405(d) Program Presents:
2021 Cyber Threat Review

Aligning Health Care Industry Security Approaches

- **Nick Rodriguez-** 405(d) Program Manager at the U.S. Department of Health and Human Services (HHS)
- **Rahul Gaitonde-** Acting Branch Chief, Health Sector Cybersecurity Coordination Center (HC3)

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) Task Group member; each iteration does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute this webinar series.

- This Webinar is being recorded and will be available for future viewing
- A note for media: While this event is open to the public, we would like to direct any media representatives to contact the public affairs office of whichever representative you have questions for to receive an official statement on behalf of the organization and refrain from quoting panelists during this event directly.

405(d) Events and Announcements

- **January**
  - 405(d) Post Volume XIV Releases 1/21

- **February**
  - Spotlight Webinar! Date, Time, Topic TBD

New 405(d) website launched last week!
Find all our resources at https://405d.hhs.gov

Email: CISA405d@hhs.gov

Social Media: @Ask405d LinkedIn, Twitter, Facebook, Instagram

Agenda

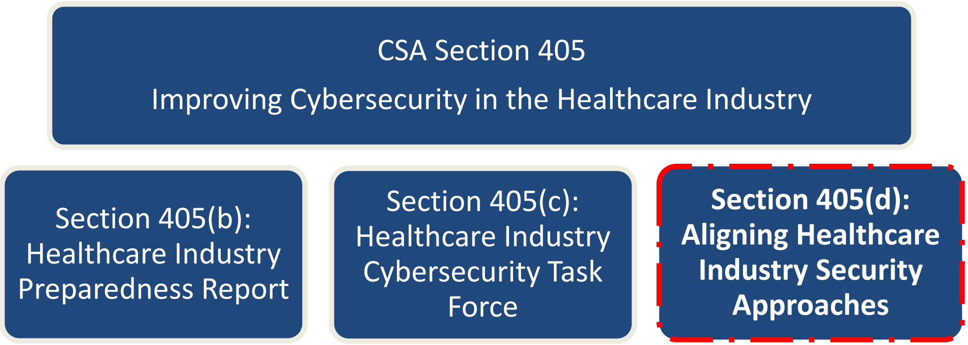
Time	Topic	Speaker
5 minutes	Opening Remarks and Introductions	Nick Rodriguez, 405(d) Program Manager
25 Minutes	2021 Year in Review	Rahul Gaitonde, HC3 Branch Manager
10 Minutes	405(d) Resources	Nick Rodriguez, 405(d) Program Manager
15 Minutes	Q&A	Rahul Gaitonde, HC3 Branch Manager and Nick Rodriguez, 405(d) Program Manager
5 Minutes	Closing	405(d) Team

Cybersecurity Act of 2015: Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of "Aligning Health Industry Security Approaches" by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !



CSA Section 405

Improving Cybersecurity in the Healthcare Industry

Section 405(b): Healthcare Industry Preparedness Report

Section 405(c): Healthcare Industry Cybersecurity Task Force

Section 405(d): Aligning Healthcare Industry Security Approaches

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

2021 Year in Review

12/08/2021

TLP: WHITE, ID# ***202112081300***

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

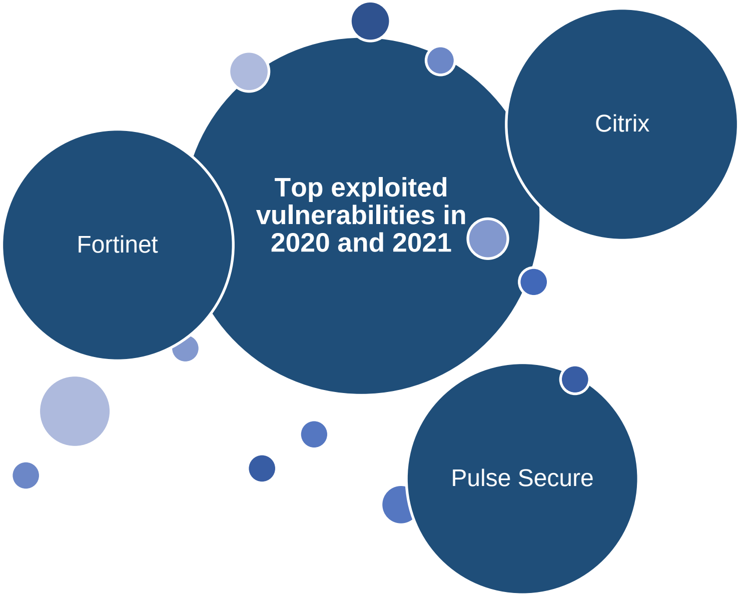
Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Executive Summary: 2021 Cybersecurity Trends

650% The percentage that supply chain attacks have increased by in the last year

82% The percentage of healthcare systems that reported a cyber attack in the past 18 months



The percentage of those attacks that involved ransomware **34%**

133 The number of healthcare entities **in the U.S.** that appeared on a ransomware extortion blog

210 The number of healthcare entities **globally** that appeared on a ransomware extortion blog

Increased Exploitation of VPN Products Highlight Difficulties with Telehealth and Secure Patient Data

2021 Trends

- APT and financially-motivated actors exploiting various vulnerabilities in commonly-used VPN products
- Top exploited vulnerabilities in 2020 and 2021 included Citrix, Pulse Secure, and Fortinet

Major Actors

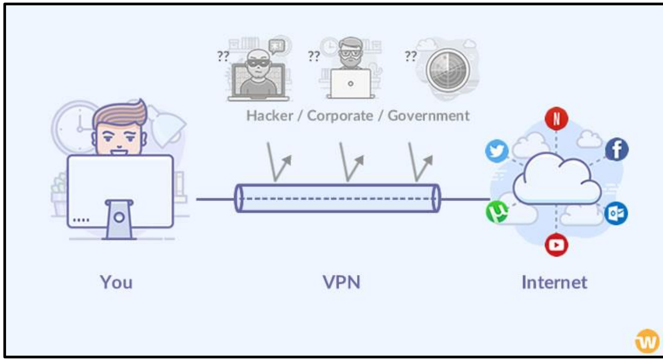
- State-sponsored APT groups exploiting Microsoft Exchange via Fortinet vulnerabilities since March 2021
- Multiple ransomware groups exploiting zero-day in EntroLink VPN appliances since September 2021

Impact to HPH

- Compromised PHI & IP, interruption to patient care, etc.

