Transcript: Ransomware Video

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Imagine this: A small town's family medical practice is unable to treat its patients after being locked out of patient records, appointment schedules, and payment information. Cyber attackers have taken control of all systems and encrypted the data.

The threat actors demand $7,000 for the key to decrypt the files or they will delete all of the data. After consulting with the proper authorities, the practice makes the tough decision not to pay the ransom.

In this example, the practice experienced a ransomware attack in which a type of malicious software, better known as malware, encrypted their data and prevented their access until they paid the ransom.

Ransomware incidents can severely impact business processes and leave healthcare organizations of all sizes without the data they need to operate mission-critical services and continue delivering care.

In healthcare our business is caring for people. In many cases, care must be timely for the safety of the patient.

Because of this, the healthcare industry is considered a data rich industry and frequently targeted by threat actors.

Threat actors often pressure victims into payment by threatening to release stolen data if they refuse to pay. They also publicly name and shame victims as a secondary form of extortion.

This can lead to impacts such as loss of access to records, diversion of care to other hospitals, tarnished company reputation, interrupted workflow and communications, credit monitoring for affected patients, and acquiring additional cyber insurance.

Ransomware attacks are expected to happen more and more often in the years to come.

So, how can you be proactive in preventing and responding to ransomware attacks against your organization?

You can:

Use strong and unique usernames and passwords, and implement multi-factor authentication;

Maintain a complete and updated inventory of assets;

Implement a backup strategy and secure the backups so they are not accessible on the network they are backing up;

And develop a ransomware recovery playbook and test it regularly.

The best way to prevent a ransomware attack is to maintain consistent communication with your organization's IT or cybersecurity professionals, and to implement up-to-date cybersecurity policies.

The Department of Health and Human Services, or HHS for short, and the public-private partnership known as 405(d) are committed to aligning health industry cybersecurity approaches by creating, managing, and leading all industry-led processes to develop consensus-based, industry tested guidelines, practices, and methodologies to strengthen the health sector's cybersecurity posture against cyber threats like ransomware.

Ransomware is one of the five threats identified in the HHS 405(d) publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), which aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector.

Each individual threat discussed in the HICP publication provides threat specific mitigation practices, such as those provided earlier.

Additionally, the HHS 405(d) Program has more resources like other publications, awareness products, and outreach-focused social media platforms and events to keep your organization cyber safe, which keeps your patients safe.

No matter what role you serve in your organization, the 405(d) website at 405d.hhs.gov has resources to help you protect your organization and its patients from cyber threats.

As healthcare industry professionals, the best way for us to stay vigilant is for everyone, including you, to play a part and remember that Cyber Safety is Patient Safety.

Produced by the U.S. Department of Health and Human Services at Taxpayer expense.