LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

2021 Forecast: The Next Year of Healthcare Cybersecurity

03/11/2021

TLP: WHITE, ID# ***202103111030***

Agenda

- Ransomware
  - Big Game Hunting
  - Automation and Spear Phishing
  - Double Extortion
  - Ransomware Trends
- Data Breaches
  - VPN Usage Risks
  - Zero Trust Security Strategy
  - Supply Chain Attacks
- Continuing Impacts of COVID-19
- Internet of Medical Things (IoMT)
- Cybersecurity Spending in the Healthcare and Public Health (HPH) Sector
- Mitigations
- References
- Questions

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

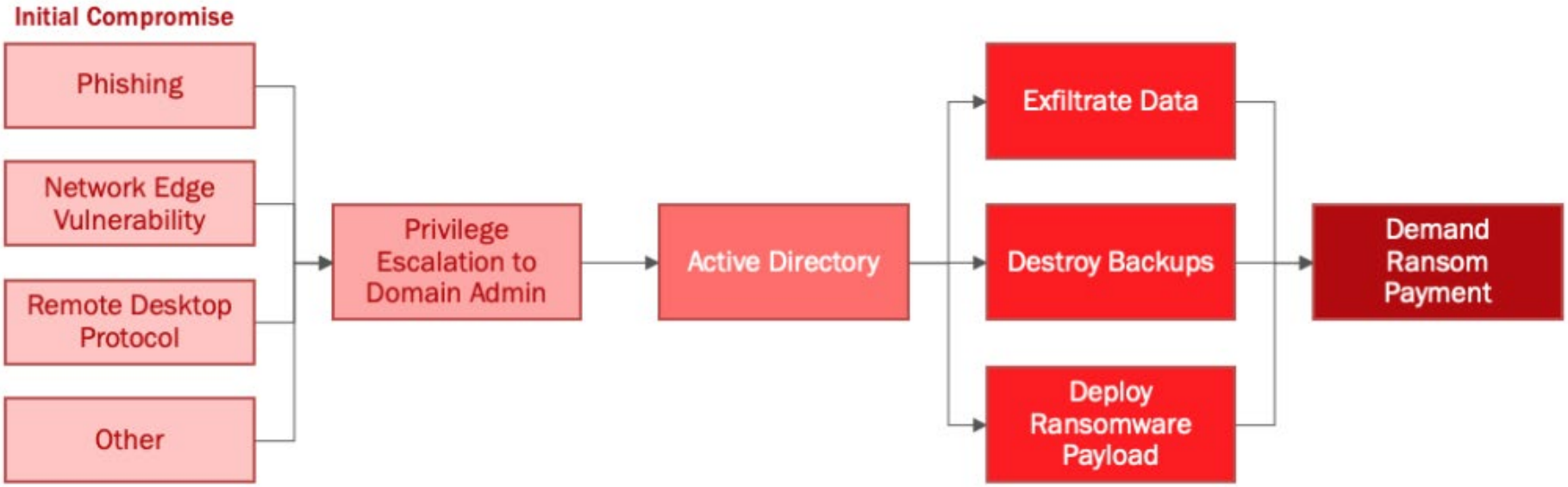
Ransomware: The Rise of Big Game Hunting

- CrowdStrike predicts a trend away from a “spray and pray” approach to ransomware attacks to ones known as “big-game hunting”.
- Actors pursuing fewer higher value targets with more targeted approaches.
- Once actors have gained access to the network, they are more likely to take their time before striking.

