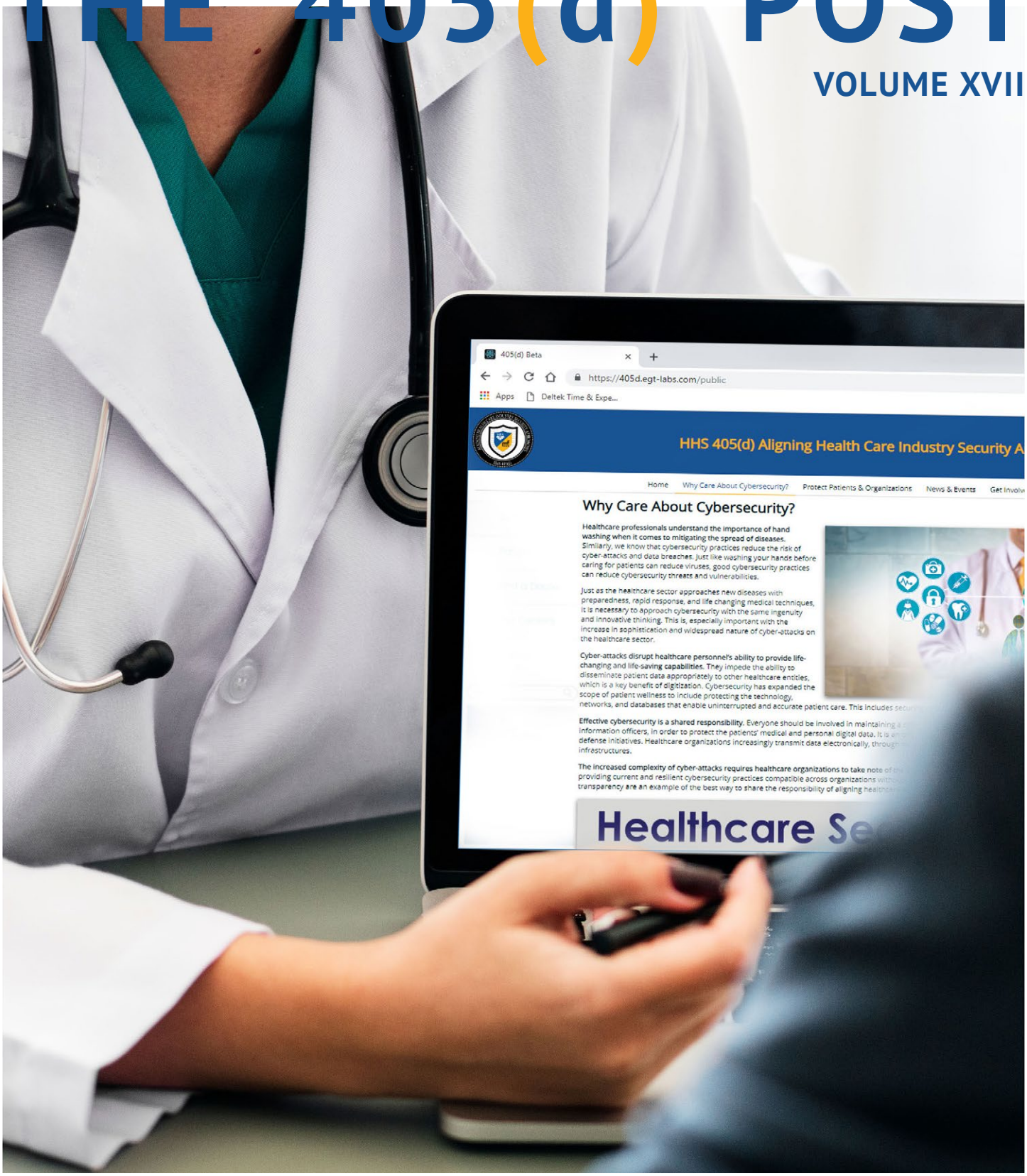
THE 405(d) POST

VOLUME XVII



HHS 405(d)
Aligning Health Care Industry Security Approaches

A Word from the Task Group

Legal Implications of a Cyber-Attack

By Paul Otto, Cindi Bassford, and Dan Ongaro,
405(d) Task Group members

The average cost of a cyber-attack continues to rise, hitting an all-time high last year (according to one leading report) of $4.24M, a 10% rise from 2019's average cost.[1] Healthcare remained the industry with the highest average cyber-attack costs for the eleventh year in a row.[2] And the FBI reported that the health sector was hardest-hit by ransomware cyber-attacks in 2021.[3] Some of the costs are harder to measure, such as reputational impact. Beyond the measurable cost associated with technical containment and remediation, a portion of this cost is attributable to fulfilling legal obligations. These may include costs of the investigation, notification and communications, regulatory enforcement, and litigation.

What Laws Apply and Why?

Not all cyber-attacks raise the same legal implications. There is no overarching, generally applicable U.S. privacy or cybersecurity law, so there is a need to consider which specific laws apply depending on the circumstances. Factors for what laws apply include:

- the entity's industry/sector (and whether the entity is part of critical infrastructure),
- nature of the cyber-attack,
- categories of data impacted,
- affected individuals' location of residency (including end users and employees), and
- contractual obligations that incorporate laws by reference or include flow-down requirements.

In particular, the categories of data impacted (e.g. Protected Health Information (PHI), export controlled information), industry/sector, and the state(s) of residency of affected individuals can determine which laws apply. Applicable laws can be overlapping or nonintuitive. For example many of us in the Health and Public Health industry are familiar with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively, HIPAA) which applies only to certain types of entities (health plans, providers, and clearinghouses engaged in certain types of electronic transactions) and their service providers handling PHI. However, when you look at the category of data, PHI is defined broadly to include what some may think of as 'mere' demographic information, when held by HIPAA-regulated entities. Then beyond HIPAA, health information may also be subject to requirements that include state data breach notification laws, the Federal Trade Commission Act (and state equivalents), the National Association of Insurance Commissioners (NAIC), Data Security Model Law (Model Law) as adopted by numerous states, and government contracts, incorporating regulatory requirements.