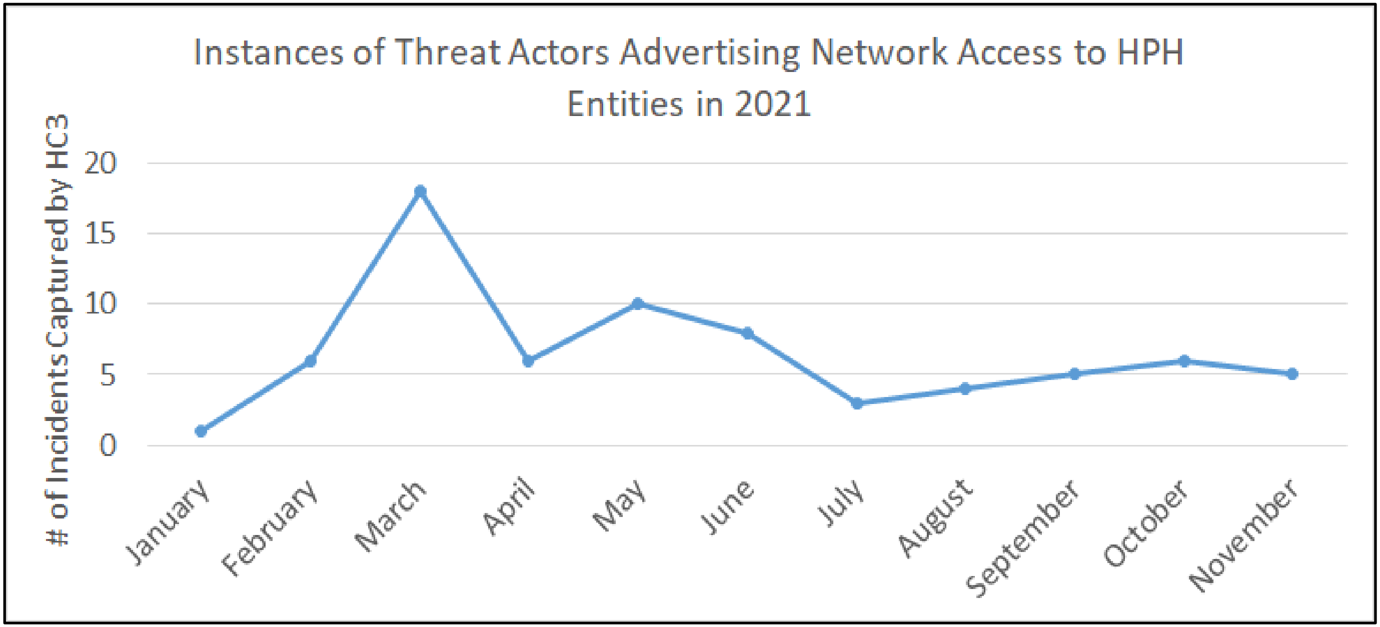
2022 Predictions

- Continued exploitation of newly identified and zero-day vulnerabilities in various VPN products to conduct cyber espionage and financially-motivated follow-on activity, such as ransomware deployment



Increased Exploitation of VPN Products Highlight Difficulties with Telehealth and Secure Patient Data (cont.)

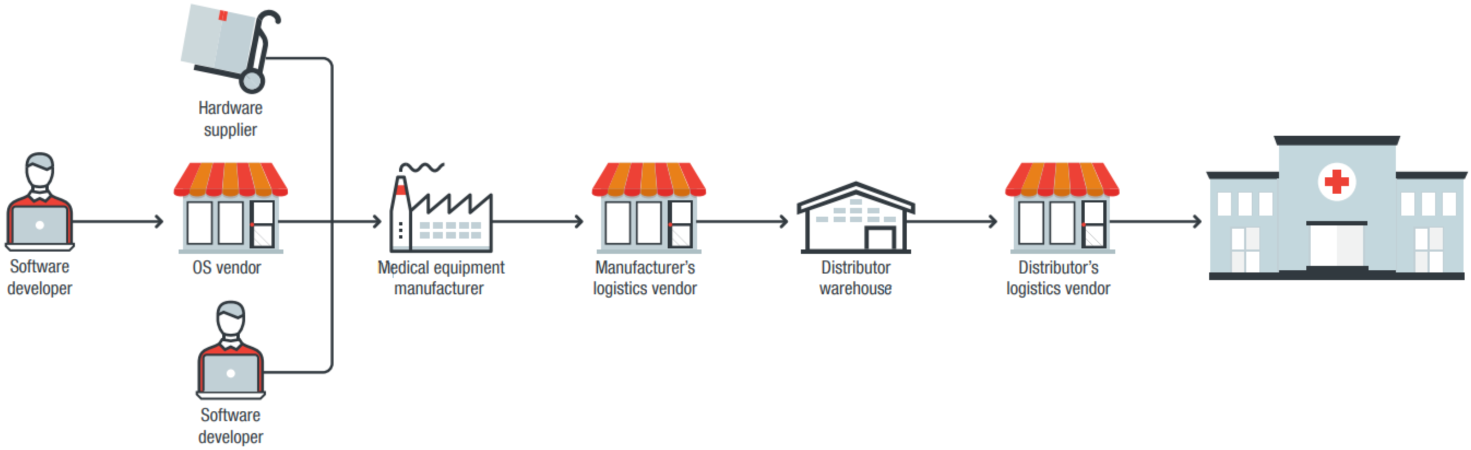
- HC3 tracked at least 75 instances of actors advertising network access to healthcare entities worldwide in 2021 on cybercriminal/hacking forums.
- Data mainly includes public forum posts, although threat actors may conduct transactions privately or via other channels to avoid law enforcement detection, and those instances may not be included below.



Source: HHS/HC3

Successful Supply Chain Attacks Enable Threat Actors to Easily Target Many by Compromising One

- The image below shows a sample supply chain for a modern hospital, from software developers and hardware suppliers, through medical device manufacturers, manufacturer's logistics vendors, distributors, and the distributor's logistics vendor, before making it to the hospital.


Hardware supplier
Software developer
OS vendor
Software developer
Medical equipment manufacturer
Manufacturer's logistics vendor
Distributor warehouse
Distributor's logistics vendor

Successful Supply Chain Attacks Enable Threat Actors to Easily Target Many by Compromising One (cont.)