Phishing	Network Edge Vulnerability	Remote Desktop Protocol (RDP)
• A threat actor uses an email to entice the victim to provide credentials or other access tools	• Unpatched vulnerabilities in the network create opportunities for compromise	• A remote desktop software tool that already has access to a machine is exploited, and then uses the access to the device to steal information

Big Game Hunting

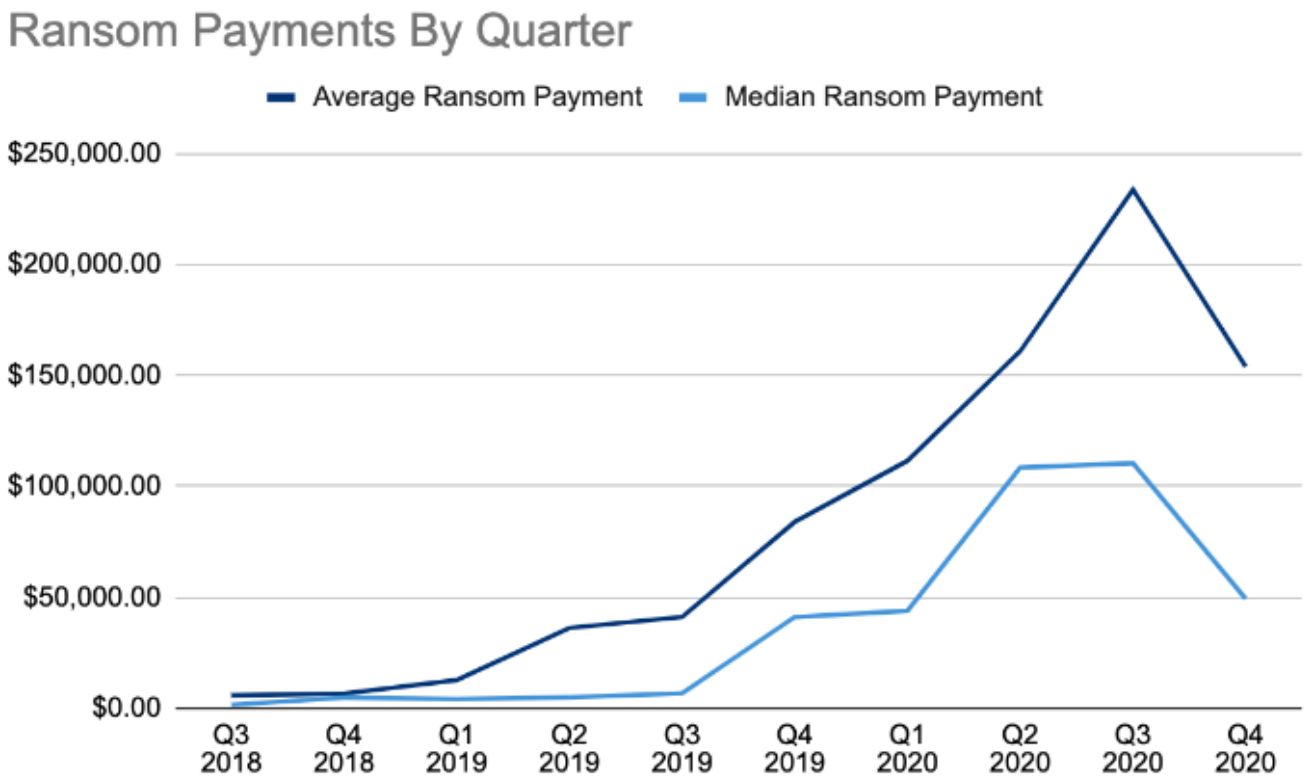
The new ransomware pattern



Automation and Spear Phishing

- Cybersecurity firm WatchGuard predicts that “cybercriminals have already started to create tools that can automate the manual aspects of spear phishing.”
- This automation could combine the automation of phishing with the highly targeted nature of spear phishing.
- Ongoing instability and uncertainty from the global pandemic makes all phishing attempts more effective.