1 IBM, *Cost of a Data Breach Report 2021* (July 2021), https://www.ibm.com/downloads/cas/OJDVQGRY#. Not all cyber-attacks result in data breaches (which have specific triggers under the applicable laws), and not all data breaches involve cyber-attacks; the statistics regarding data breaches are thus used as a close proxy for purposes of this discussion.

2 *Id.*

3 FBI, *Internet Crime Report 2021*, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

These laws are not static; for example, several states recently have passed comprehensive privacy laws that have cyber-attack components, most notably California (with a private right of action available where an entity allegedly failed to have reasonable security that led to a data breach). And the Cybersecurity & Infrastructure Security Agency (CISA) is poised to initiate a rulemaking related to new cyber-attack reporting requirements applicable to certain entities supporting critical infrastructure, including a novel obligation to report ransom payments.[4] In addition to those laws more specific to cyber-attacks and cybersecurity expectations, individuals' rights and remedies under traditional "common law" and their state law equivalents can be a nexus for litigation in the wake of a cyber-attack.[5]

Obligations and Costs

Regardless of which specific laws and contractual obligations apply, there are common themes that dictate an entity's obligations following a cyber-attack that can influence cost. These include:

- **Notification requirements:** Entities must pay to provide notification to individuals and regulators, and in some cases to the media and other third parties. Because different laws have various requirements on what must (and must explicitly not) be included, this is less straightforward than it may seem. Further, the laws have various requirements on form of notification, such as when a physical letter is needed or permissible forms of "substitute notice" to reach affected individuals.
- **Credit monitoring services and identity restoration:** Depending on the personal data at issue, state laws and regulators may require offers of complimentary credit monitoring services, often 1-2 years, to affected individuals. Also, entities may opt to pay additional fees for identity restoration to mitigate potential harm to individuals (and perhaps decrease the likelihood of litigation).