2021 Trends

- Software supply chain attacks have increased by 650% in the last year
- 58% of supply chain incidents predominantly targeted customer data (i.e. PII, PHI, IP)

Major Actors

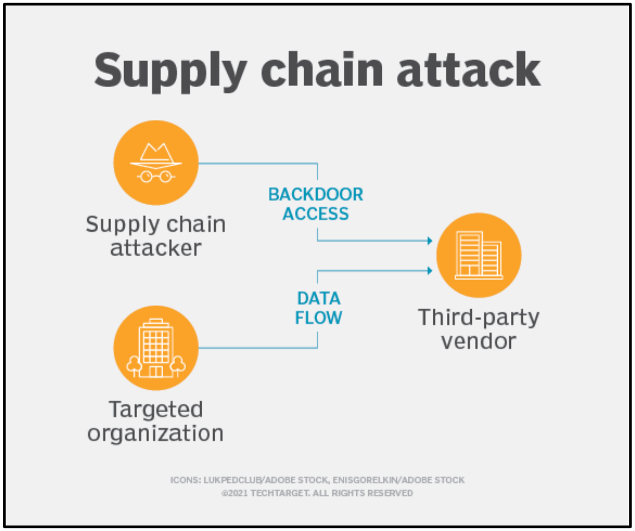
- REvil/Sodinokibi RaaS group exploited zero-day in Kaseya VSA to distribute ransomware to 1,500 victims
- Russian cyberespionage group APT29 exploited a flaw in SolarWinds Orion, impacting 18,000 customers; the flaw was also believed to be exploited by China
- Accellion FTA zero-day attacks exploited by financially-motivated FIN11 and CL0P RaaS group

Impact to HPH

- Hardware (i.e. medical devices) & Software (i.e. EMR supplier, internal portal) Supply Chain Impacts

2022 Predictions

- Supply chain attacks are expected to become more common, with governments establishing regulations to address the issue and protect networks



ICONS: LUKPEDCLUB/ADOBE STOCK, ENISGORELKIN/ADOBE STOCK
©2021 TECHTARGET. ALL RIGHTS RESERVED

Ransomware Pandemic Continues Despite Drastic Law Enforcement Efforts

2021 Trends

- Ransomware is a long-standing problem and a growing national security threat
- 82% of healthcare systems reported a cyber attack in the past 18 months, with 34% involving ransomware
- Healthcare Industry Services organizations were the most impacted by ransomware

Major Actors

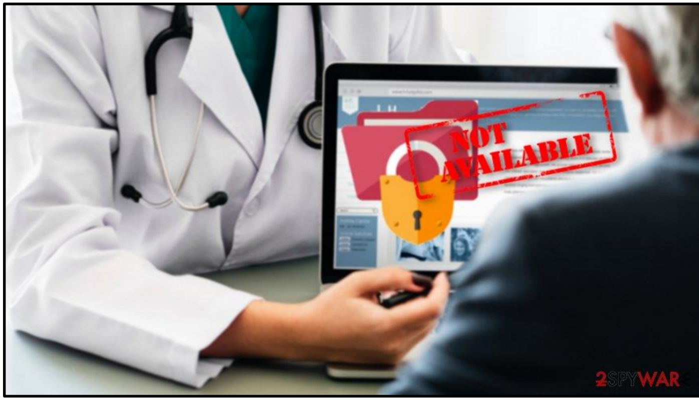
- Conti, Pysa, Avaddon, REvil

Impact to HPH

- Data theft, inaccessible EMR, million-dollar ransoms, and negative impact on patient care

2022 Predictions

- Rebirth of Emotet botnet will likely lead to increased ransomware infections, with development efforts continuing into 2022
- Ransomware-as-a-Service (RaaS) groups are likely to buy and use zero-day vulnerabilities
- APT actors are likely to buy initial network access from cybercriminals, with potential use for ransomware



State-Sponsored Cyber Espionage Campaigns Targeting Pharmaceutical and Vaccine Development

China

- Attacks from Chinese state-sponsored group HAFNIUM on Microsoft Exchange servers impacted over 30,000 organizations, including healthcare entities
- APT41 state-sponsored campaign took advantage of COVID-themed phishing lures to target victims in India

Russia

- October 2021: Russia denied claims that its spies stole a blueprint for the Oxford-AstraZeneca vaccine and used it to create its own Sputnik V shot

Iran

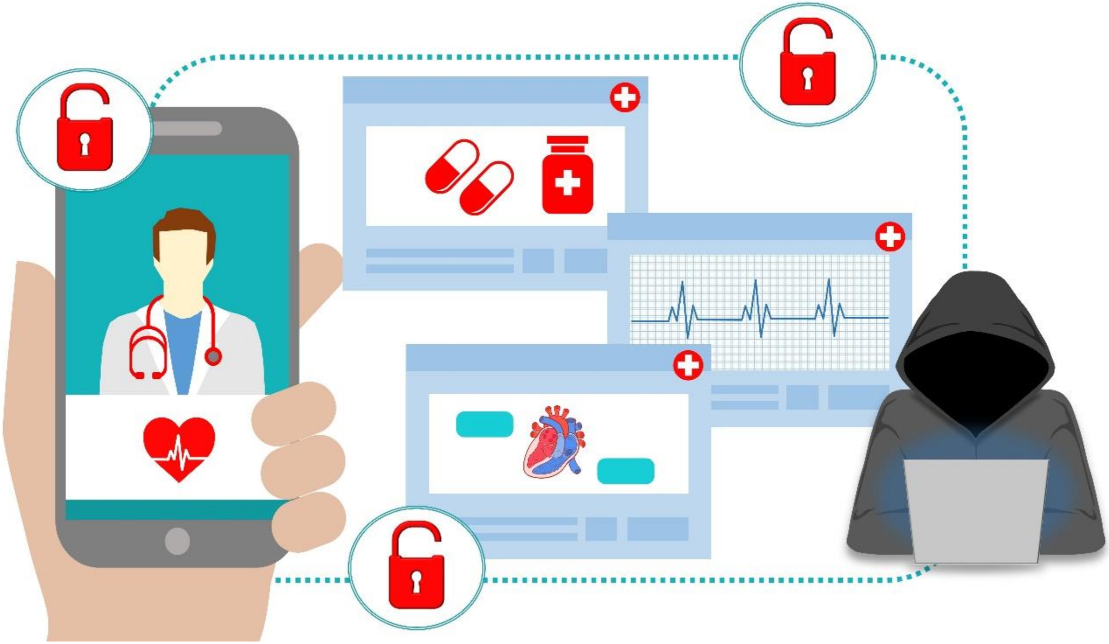
- March 2021: Hackers linked to Iran targeted 25 senior professionals at various medical research organizations located in the U.S. and Israel in weeks-long phishing campaign
- Six Iranian hacking groups capable of executing increasingly sophisticated cyber espionage, destructive and supply chain attacks

North Korea

- HC3 remains cautious of continued indications that North Korea (Lazarus Group) is ceasing focus on healthcare targeting and resuming traditional targeting of the Defense Industrial Base (DIB), think tanks, etc.