- **"It's a plague on business… This is not your father's ransomware." – Garin Pace, AIG Cyber Product Lead**
- Further expansion of double-extortion
  - Expanded from exclusively Maze in 2019, to 18 ransomware operators in 2020
    - Requires data exfiltration prior to encryption
  - Potential threats:
    - Releasing or publishing stolen data (Maze)
    - Permanently deleting stolen data entirely (REvil/Sodinokibi)
    - Targeting executives to encourage ransom payment (CL0P)
  - Some techniques only used by a single RaaS actor, but probably not for long
  - "Ransomware gangs are very quick to adopt new techniques, especially those that make ransom payment more likely." – Allan Liska, Record Future Senior Security Architect



COVEWARE

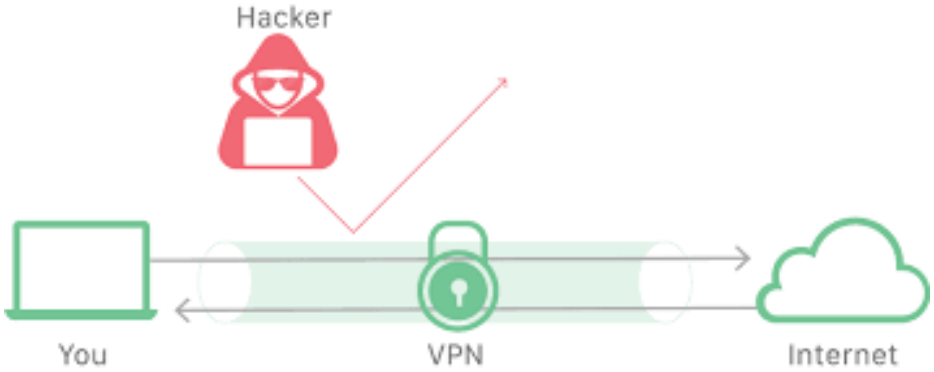
- Paying the ransom may not prevent RaaS gangs from selling the stolen data
- RaaS gangs may not have the ability or will to follow through on threats
- In October 2020, the US Department of the Treasury's Office of Foreign Assets Control advised that paying ransomware demands may risk violating US sanctions

"When fewer companies pay, regardless of the reason, it causes a long term impact, that compounded over time can make a material difference in the volume of attacks." – Coveware

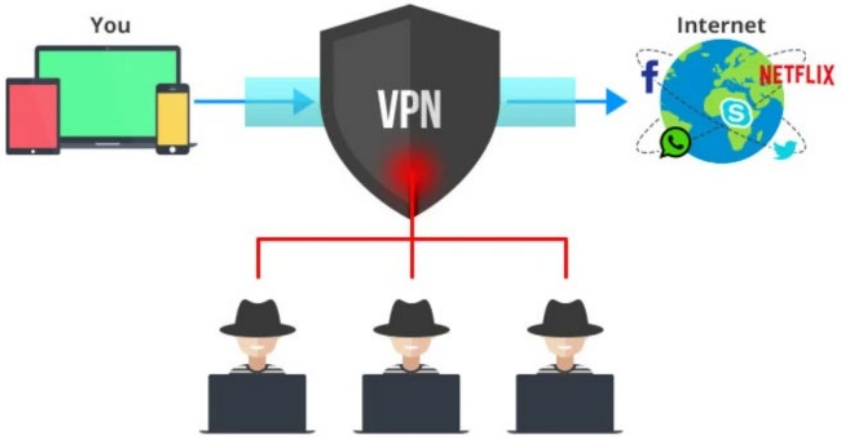
VPN-Usage Protects but Can Introduce Vulnerabilities

- Like ransomware attacks, data breaches are a major plague to healthcare in cyberspace.
  - Through double extortion, these two attacks are often combined.
  - Ransomware attacks were responsible for almost 50% of all healthcare data breaches in 2020.
- Healthcare is the most targeted sector for data breaches.
- VPNs protect organizations from many forms of attacks, but VPN vulnerabilities can leave users and organizations at risk:
  - PulseSecure and VMWare had major vulnerabilities in 2020.