- **Regulator investigations and inquiries:** Regulators are given broad authority to conduct investigations or less formal inquiries regarding a cyber-attack. For example, HIPAA-regulated entities face a mandatory investigation by the HHS Office for Civil Rights (OCR) if a cyber-attack resulted in 500+ impacted individuals receiving notice of a data breach. Responding to document requests and written questions is often resource intensive and can last months or years, with investigations often shifting from the specific facts of a cyber-attack to the broader cybersecurity program and risk management strategies.
- **Penalties:** Entities may face substantial penalties for violations of specific laws and these may not be mutually exclusive. Multiple regulators may pursue penalties for the same cyber-attack.
- **Litigation:** Class-action counsel continue to innovate litigation approaches following reported cyber-attacks. Before, smaller cyber-attacks often would not be pursued for litigation, but this trend has changed, especially in light of the California Consumer Privacy Act (CCPA) and its successor, the California Privacy Rights Act (CPRA), which feature statutory damages of up to $750 per individual (or actual damages if greater). In addition, publicly traded companies may face securities litigation and shareholder suits following cyber-attacks, for example alleging mismanagement of the cybersecurity program or cyber-attack response.

Keeping Compliant Without Breaking the Bank

Although the costs of cybersecurity can seem daunting, a strong cybersecurity posture can save significant costs from multiple perspectives, including from decreased legal liabilities after a cyber-attack. Recommended upfront activities include:

- **Incident response plan:** A documented incident response plan (IRP) can serve as a strong foundation for more effective response and mitigation in the face of a cyber-attack. As HICP suggests, an IRP should incorporate leading guidance, be tested regularly, and updated based on lessons learned (which may be particularly important later, should an organization suffer a series of similar cyber-attacks). This is one of the focus areas highlighted in the CISA "Shields Up" guidance launched in early 2022 and is included as a priority in the HHS 405(d) Technical Volume 1 and 2 guidance. Potentially useful references include

4 Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 116th Cong. (2022), https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

5 Common law causes of action for plaintiffs include: negligence, negligence per se, and breach of (implied) contract.

NIST Special Publication 800-61 or Health Sector Coordinating Council (HSCC) Operational Continuity – Cyber Incident.

- **Use of a cybersecurity framework:** There are various cybersecurity frameworks organizations can align their approach to. These frameworks can provide a more comprehensive approach to cybersecurity and to pinpoint opportunities for improvement. Use of these frameworks can alter legal considerations. For example, the U.S. Department of Health and Human Services (HHS) recently requested information regarding recognized security practices, including under the NIST Cybersecurity Framework and 405(d) of the Cybersecurity Act of 2015 to influence HHS's decisions regarding fines, audits, and remedies to resolve potential violations of HIPAA. And a small number of states have adopted "safe harbor" laws against litigation following cyber-attacks where the organization can show use of a recognized cybersecurity framework.
- **Encryption:** Effective encryption can cause an otherwise reportable data breach stemming from a cyber-attack to fall outside the law's various requirements and remedies.[6] Many individual laws allow for a "safe harbor" if sensitive data is securely encrypted (and the encryption keys were not also subject to compromise) so that any data access or acquisition would present limited risk of harm.
- **Contractual protections:** Increasingly, entities are facing significant costs due to cyber-attacks at their third-party vendors and suppliers. Various contractual protections can be used to help drive stronger cybersecurity controls and decrease costs from a cyber-attack (or to provide cost recovery in the event of a third party's cyber-attack), such as: limitation of liability, indemnification, audit rights, and representations to comply with various cybersecurity and privacy requirements. Associated diligence and oversight of third parties, as part of a third-party risk management program, can also help mitigate risk in this regard. HSCC has published Model Contract Language specific to medtech cybersecurity that can serve as a reference (subject to customization and your counsel's advice).
- **Cyber insurance:** As discussed in the May 2022 405(d) Post, cyber insurance provides an opportunity to transfer some monetary risk from a cyber-attack.
- **Law enforcement relationships and cooperation:** By building a proactive relationship with law enforcement, entities can be better prepared to coordinate with them in the event of a cyber-attack; cooperation with law enforcement can be a factor in various legal considerations.
- **Cyber Hygiene:** In addition to guidance such as the HICP practices for small health care organizations and medium to large organizations, CISA offers a number of technical hygiene services and resources.