Questions

HHS 405(d) Program Resources



Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients

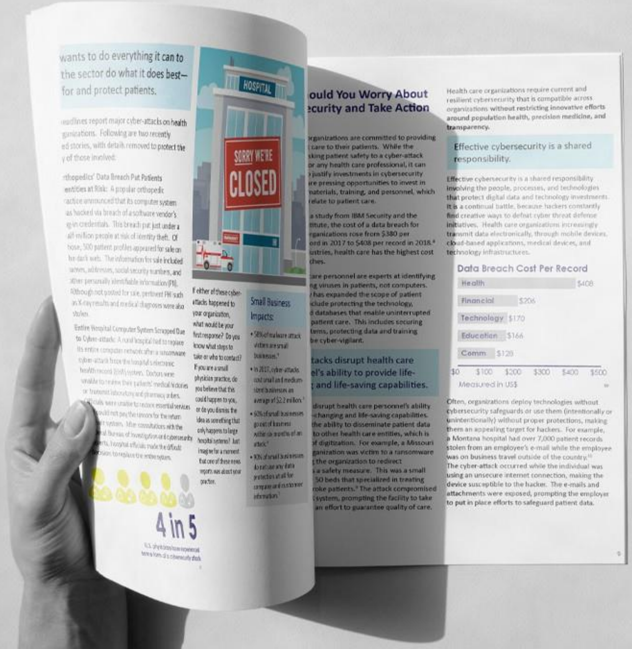
405(d)'s Cornerstone Publication

After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

The **Main Document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

Technical Volume 1 discusses these ten cybersecurity practices for small healthcare organizations.

Technical Volume 2 discusses these ten cybersecurity practices for medium and large healthcare organizations.



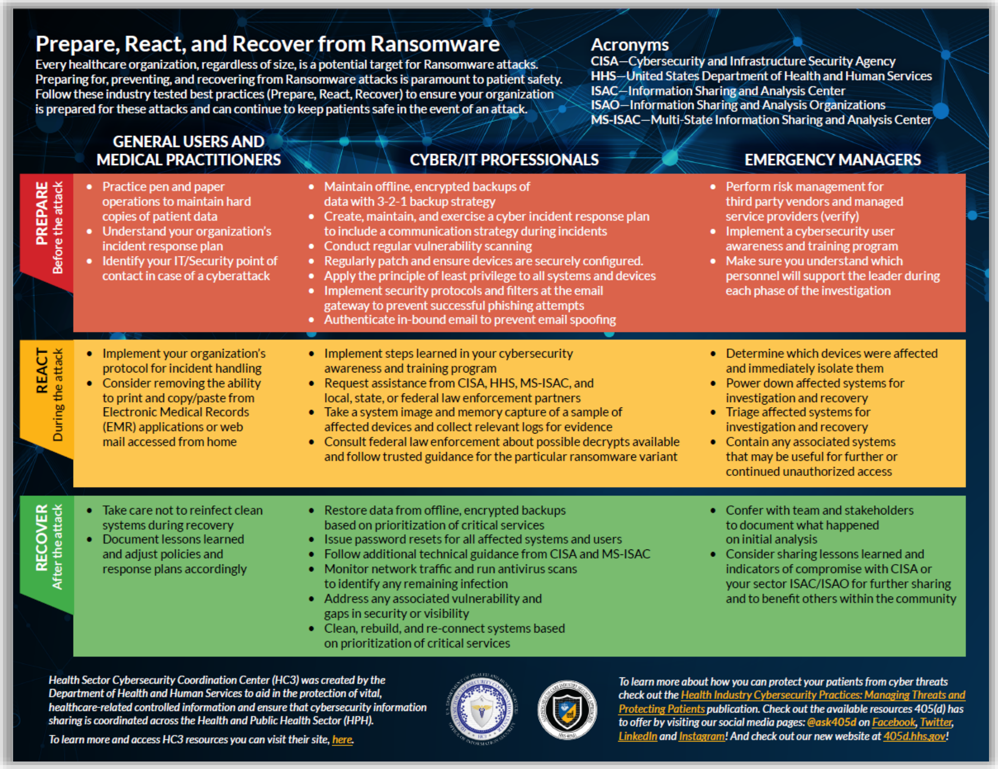
Preventing Ransomware Attacks

The HHS 405(d) HICP Publication provides small and medium/large organizations with mitigating practices to prevent Ransomware attacks. See below for a quick list of mitigating practices you can implement now to prevent Ransomware attacks:

- Social Engineering and Email Phishing Training
- Email Protection Systems / Multi-Factor Authentication
- Endpoint Protection and Asset Management (Computers, Smartphones, Devices)
- Access Management (Unique Accounts, Role-Based Access)
- Network Management (Network Segmentation, Physical Security and Guest Access)
- Incident Response Plan (Back-ups, Downtime Procedures)

Prepare, React, and Recover from Ransomware

Introducing a new resource released today created by the HHS HC3 program and 405(d) Program. Every healthcare organization, regardless of size, is a potential target for Ransomware attacks. Preparing for, preventing, and recovering from Ransomware attacks is paramount to patient safety. Follow these industry tested best practices (Prepare, React, Recover) to ensure your organization is prepared for these attacks and can continue to keep patients safe in the event of an attack.



Prepare, React, and Recover from Ransomware

Every healthcare organization, regardless of size, is a potential target for Ransomware attacks. Preparing for, preventing, and recovering from Ransomware attacks is paramount to patient safety. Follow these industry tested best practices (Prepare, React, Recover) to ensure your organization is prepared for these attacks and can continue to keep patients safe in the event of an attack.

Acronyms

CISA—Cybersecurity and Infrastructure Security Agency
HHS—United States Department of Health and Human Services
ISAC—Information Sharing and Analysis Center
ISAO—Information Sharing and Analysis Organizations
MS-ISAC—Multi-State Information Sharing and Analysis Center

	GENERAL USERS AND MEDICAL PRACTITIONERS	CYBER/IT PROFESSIONALS	EMERGENCY MANAGERS
PREPARE Before the attack	• Practice pen and paper operations to maintain hard copies of patient data • Understand your organization's incident response plan • Identify your IT/Security point of contact in case of a cyberattack	• Maintain offline, encrypted backups of data with 3-2-1 backup strategy • Create, maintain, and exercise a cyber incident response plan to include a communication strategy during incidents • Conduct regular vulnerability scanning • Regularly patch and ensure devices are securely configured. • Apply the principle of least privilege to all systems and devices • Implement security protocols and filters at the email gateway to prevent successful phishing attempts • Authenticate in-bound email to prevent email spoofing	• Perform risk management for third party vendors and managed service providers (verify) • Implement a cybersecurity user awareness and training program • Make sure you understand which personnel will support the leader during each phase of the investigation
REACT During the attack	• Implement your organization's protocol for incident handling • Consider removing the ability to print and copy/paste from Electronic Medical Records (EMR) applications or web mail accessed from home	• Implement steps learned in your cybersecurity awareness and training program • Request assistance from CISA, HHS, MS-ISAC, and local, state, or federal law enforcement partners • Take a system image and memory capture of a sample of affected devices and collect relevant logs for evidence • Consult federal law enforcement about possible decrypts available and follow trusted guidance for the particular ransomware variant	• Determine which devices were affected and immediately isolate them • Power down affected systems for investigation and recovery • Triage affected systems for investigation and recovery • Contain any associated systems that may be useful for further or continued unauthorized access
RECOVER After the attack	• Take care not to reinfect clean systems during recovery • Document lessons learned and adjust policies and response plans accordingly	• Restore data from offline, encrypted backups based on prioritization of critical services • Issue password resets for all affected systems and users • Follow additional technical guidance from CISA and MS-ISAC • Monitor network traffic and run antivirus scans to identify any remaining infection • Address any associated vulnerability and gaps in security or visibility • Clean, rebuild, and re-connect systems based on prioritization of critical services	• Confer with team and stakeholders to document what happened on initial analysis • Consider sharing lessons learned and indicators of compromise with CISA or your sector ISAC/ISAO for further sharing and to benefit others within the community

