Access the entire webinar series here:
https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-preparedness-considerations-speaker-series-summary.pdf

Access this recording here: https://attendee.gotowebinar.com/recording/3749129476175342175

TRACIE
HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

Healthcare System Preparedness Considerations Speaker Series

ASPR
Administration for Strategic Preparedness and Response

Cybersecurity Incident Response Preparedness
Rahul Gaitonde, Branch Chief, HC3

Rahul Gaitonde is the Branch Chief of the Health Sector Cybersecurity Coordination Center (HC3), a U.S. Department of Health and Human Services (HHS) group working to improve cybersecurity in the healthcare and public health sector through information sharing and coordination. Prior to joining HHS, Mr. Gaitonde spent 9 years in government consulting supporting the Departments of Health and Human Services and Homeland Security.

Cybersecurity Incident Response Preparedness

September 27, 2023

HC3 History & Mission

- The **Health Sector Cybersecurity Coordination Center (HC3)** was established in response to the Cybersecurity Information Sharing Act of 2015. A federal law mandated to "improve the cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats, and for other purposes."

- HC3's mission is to support the defense of the healthcare and public health sector's information technology infrastructure, by strengthening coordination and information sharing within the sector and by cultivating cybersecurity resilience, regardless of organizations' technical capacity.

- HC3 provides objective information to the health and public health sector.

Agenda

- Cyber Threats Impacting HPH Operations
- Cyber Incident Response (IR) Planning
- Recommendations & Best Practices
- Resources

Threats to the HPH Sector

Cyber Threat Actors

- Malicious groups or individuals who aim to exploit weaknesses in an information system, or to exploit its operators to gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks
- Cyber threat actors pursue their objectives by exploiting technical vulnerabilities, using social engineering, and by creating, disseminating, or amplifying false or misleading content online to influence individuals' behavior and beliefs
- Health Sector is targeted because of the valuable data and ease of network intrusion
- Threat Actors have a financial impact on:
  - **Customers/Patients:**
    - Hackers can make use of the stolen data for identity theft, financial gain, targeted blackmailing, and insurance fraud
    - If the hackers don't make use of the information themselves, they can make a profit off it on cybercriminal forums
  - **Healthcare Entities:**
    - Financial burden
    - Legal ramifications
    - Reputational damage

Top Cyber Threats

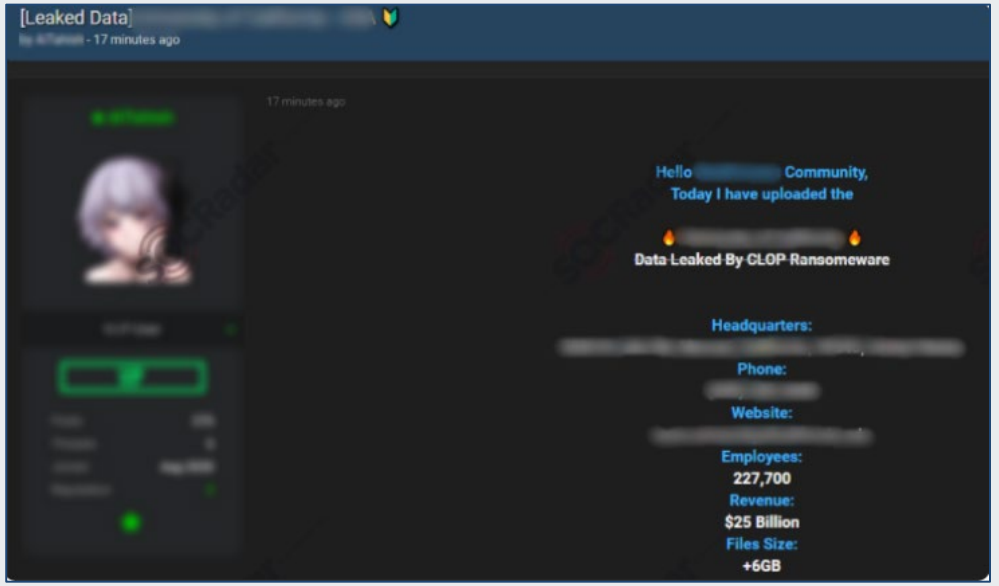
- **Ransomware:** Malicious software that restricts access to or operation of a computer or device, restoring it following payment
- **Phishing:** Mainly conducted through email spoofing and text messages, a common method by which threat actors disguise themselves as a trustworthy entity with the intent to lure many recipients into providing information such as login credentials, banking information, and other personally identifiable information
- **Business Email Compromise (BEC):** Emails designed to trick an employee of the target organization into directly providing PII, credentials, etc. to cyber threat actors
- **Distributed Denial of Service (DDoS):** A DoS attack that originates from numerous machines at once; can be controlled by a group of threat actors working together or be part of a botnet acting under the direction of a single threat actor
- **Botnet:** A group of compromised devices that are coordinated by a threat actor; can be used for distributed denial of service (DDoS), spreading ransomware and malware, sending spam, diverting traffic, stealing data, and/or more
- **Zero-day Vulnerability**: A vulnerability that is not yet known by the vendor, and therefore has not been mitigated by a patch; Zero-day Exploit: An attack directed at a zero-day vulnerability