Many cyber-attacks will involve legal counsel (both in-house and at outside firms). Courts increasingly scrutinize the application of privilege protections to documents and information related to incident response efforts, particularly post-incident forensic reports. Without these protections, the report may be used as Exhibit A in any litigation or enforcement action. Therefore, entities are well advised to have legal counsel help shape their incident response program in a manner that considers the various legal implications and role of legal counsel in key workstreams, from upfront planning, the containment and investigation of a cyber-attack, and any follow-up obligations.

For more information on the legal implications of a cyber-attack, join our September Spotlight Webinar on September 21st at 1PM EDT to hear from Dan, Cindi and Paul do a further deep dive. Register on the main page of our website: 405d.hhs.gov.

6 Encrypted backups, to make them more resilient for recovery in the event of a ransomware event, also can be the difference from a quick recovery and prolonged downtime.

HICP in the Spotlight

Cybersecurity Policies for Small Healthcare Organizations

Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective means of preventing cyberattacks. They set expectations and foster a consistent adoption of behaviors by your workforce. With clearly articulated cybersecurity policies, your employees, contractors, and third-party vendors know which data, applications, systems, and devices they are authorized to access and the consequences of unauthorized access attempts.

Policies are established first and are then supplemented with procedures that enable the policies to be implemented. Policies describe what is expected, and procedures describe how the expectations are met. For example, a policy is established that all users will complete privacy and security training. The policy specifies that training courses will be developed and maintained for both privacy and security, that all users will complete the training, that a particular method will be used to conduct the training, and that specific actions will be taken to address noncompliance with the policy. The policy does not describe how your workforce will complete the training, nor does it identify who will develop the courses. Your procedures provide these details, for example, by clearly stating that privacy and security professionals will develop and release the courses. Additionally, the procedures describe the process to access the training.

Examples of policy templates are provided in Appendix G of the Main document. Policy examples with descriptions and recommended users are listed below:

Policy Name	Description	User Base
Roles and Responsibilities	Describe cybersecurity roles and responsibilities throughout the organization, including who is responsible for implementing security practices, and setting and establishing policy.	• All users
Education and Awareness	Describe the mechanisms by which the workforce will be trained on cybersecurity practices, threats, and mitigations.	• All users • Cybersecurity team
Acceptable Use / Email Use	Describe what actions users are permitted and not permitted to execute, including detailed descriptions of how e-mail will be used to complete work.	• All users
Data Classification	Describe how data will be classified, with usage parameters for each classification. This classification should be in line with Cybersecurity Practice #4.	• All users
Personal Devices	Describe the organization's position on usage of personal devices, also referred to as bring your own device (BYOD). If usage of personal devices is permitted, describe the expectations for how the devices will be managed.	• All users
Laptop, Portable Device, and Remote Use	Describe the policies that relate to mobile device security and how these devices may be used in a remote setting .	• All users • Cybersecurity team
Incident Reporting and Checklist	Describe requirements for users to report suspicious activities in the organization and for the cybersecurity department to manage incident response.	• All users • Cybersecurity team

Using the 405(d) Website to Help Develop or Improve an Organization's Cybersecurity Program