Health Sector Cybersecurity Coordination Center (HC3) was created by the Department of Health and Human Services to aid in the protection of vital, healthcare-related controlled information and ensure that cybersecurity information sharing is coordinated across the Health and Public Health Sector (HPH).

To learn more and access HC3 resources you can visit their site, here.

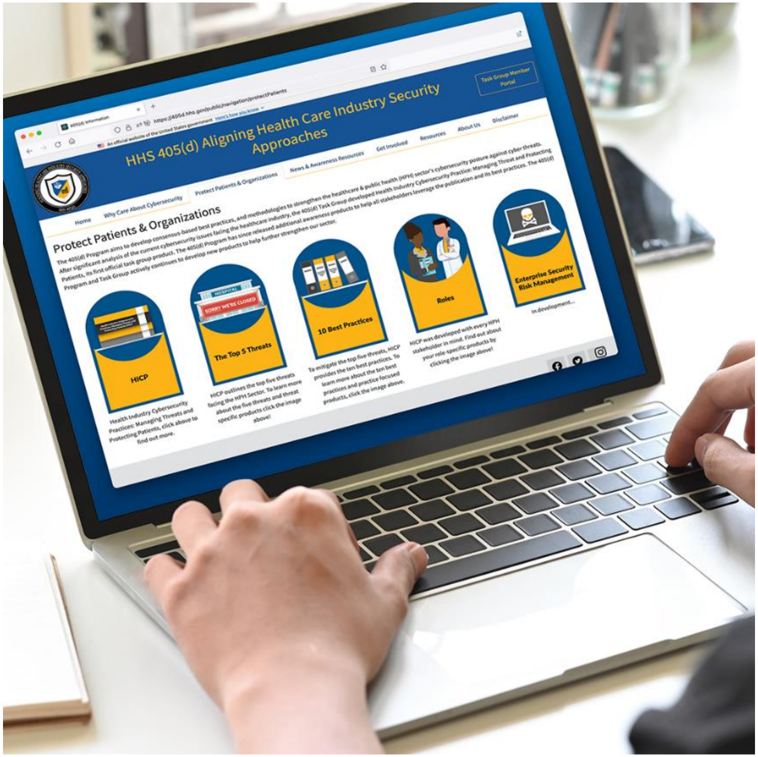
To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram! And check out our new website at 405d.hhs.gov!

HHS 405(d) Website

The New 405(d) Website is now LIVE!!!

On it you will find:

- HICP Publication
- Tips on how to get started with your cybersecurity protection
- 5 Threat Resources
- 10 Practice Resources
- Infographics
- SBARs
- 405(d) Post Editions
- 405(d) Spotlight Webinars
- General Cybersecurity Awareness Resources for your organization!


405(d) Information
https://405d.hhs.gov/public/navigation/protectPatients
An official website of the United States government Here's how you know
HHS 405(d) Aligning Health Care Industry Security Approaches
Task Group Member Portal
Home
Why Care About Cybersecurity
Protect Patients & Organizations
News & Awareness Resources
Get Involved
Resources
About Us
Disclaimer
Protect Patients & Organizations
HOSPITAL
SORRY WE'RE CLOSED
HICP
The Top 5 Threats
10 Best Practices
Roles
Enterprise Security Risk Management
In development...

The 405(d) Program aims to develop consensus-based best practices, and methodologies to strengthen the healthcare & public health (HPH) sector's cybersecurity posture against cyber threats. After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group developed Health Industry Cybersecurity Practice: Managing Threat and Protecting Patients, its first official task group product. The 405(d) Program has since released additional awareness products to help all stakeholders leverage the publication and its best practices. The 405(d) Program and Task Group actively continues to develop new products to help further strengthen our sector.

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, click above to find out more.

HICP outlines the top five threats facing the HPH Sector. To learn more about the five threats and threat specific products click the image above!

To mitigate the top five threats, HICP provides the ten best practices. To learn more about the ten best practices and practice focused products, click the image above.

HICP was developed with every HPH stakeholder in mind. Find out about your role-specific products by clicking the image above!

405(d) Resources

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released over 50 awareness products which organizations across the HPH sector can leverage.

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters, The 405(d) Post, and Spotlight Webinars to increase cybersecurity awareness and present new and emerging cybersecurity news and topics, as well highlight the HICP Publication!

CYBERSECURITY TOWN HALL EVENT

October 22-23

PATIENTS TRUST US WITH THEIR LIVES,
BUT DO WE PROTECT THEM FROM CYBER THREATS?

Join UChicago Medicine and United States Health and Human Services 405(d) to discuss the five main cybersecurity threats facing the healthcare industry and leading practices to mitigate them.

Town Hall Events:
Practitioners and Practice Managers:
10/22/19 1:30pm-3:00pm
10/23/19 9:00am-10:30am

IT Professionals:
10/22/19 3:30pm-5:00pm
10/23/19 11:00am-12:30pm

405(d) Social Media

The 405(d) Program is now live on LinkedIn Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

Guest Webinars

The 405(d) program offers "Guest Webinars" to healthcare organizations where we provide information on the HICP Publication, 405(d) resources, how to engage your co-workers, and more

SBARs

The 405(d) SBAR is a timely, event-oriented document to help healthcare organizations react and relate to current cyber events.

Questions?

