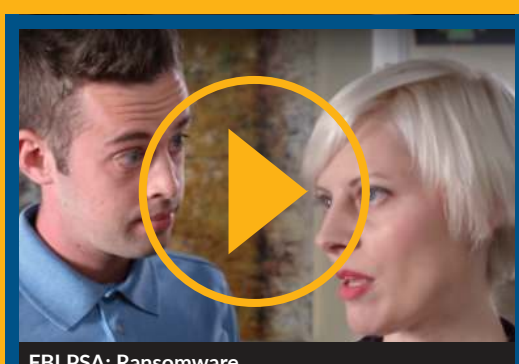
HAVE YOU HEARD ABOUT RANSOMWARE?

What is Ransomware?

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key.



FBI PSA: Ransomware

Public service announcement warning of the dangers of ransomware and how to avoid them.

Healthcare is targeted more than any other industry

Source: Cylance Threat Report (2018)

~50% of all ransomware attacks in the last year targeted North America
McAfee Labs Threats Report (2019)

1 in 4 healthcare organizations are successfully **attacked by ransomware**
Kaspersky Cyber Pulse: The State of Cybersecurity in Healthcare (2018)

88% of all ransomware attacks target the **HEALTHCARE INDUSTRY**
Solutionary Security Engineering Research Team (Q2, 2016)

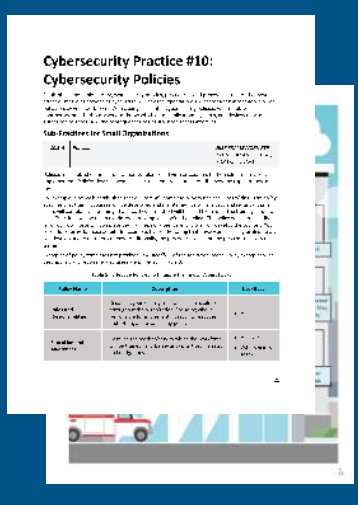
Ransomware attacks **TRIPLED** in 2017

Source: Cylance Threat Report (2018)

HEALTH INDUSTRY CYBERSECURITY PRACTICES:

Managing Threats and Protecting Patients

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication aims to raise awareness, provide vetted cybersecurity practices, and moves toward consistency in mitigating the current most pertinent cybersecurity threats to the sector. The main document examines cybersecurity threats and vulnerabilities that affect the health industry. Technical volumes 1 & 2 discuss ten cybersecurity practices for small, medium and large healthcare organiztions. Lastly the resources and templates volume provides additional cybersecurity resources and references. **CLICK HERE TO ACCESS THESE DOCUMENTS.**



LOOKING FOR MORE TELEHEALTH CYBERSECURITY INFORMATION?

Check Out The Below Resources From Across HHS and HSCC Partners!

HHS - 405(d) Aligning Health Care Industry Security Approaches

405(d) aims to enhance cybersecurity and align industry/sector approaches by developing best practices and mitigation strategies to attack the most common cyber threats facing the healthcare sector. One of the threats covered in the HICP publication is ransomware. The 405(d) initiative develops a variety of resources that can help HPH organizations mitigate cyber-risks.

RESOURCES

- Ransomware Spotlight Webinar
- HICP

HC3 - Health Sector Cybersecurity Coordination Center

The Health Sector Cybersecurity Coordination Center (HC3) provides recommendations and mitigation strategies for protecting the sector against cyber threats, especially threats that impact patient safety, security, and privacy, including ransomware. For more information please email HC3@hhs.gov.

RESOURCES

- Ransomware Briefing
- Aggressive Ransomware Impacts

HHS - Office for Civil Rights

The HHS Office for Civil Rights (OCR) is expanding the capabilities of the Healthcare and Public Health sector's to offer telehealth to patients during unprecedented time. OCR has exercised its enforcement discretion and will waive penalties for HIPAA violations against providers that serve patients via telehealth. As this new policy is being put in place, OCR has released an FAQ sheet to provide guidance on telehealth remote communications.

RESOURCES

- Ransomware Fact Sheet
- Cyber Attack Checklist
- Cyber-Attack Response Infographic

DHS - Cybersecurity and Infrastructure Security Agency

The Cybersecurity and Infrastructure Security Agency (CISA) encourages organizations to adopt a heightened state of cybersecurity during this unprecedented time. As Healthcare Organizations move more towards telework and telehealth procedures they should implement an enterprise virtual private network (VPN) solution to connect their employees to their organization's IT network. CISA has detailed out cybersecurity considerations and mitigation recommendations when moving to a telework or telehealth environment

RESOURCES

- CISA Insights Ransomware Outbreak
- Safeguard Against Ransomware Recommendation

NIST - National Institute of Standards 23 and Technology

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards 23 and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and 24 academic institutions work together to address businesses' most pressing cybersecurity issues. NCCoE at NIST along with vendors and businesses within the cyber security community teamed up to develop a series of practices guides for firms hit with ransomware attacks.

RESOURCES

- Data Integrity Publication
- Guide for Cybersecurity Event Recovery
- Identifying and Protecting Assets Against Ransomware and Other Destructive Events
- Detecting and Responding to Ransomware and Other Destructive Events
- Recovering from Ransomware and Other Destructive Events

PROTECTED VOICES

Looking for a few mitigation practices? Check out the video from the FBI covering a few mitigation practices to help protect organizations from a ransomware attack. Looking for more information on these mitigation practices and others? Check out 405(d)'s HICP publication!

HHS 405(d)
Aligning Health Care Industry Security Approaches

FIND US @ask405d
Visit us at405d.hhs.gov!

The Have You Heard Campaign is brought to you by the 405(d) Program which aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. The Have You Heard Campaign spotlights various topics and provides the HPH sector with different resources from across HHS and the federal government. These emails are meant to be for general awareness.