By Frank Ruelas, 405(d) Task Group Member

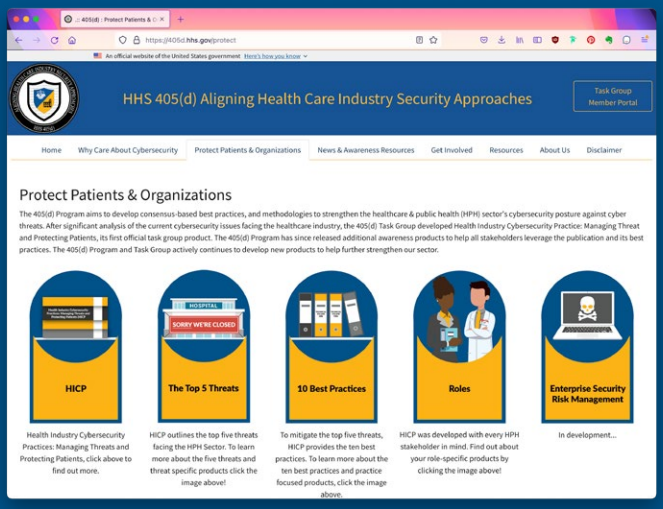
The 405(d) Chronicles is a platform for sharing firsthand insight, lessons learned, and perspectives from cybersecurity professionals in the field today.

It is very likely that most people would agree that the topic of cybersecurity is very likely in their "Top 5" list of important areas of focus and emphasis. As more organizations continue to explore new ways of applying technology in supporting their processes, this also puts a greater emphasis and focus on an organization's practices in developing a strong cybersecurity position to respond to the ever-growing lists of threats that can pose a cybersecurity risk.

When developing the idea of the importance of cybersecurity or promoting a culture that contributes to people developing a commitment to observe cybersecurity practices, it is important that everyone understands that cybersecurity is not the responsibility of the Information Technology or "IT" department. Rather, it is a mutually shared responsibility by everyone within the organization. This is easily said and understood, but how does one go about meeting the challenge of effectively engaging everyone to share in the responsibility of promoting cybersecurity? This is where the 405(d) website and its resources can provide a number of options in answering this question.

Certainly, many members of the organization are actively participating in some type of cybersecurity practices at some level on a regular basis. For example, signing into one's workstation by utilizing a VPN is one way that organization's limit who can access their information systems. So how can the HICP resources build on this level of familiarity that many people already have developed over time? The HICP resources accomplish this by making cybersecurity relatable to the HPH sector in terms of allowing each person in an organization to understand that they have a role to play to protect patients from cyber threats.

Let us start with the idea of raising awareness. By raising awareness, people can develop an idea or sense of why they need to follow certain steps or follow certain



Check out the Protect Patients & Organizations page to learn more about the Top 5 Threats, the 10 Best Practices, and HICP.

procedures related to cybersecurity. For those working in healthcare, the HICP introduces the theme of how managing threats can also help protect patients.[1] Given that one of the prime objectives of healthcare providers is to provide quality care to patients, the idea of protecting patients can help align how promoting cybersecurity is also at the core of what healthcare providers must do in the performance of their jobs. However, what is a good starting point for the organization to focus on when establishing its cybersecurity framework? Again, the HICP resources provide an answer.

Within the HICP resources, there is content that identifies key threats that organizations should focus on. These threats include email phishing, ransomware, the loss or theft of equipment, insider threats, and attacks against connected medical devices.[2] Each of these threats is supplemented by content that can provide cybersecurity planners with practices that can help develop the organization's resistance to falling victim to these

1 https://405d.hhs.gov/protect/hicp
2 https://405d.hhs.gov/protect/topFiveThreats

identified threats. The practices follow the same format as described here with respect to each of the five threats.