Do you follow us on Social Media?
Check us out at **@ask405d**

Linkedin.com/company/hhs-ask405d

https://405d.hhs.gov

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

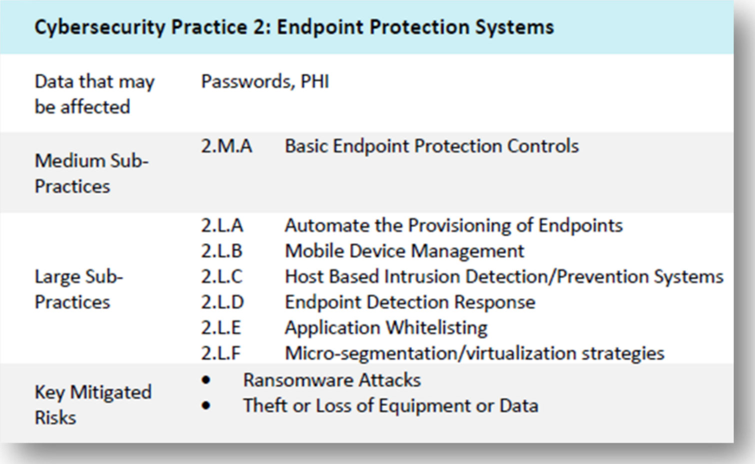
Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

The publication details the top five threats facing the healthcare industry and the ten practices to mitigate. Read the entire publication on our website: https://405d.hhs.gov

Appendix

How to Use Practices and Sub-Practices

- There are a total of **10** Cybersecurity Practices, and **89** Sub-Practices.
- Each Cybersecurity Practice has a corresponding set of Sub-Practices, risks that are mitigated by the Practice, and suggested metrics for measuring the effectiveness of the Practice
- Medium Sized orgs can review the Medium Sub-Practices
- Large Sized orgs can review the Medium **and** Large Sub-Practices
- Each Practice is designed to mitigate one or many threats

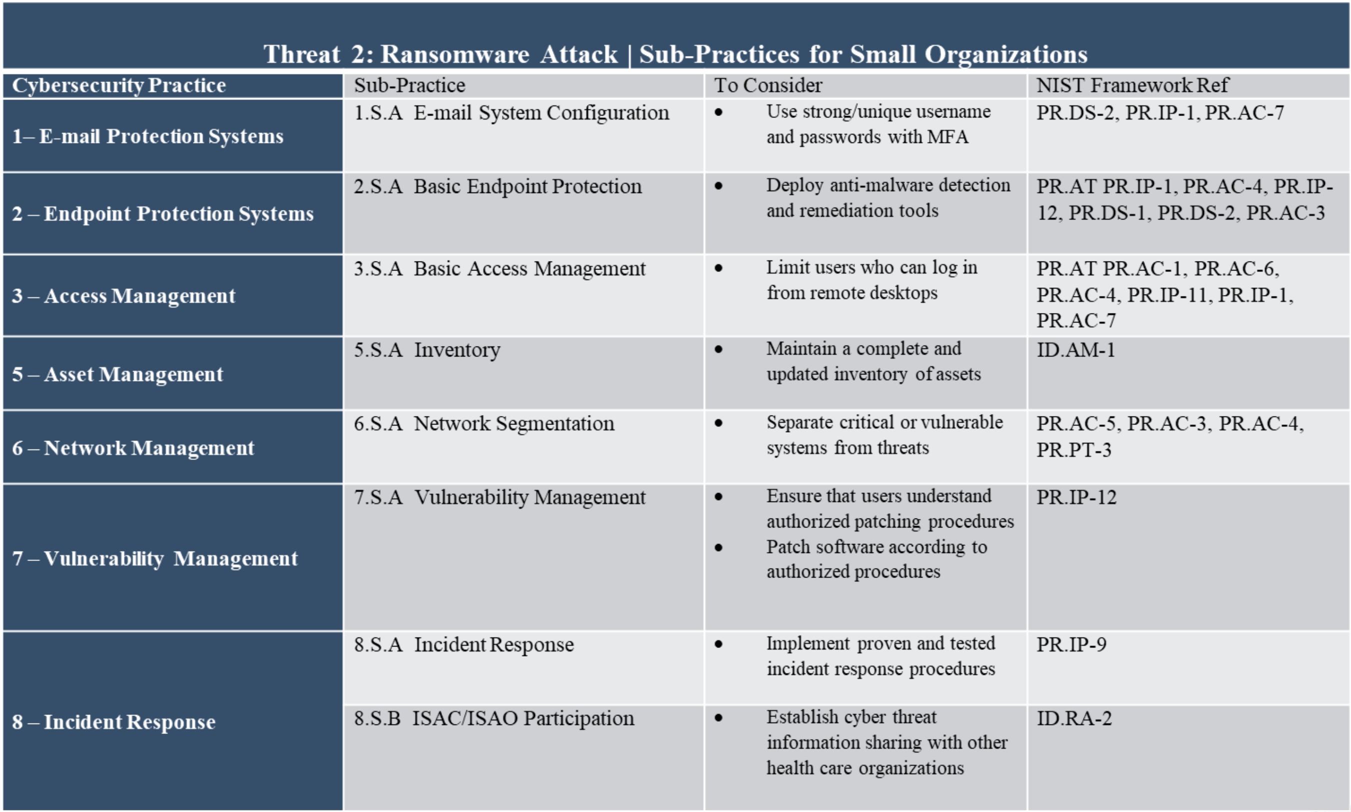


Cybersecurity Practice 2: Endpoint Protection Systems		
Data that may be affected	Passwords, PHI	
Medium Sub-Practices	2.M.A	Basic Endpoint Protection Controls
Large Sub-Practices	2.L.A 2.L.B 2.L.C 2.L.D 2.L.E 2.L.F	Automate the Provisioning of Endpoints Mobile Device Management Host Based Intrusion Detection/Prevention Systems Endpoint Detection Response Application Whitelisting Micro-segmentation/virtualization strategies
Key Mitigated Risks	• Ransomware Attacks • Theft or Loss of Equipment or Data	