Rhysida

- Rhysida emerged in May 2023
- The group drops an eponymous ransomware via phishing attacks and Cobalt Strike to breach targets' networks and deploy their payloads
- The group threatens to publicly distribute the exfiltrated data if the ransom is not paid. Rhysida is still in early stages of development, as indicated by the lack of advanced features and the program name Rhysida-0.1
- The ransomware also leaves PDF notes on the affected folders, instructing the victims to contact the group via their portal and pay in Bitcoin.
- Its victims are distributed throughout several countries across Western Europe, North and South America, and Australia
- They primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector
- ***Related HC3 Products***: 202308041500 Rhysida

ClOp

- Russia-linked ransomware group
- First observed in February 2019
- Mostly targets Windows systems, but also Linux servers
- Known to target organizations with a revenue of $5 million U.S. Dollars (USD) or higher. Operators have seen payouts of up to $500 million USD
- **Notable Victims:** Microsoft; also claimed responsibility for a mass attack on more than 130 organizations, including those in the healthcare industry
- ***Related HC3 Products***: ClOp Allegedly Targets Healthcare Industry in Data Breach; Clop Ransomware



An alleged database leaked by ClOp is detected in a hacker forum monitored by SOCRadar.
Source: SOCRadar

Nation State Actors

- Nation state actors sponsor threat groups that launch attacks against foreign governments and organizations to advance their geopolitical objectives
- Frequently the most sophisticated threat actors, with dedicated resources and personnel, and extensive planning and coordination
  - Designated as an APT, or an Advanced Persistent Threat
  - APTs are considered capable of composing and executing state-of-the-art attacks using the most modern malware-obscuring techniques
- The activities of state-sponsored cyber threat actors include:
  - Espionage against governments, organizations, and individuals
  - Disrupting critical systems
  - Influencing and shaping public discourse
  - Building networks of compromised devices to enable further cyber threat activity
  - May also pursue financially motivated threat activity

Insider Threats

An insider threat in the Healthcare and Public Health (HPH) sector is a person within a healthcare organization, or a contractor, who has access to assets or inside information concerning the organization's security practices, data, and computer systems. The person could use this information in a way that negatively impacts the organization. There are several types of insider threats within an organization, all with different goals. Some insider threats are as follows:

- Careless or negligent workers
- Malicious insiders
- Inside agents
- Disgruntled employees
- Third parties

Planning and Exercising

Effective Incident Response Requires Planning

- Organizations should include cyber incidents as part of the wider all hazards response planning.

- A comprehensive incident response plan should include:
  - Key personnel with Roles and Responsibilities along with back ups
  - Decision matrixes to determine system importance and recovery order
  - Points of Contact information for FBI, CISA, Regional Health Reps, Cyber Insurance
  - A basic communications plan

- Conduct a tabletop exercise to ensure that all participants understand their roles during an incident

- Regularly test the plan during various shifts and with the inclusion of back up staff

Incident Response Stakeholders

- The Information Security Office (ISO), which coordinates the response and is led by the Chief Information Security Officer (CISO), who serves as the Incident Commander
- Chief Medical Officer, which serves as the SME for all medical related issues and provides guidance on the importance of systems
- The IT Services, which provide technical support and assistance to the incident response team
- The Security Management, which oversees the security policies and procedures and provides guidance and oversight to the incident response team
- The Legal Counsel, which advises on the legal implications and obligations of the incident, such as compliance, liability, and disclosure
- The Human Resources, which handles the personnel issues related to the incident, such as user awareness, training, disciplinary actions, and employee assistance
- The Public Relations, which manages the communication with the media, customers, partners, and other stakeholders about the incident
- The Data Stewards, which are responsible for the protection and integrity of the data affected by the incident