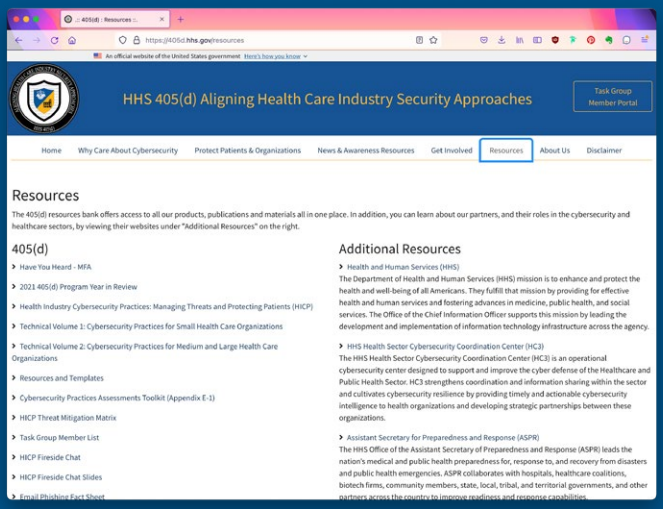
The resources that address each threat include a flyer, threat series slides, and a poster. The flyer explains the threat in a practical, non-technical way that can be used in educational content that the organization may wish to use with its employees. The flyer also provides a real-world scenario which can make the threat relatable and also provides details on how the resources available on the HICP website can help in dealing with the threat.[3] In addition to the flyer, each threat is also broken down and explained by a slide deck presentation. The slide deck presentation explains the threat in more depth. The slide deck is also organized to provide information on mitigating practices related to the threat. These mitigating practices are broken down by organizational size and include references to the HICP Technical Volume where additional information on mitigation strategies can be found.[4] Lastly, each section related to the identified threats includes a poster. The poster provides a visual aid that organizations can post in areas where employees will see them to reinforce and maintain a level of awareness of a particular threat and why it is important to protect against that threat.[5] For example, the poster related to ransomware emphasizes the importance of checking a sender's credentials before opening attachments.

When one considers that each of the key threats identified on the HICP website are supported by content as previously described, one can appreciate just how helpful these resources can be. By having such resources readily available, cybersecurity efforts can be more focused on how to engage those within the organization through training and education without having to spend the time and other resources to develop the content.

When planning what best practices can be used to promote cybersecurity, there is documentation to identify ten best practices that organizations should consider.[6] Similar to the other guidance presented on the HICP website, the content related to best practices also follows a specific format. Each of the best practice documents begins by identifying the best practice which is then followed by what organizations can do to implement and exercise the described best practice. These are also broken down and separated by the size of the organization which can help present the suggested actions within the context of the organization's size.

Perhaps the most significant webpage on the HICP website is its Resources page.[7] This page lists all the resources available on the HICP website and is neatly organized into sections which make it easy to locate the different documents that are available. The 405(d) section lists educational material that relates to the five identified threats. In the 405(d) section the HICP Technical Volumes 1 and 2 are also listed. The HICP technical volumes provide what can be considered some of the most comprehensive descriptions of the identified threats and practices on how to mitigate against these threats. A quick preview of each volume's table of contents can help the cybersecurity professional quickly find and access useful information quickly and easily.

Other sections on the Resource page include listings of newsletters arranged by month and year, copies of slides used in webinars, and general awareness documents with a "how to" focus.



The Resource page includes outreach products, webinars, and nearly all of the products the 405(d) Program has produced to date.

The depth and breadth of the information that the HICP website provides can indeed appear overwhelming. However, by taking time to become familiar with the layout of the HICP website is a wise investment of time. Within minutes, one can become familiar with content that is available which can be used to promote an effective cybersecurity program in a way that is practical, systematic, and efficient.