Sample Metrics

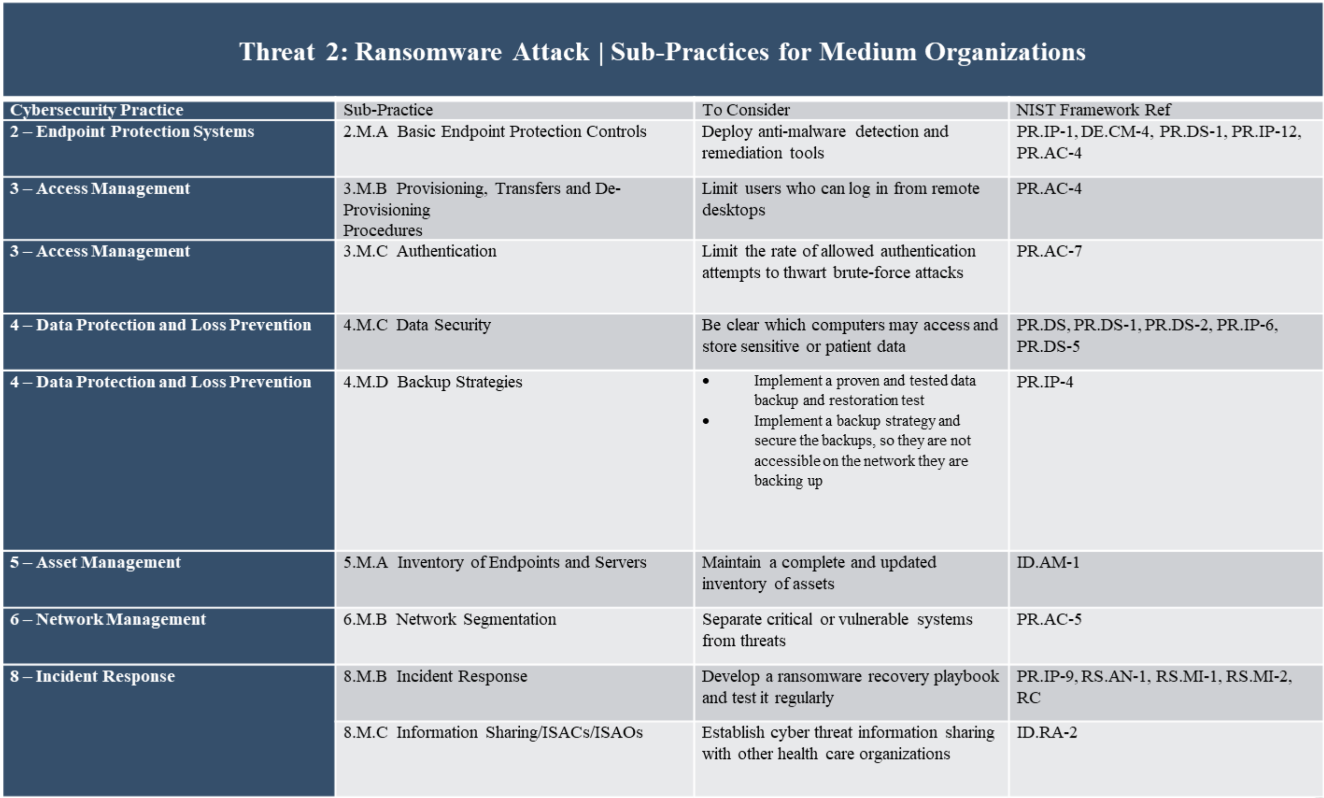
- Percentage of endpoints encrypted based on a full fleet of known assets, measured weekly.
- Percentage of endpoints that meet all patch requirements each month.
- Percentage of endpoints with active threats each week.
- Percentage of endpoints that run non hardened images each month.
- Percentage of local user accounts with administrative access each week.

Ransomware Attack Mitigating Practices – Small Organizations



Threat 2: Ransomware Attack | Sub-Practices for Small Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
1– E-mail Protection Systems	1.S.A E-mail System Configuration	• Use strong/unique username and passwords with MFA	PR.DS-2, PR.IP-1, PR.AC-7
2 – Endpoint Protection Systems	2.S.A Basic Endpoint Protection	• Deploy anti-malware detection and remediation tools	PR.AT PR.IP-1, PR.AC-4, PR.IP-12, PR.DS-1, PR.DS-2, PR.AC-3
3 – Access Management	3.S.A Basic Access Management	• Limit users who can log in from remote desktops	PR.AT PR.AC-1, PR.AC-6, PR.AC-4, PR.IP-11, PR.IP-1, PR.AC-7
5 – Asset Management	5.S.A Inventory	• Maintain a complete and updated inventory of assets	ID.AM-1
6 – Network Management	6.S.A Network Segmentation	• Separate critical or vulnerable systems from threats	PR.AC-5, PR.AC-3, PR.AC-4, PR.PT-3
7 – Vulnerability Management	7.S.A Vulnerability Management	• Ensure that users understand authorized patching procedures • Patch software according to authorized procedures	PR.IP-12
8 – Incident Response	8.S.A Incident Response	• Implement proven and tested incident response procedures	PR.IP-9
	8.S.B ISAC/ISAO Participation	• Establish cyber threat information sharing with other health care organizations	ID.RA-2

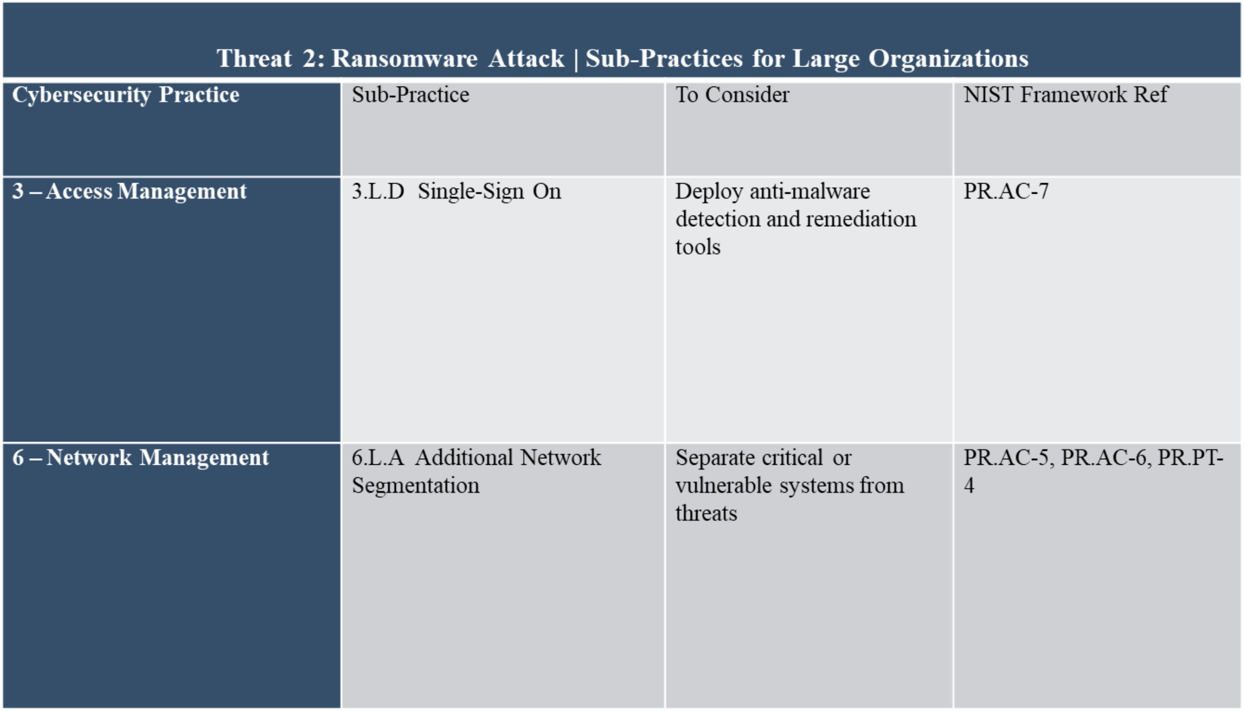
Ransomware Attack Mitigating Practices – Medium Organizations