Key Steps to Incident Response

- Preparation: Establish roles and responsibilities, policies and procedures, tools and resources, training and awareness, and communication channels for incident response
- Identify the Threat: Monitor and analyze network activity, identify potential threats, verify incidents, and assess their scope and impact
- Contain: Isolate affected systems, networks, or devices to prevent further damage or spread of the incident
- Removal: Remove malicious or compromised elements from the environment, restore normal operations, and verify system integrity
- Restoration: Recover data and functionality from backups or other sources, test and validate systems, and resume normal operations
- After Action: Analyze the incident, identify root causes, lessons learned, best practices, gaps, and weaknesses, and document findings and recommendations

Incident Response Communications

- Develop templates for communications prior to the incident for common responses therefore allowing the responses to be properly vetted by key staff
- Assume that any communications being distributed to staff will also become public
- Coordinate and collaborate with other relevant entities, such as law enforcement, regulators, media, and industry partners
- Provide timely, accurate, consistent, and transparent information to the stakeholders
- Tailor the messages to the specific audiences and situations
- Use clear, concise, and simple language that avoids technical jargon and acronyms
- Follow up with the stakeholders after the incident to provide updates, feedback, lessons learned, and recommendations

Key Considerations of Tabletop Exercise Planning and Execution

- **Purpose/Objectives:** To test and improve the organization's readiness and response to cyber incidents by evaluating various aspects of their protocols and plans
- **Exercise Format:** A facilitated discussion and simulation of a realistic cyber scenario, where participants analyze and discuss how they would respond
- **Scenario Development:** A realistic and challenging cyber crisis that tests the organization's response and coordination capabilities, designed by a separate team from the participants
- **Participants:** Key stakeholders from various departments within the healthcare organization, as well as subordinate employees, who have roles and responsibilities in responding to cyber incidents
- **Roles and Responsibilities:** Specific roles assigned to each participant, such as crisis manager, performance evaluator, emergency coordination specialist, or operational and tactical personnel, or observer
- **Documentation:** Essential documents and resources that participants need to access and use during the exercise, such as emergency response plans, contact lists, communication protocols, incident reporting forms, technical resources, recovery procedures, legal and regulatory requirements, and training materials
- **Evaluation Criteria:** Measures of performance during the exercise, such as response times, decision-making effectiveness, communication skills, overall coordination, or problem identification
- **After-Action Review:** A process to assess performance and identify areas for improvement based on evaluation criteria and unexpected events during the exercise
- **Training and Preparation:** Training and awareness initiatives to enhance staff knowledge of cybersecurity best practices and response protocols before the exercise

Resources

Free Services to Conduct TTX

- Tabletop Exercise (TTX) Templates:
  - Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Tabletop Exercise Package
  - Centers for Medicare & Medicaid Services Tabletop Exercise Template
  - California Association of Health Facilities Disaster Planning Guide
  - State of Oregon Tabletop Exercise Facilitator Handbook Template
- Web-based Simulation Tools:
  - EPA's Cybersecurity Tabletop Exercise Tool for Drinking Water and Wastewater Utilities
  - TTX scenarios provided by the Center for Internet Security
- Exercise Training and Evaluation Programs:
  - DHS Cyber Tabletop Exercise for the Healthcare Industry
- Tabletop Exercise Services:
  - CISA National Cyber Exercise Program, exercises planned and conducted by DHS-CISA, or by interested parties in collaboration with DHS-CISA.

HC3 and Partner Resources

Health Sector Cybersecurity Coordination Center (HC3)

- HC3 Products

405(D) Program and Task Group

- 405(D) Resources
- 405(D) Health Industry Cybersecurity Practices

Food and Drug Administration (FDA)

- FDA Cybersecurity

Cybersecurity and Infrastructure Security Agency (CISA)

- CISA Stop Ransomware
- CISA Free Cybersecurity Tools
- CISA Current Activity
- CISA Incident Reporting

Federal Bureau of Investigation (FBI)

- FBI Cybercrime
- FBI Internet Crime Complaint Center (IC3)
- FBI Ransomware

Health Sector Coordinating Council (HSCC)

- HSCC Recommended Cybersecurity Practices
- HSCC Resources

Health – Information Sharing and Analysis Center (H-ISAC)

- H-ISAC Threat Intelligence: H-ISAC Hacking Healthcare
- H-ISAC White Papers

Contact ASPR TRACIE

asprtracie.hhs.gov

1-844-5-TRACIE

askasprtracie@hhs.gov