VPNs in Theory

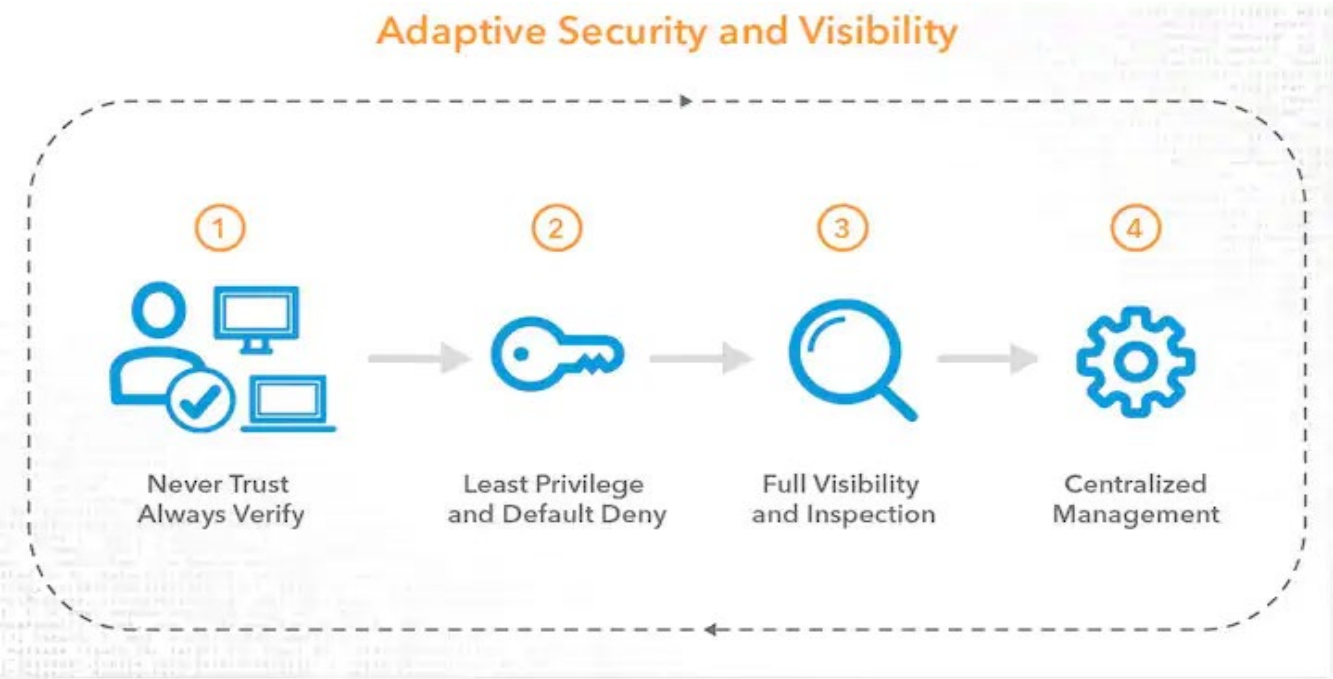


VPNs in Practice

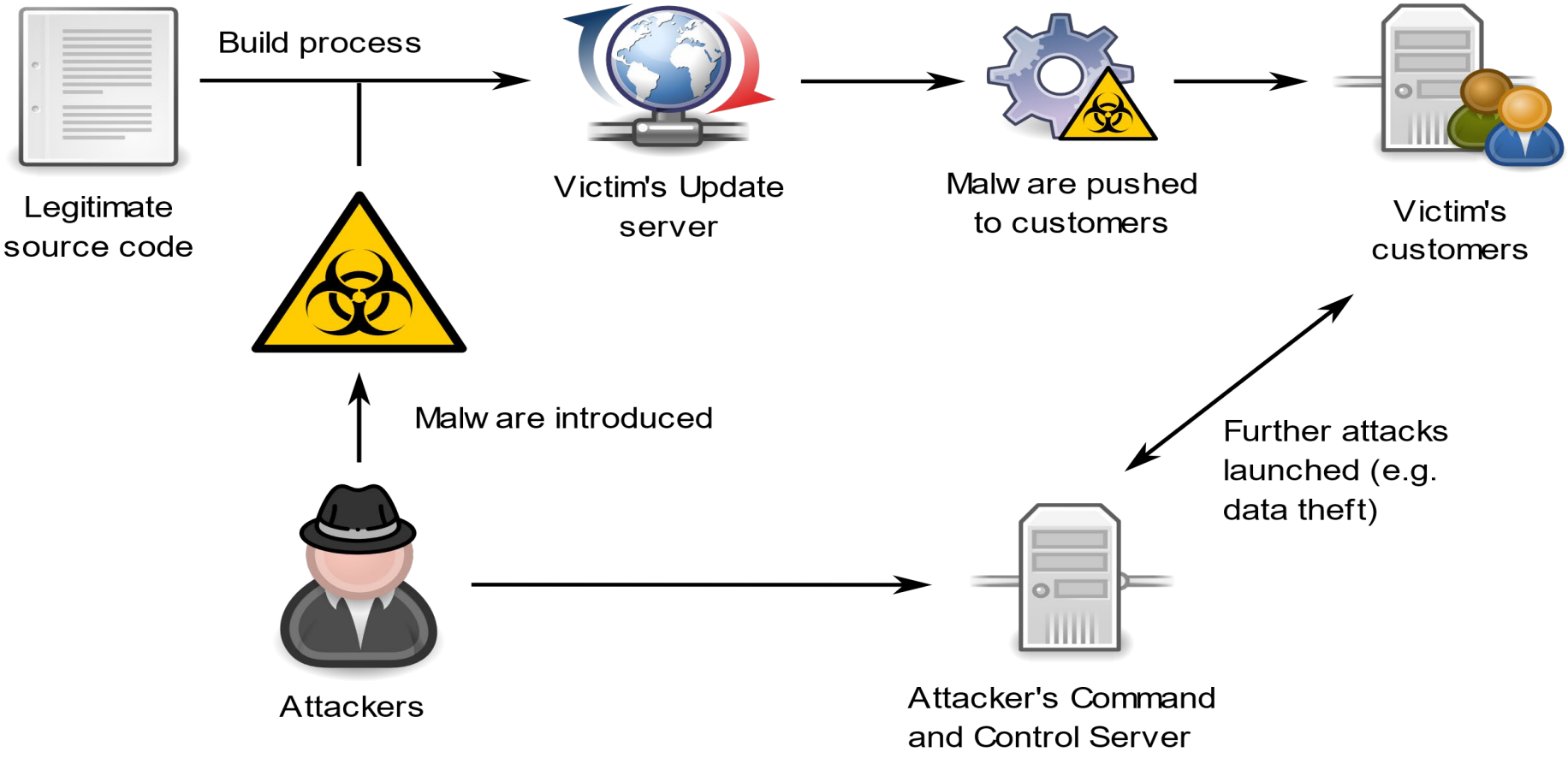


VPN-Usage Accelerates Move to Zero Trust

- 34% of IT security teams across the globe claim to be in the process of implementing a Zero Trust security model (Gartner).
  - "Zero Trust is a security concept that requires **all users, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validating security configuration and posture,** before being granted or keeping access to applications and data." – CrowdStrike
- Gartner predicts 60% of enterprises will be phased out of VPNs in favor of Zero Trust network access by 2023.