Threat 2: Ransomware Attack | Sub-Practices for Medium Organizations

Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
2 – Endpoint Protection Systems	2.M.A Basic Endpoint Protection Controls	Deploy anti-malware detection and remediation tools	PR.IP-1, DE.CM-4, PR.DS-1, PR.IP-12, PR.AC-4
3 – Access Management	3.M.B Provisioning, Transfers and De-Provisioning Procedures	Limit users who can log in from remote desktops	PR.AC-4
3 – Access Management	3.M.C Authentication	Limit the rate of allowed authentication attempts to thwart brute-force attacks	PR.AC-7
4 – Data Protection and Loss Prevention	4.M.C Data Security	Be clear which computers may access and store sensitive or patient data	PR.DS, PR.DS-1, PR.DS-2, PR.IP-6, PR.DS-5
4 – Data Protection and Loss Prevention	4.M.D Backup Strategies	• Implement a proven and tested data backup and restoration test • Implement a backup strategy and secure the backups, so they are not accessible on the network they are backing up	PR.IP-4
5 – Asset Management	5.M.A Inventory of Endpoints and Servers	Maintain a complete and updated inventory of assets	ID.AM-1
6 – Network Management	6.M.B Network Segmentation	Separate critical or vulnerable systems from threats	PR.AC-5
8 – Incident Response	8.M.B Incident Response	Develop a ransomware recovery playbook and test it regularly	PR.IP-9, RS.AN-1, RS.MI-1, RS.MI-2, RC
	8.M.C Information Sharing/ISACs/ISAOs	Establish cyber threat information sharing with other health care organizations	ID.RA-2

Ransomware Attack Mitigating Practices - Large Organizations



Threat 2: Ransomware Attack | Sub-Practices for Large Organizations			
Cybersecurity Practice	Sub-Practice	To Consider	NIST Framework Ref
3 – Access Management	3.L.D Single-Sign On	Deploy anti-malware detection and remediation tools	PR.AC-7
6 – Network Management	6.L.A Additional Network Segmentation	Separate critical or vulnerable systems from threats	PR.AC-5, PR.AC-6, PR.PT-4

References

- "2021 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT," Sonatype. September 13, 2021. https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021.
- (ENISA), European Union Agency for Cybersecurity. 2021. Understanding the increase in Supply Chain Security Attacks. July 29. Accessed November 2021, 17. https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks.
- (MSTIC), Microsoft Threat Intelligence Center. 2021. Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021. November 16. Accessed November 16, 2021. https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/.
- Abrams, Lawerence. 2021. Lazarus hackers target researchers with trojanized IDA Pro. November 10. Accessed November 16, 2021. https://www.bleepingcomputer.com/news/security/lazarus-hackers-target-researchers-with-trojanized-ida-pro/.
- Abrams, Lawrence. 2021. Emotet malware is back and rebuilding its botnet via TrickBot. November 15. Accessed November 16, 2021. https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/.
- Barnes, Julian E. 2020. Russia Is Trying to Steal Virus Vaccine Data, Western Nations Say. December 14. Accessed November 16, 2021. https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html.
- CrowdStrike, Medigate and. 2021. 82 Percent of Health Systems Reported Experiencing an IoT Cyberattack in Last 18 Months. November 16. Accessed November 17, 2021. https://www.prnewswire.com/news-releases/82-percent-of-health-systems-reported-experiencing-an-iot-cyberattack-in-last-18-months-301425405.html.

References

- Denyer, Simon. 2021. North Korea tried to steal Pfizer coronavirus vaccine information, South says. February 16. Accessed November 16, 2021. https://www.washingtonpost.com/world/asia_pacific/north-korea-pfizer-coronavirus-vaccine-hack/2021/02/16/c09ec7fc-702e-11eb-8651-6d3091eac63f_story.html.
- Ellyatt, Holly. 2021. 'It's scientific nonsense': Russia denies claims it stole Covid vaccine blueprint from the UK. October 13. Accessed November 16, 2021. https://www.cnbc.com/2021/10/13/russia-denies-claims-it-stole-covid-vaccine-blueprint.html.
- Flashpoint. 2021. RAMP Ransomware's Apparent Overture to Chinese Threat Actors. 16 November. Accessed November 17, 2021. https://www.flashpoint-intel.com/blog/ramp-ransomware-chinese-threat-actors/.
- Gatlan, Sergiu. 2021. FBI warns of APT group exploiting FatPipe VPN zero-day since May. November 18. Accessed November 18, 2021. https://www.bleepingcomputer.com/news/security/fbi-warns-of-apt-group-exploiting-fatpipe-vpn-zero-day-since-may/.
- IronNet Threat Analysis and Research Teams, including lead contributors Morgan Demboski, Joey Fitzpatrick, and Peter Rydzynski. 2021. China cyber attacks: the current threat landscape. October 26. Accessed November 16, 2021. https://www.ironnet.com/blog/china-cyber-attacks-the-current-threat-landscape.
- Jack Stubbs, Christopher Bing. 2020. Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources. May 8. Accessed November 16, 2021. https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV.
- Miller, Joshua. 2021. BadBlood: TA453 Targets US and Israeli Medical Research Personnel in Credential Phishing Campaigns. March 30. Accessed November 16, 2021. https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential.

References

- Ponsford, Matthew. 2021. The Real Danger of a Biological Cold War with China. November 1. Accessed November 16, 2021. https://neo.life/2021/11/the-real-danger-of-a-biological-cold-war-with-china/
- Staff, Reuters. 2021. Russian, Chinese hackers targeted Europe drug regulator: newspaper. March 6. Accessed November 16, 2021. https://www.reuters.com/article/us-eu-cyber-idUSKBN2AY0F1.
- Team, BlackBerry Research & Intelligence. 2021. Drawing a Dragon: Connecting the Dots to Find APT41. October 5. Accessed November 16, 2021. https://blogs.blackberry.com/en/2021/10/drawing-a-dragon-connecting-the-dots-to-find-apt41.
- Toulas, Bill. 2021. Microsoft warns of the evolution of six Iranian hacking groups. November 16. Accessed November 16, 2021. https://www.bleepingcomputer.com/news/security/microsoft-warns-of-the-evolution-of-six-iranian-hacking-groups/.