaigns Impacting the Healthcare Sector

Health IT Security

HealthITSecurity reports that hackers have leveraged the COVID-19 public health crisis to improve the sophistication and increase the frequency of phishing attacks, specifically targeting the healthcare sector.

The 4 major campaigns are:

1. **Overlay Tactic Aimed at Employee Credential Theft**, or emails that imitate messages sent from an organization's technical support team. The hackers disguise these emails as sent from the company's email service.
2. **Hidden Text or Zero Font**, which allows malicious emails to bypass email security controls to deliver the messages to the victim's inbox by hiding malicious embedded text within an email.
3. **Agent Tesla RAT (remote access trojan) Malware**, employing malicious email attachments containing the RAT and disguised as messages that offer face masks and forehead thermometers from a mask production business.
4. **KONNI RAT Malware**, delivered in Microsoft Word documents that contain a malicious Visual Basic Application (VBA) macro code that is able to change the color of the font from light grey to black to trick the user into enabling the contents of the malicious email.

To learn more about how to protect your organization from cyber threats check out Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication.

Joint Cybersecurity Alert!

UPDATED Alert AA20-302A

This advisory was updated to include information on Conti, TrickBot, and BazarLoader, including new IOCs and Yara Rules for detection.

CISA, FBI, and HHS have credible information of **an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.** CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats.

Key Findings

- CISA, FBI, and HHS assess malicious cyber actors are targeting the HPH Sector with TrickBot and BazarLoader malware, often leading to ransomware attacks, data theft, and the disruption of healthcare services.
- These issues will be particularly challenging for organizations within the COVID-19 pandemic; therefore, administrators will need to balance this risk when determining their cybersecurity investments.

Please download the alert for more information at https://us-cert.cisa.gov/ncas/alerts/aa20-302a

405(d) Events and Announcements!

HICP 2 Year Anniversary-December

Additional Resources

COVID-19 Disinformation Activity

Risk Management for Novel Coronavirus (COVID-19)

Agent Tesla Phishing Sector Alert

Netwalker Threat Brief

Ransomware Fact Sheet

Happening Around Us Sources

1. ***The National Law Review***
2. ***Becker's Hospital Review***
3. ***Health IT Security***

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" 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 or check out our website at 405d.hhs.gov!