3 https://405d.hhs.gov/Documents/Five-Threat-Series-Ransomware-R.pdf
4 https://405d.hhs.gov/Documents/5-Threats-Series-Threat-2-Ransomeware-Attack-Powerpoint-Updated-R.pdf
5 https://405d.hhs.gov/Documents/405d-Five-Threats-Ransomware-Poster.pdf
6 https://405d.hhs.gov/protect/tenBestPractices
7 https://405d.hhs.gov/resources

Happening Around Us

CISA Alerts Healthcare Sector to OFFIS DCMTK Cybersecurity Vulnerabilities

Health IT Security released an article on June 27, 2022 explaining concerns that CISA released regarding High-severity cybersecurity vulnerabilities in OFFIS DCMTK software that could result in remote code execution (RCE) if exploited. The Cybersecurity and Infrastructure Security Agency (CISA) warned in a recent advisory that OFFIS recommended that all users update to version 3.6.7 or later as soon as possible.

"It includes software for examining, constructing and converting DICOM image files, handling offline media, sending and receiving images over a network connection, as well as demonstrative image storage and worklist servers," OFFIS states on its website.

It is used by hospitals and companies all over the world for a wide variety of purposes ranging from being a tool for product testing to being a building block for research projects, prototypes and commercial products."

CISA recommended that healthcare organizations take defensive measures to mitigate risks associated with these vulnerabilities. Specifically, all users should isolate control system networks and remote devices from the business network and put them behind firewalls. Additionally, users should minimize network exposure for all control system devices and use Virtual Private Networks (VPNs) when remote access is required.

"CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures," CISA emphasized.

You can read the entire article here.

FDA Urges Healthcare to Patch Severe Illumina Cybersecurity Vulnerabilities

The US Food and Drug Administration (FDA) urged healthcare organizations to immediately patch severe cybersecurity vulnerabilities impacting certain Illumina medical devices. The vulnerabilities impact some Illumina In Vitro Diagnostic devices that run on Local Run Manager (LRM) software.

If exploited, an unauthorized user could take control of the instrument remotely, alter settings, configurations, and data on the customer's network, or impact patient test results by causing the instruments to produce no results, incorrect results, or altered results, the FDA stated. At the time of publication, the FDA and Illumina had not received any reports of exploitation relating to these vulnerabilities.

"These instruments are medical devices that may be specified either for clinical diagnostic use in sequencing a person's DNA or testing for various genetic conditions, or for research use only (RUO). Some of these instruments have a dual boot mode that allows a user to operate them in either clinical diagnostic mode or RUO mode," the FDA noted.

You can read the entire article here.

2 Million Patients' Data Exposed in Cyberattack on New England Health Services Provider

Two million patients in New England who received care at almost 60 healthcare facilities affiliated with Shields Health Care Group, a medical imaging and outpatient surgical services provider, may have had their personal data exposed in a cyberattack earlier this year.

An "unknown actor" gained access to Shields' systems from March 7 to March 21. On March 28, Shields was alerted to suspicious activity and a subsequent investigation into the incident found that "certain data was acquired by the unknown actor within that time frame," according to Massachusetts-based Shields.

The attack is the largest so far this year, according to the HHS' data breach portal.

Read the full article here.

Recent Federal Resources

HC3

- Strengthening Cyber Posture in Healthcare
- The Return of Emotet
- Ransomware Trends Q1 2022

OCR

- HHS Issues Guidance on HIPAA Audio Telehealth

CISA

- CISA, FBI, and Treasury Release Advisory on North Korea State-Sponsored Cyber Actors Use of Maui Ransomware
- CISA Releases Second Version of Guidance for Secure Mitigation to the Cloud
- CISA Launches "More Than a Password" in new Social Media Campaign

Upcoming 405(d) Spotlight Webinar

Topic: The legal Implications of a Cyber Attack

When: September 21st at 1pm EDT

Register: On our website- 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. The news articles are not an endorsement of any product/viewpoint/entity. Use of this document is neither required by nor guarantees compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all health care providers and organizations.

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

Follow us!

Facebook Twitter

Instagram LinkedIn

Visit our website at 405d.hhs.gov!