- The SolarWinds breach was not an isolated incident
- Organizations are put at risk not just by their own attack surface, but by the attack surface of their vendors



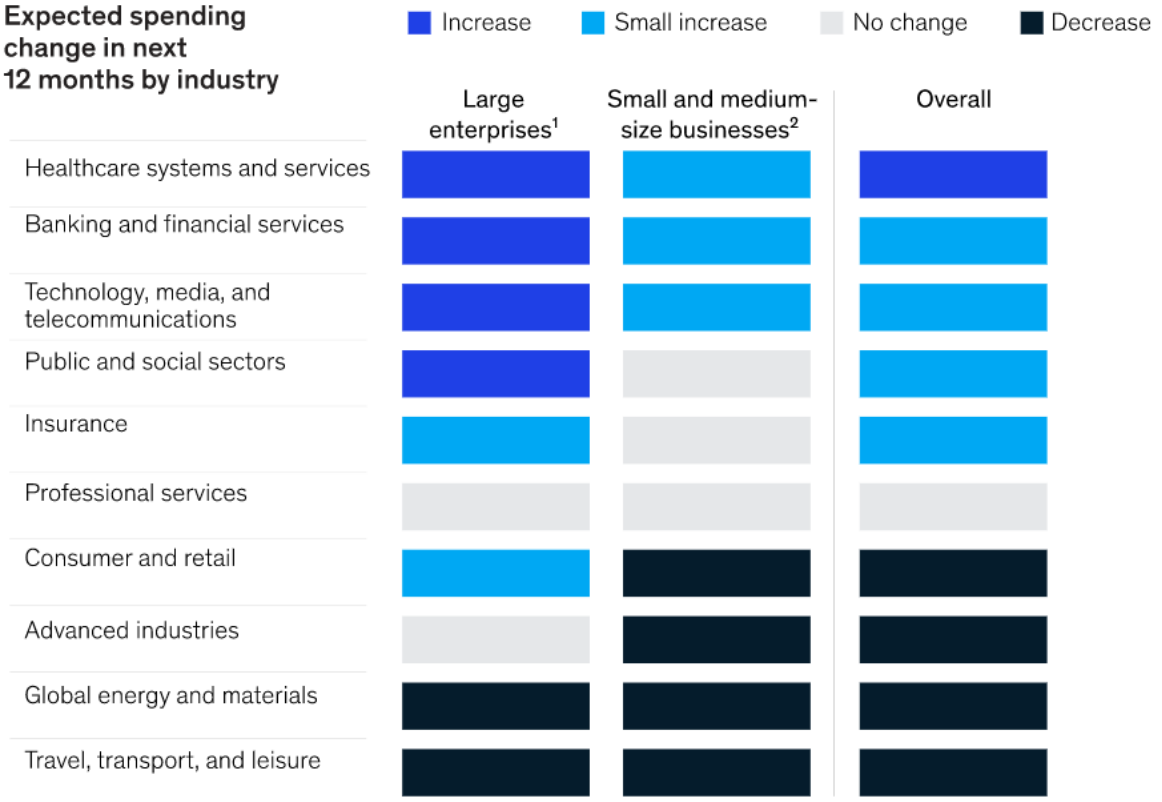
- COVID-19 was an almost unknown threat at the beginning of 2020, but shows no signs of disappearing in 2021, and poses a particular threat to the HPH sector.
- Continued threats from 2020:
  - Targeting of home environments and vulnerabilities introduced through COVID-19 protocols like WFH.
    - Pre-pandemic, 82% of organizations used some form of Bring Your Own Device (BYOD) for employees, partners, or other stakeholders.
      - 72% lacked BYOD malware protection entirely, or relied upon endpoint software installations.
      - Pandemic forced more organizations to allow BYOD.
      - Security management solutions are available for organizations that allow BYOD.
    - WFH exposed corporate resources to home networks.
  - COVID-19 phishing campaigns
    - Vaccine rollout
  - Targeting of COVID-19 research and vaccine distribution:
    - From FireEye: 2020 featured “targeting of hospitals, manufacturing groups and related critical infrastructures dedicated to development and distribution of a COVID-19 vaccine.”
    - “Increasing numbers of state-sponsored actors targeting coronavirus research, treatment and response efforts. This direct targeting of government, healthcare, pharmaceutical and non-governmental organizations will likely continue due to the high-value information involved.”

- **"[Through IoMT] healthcare will increase its attack surface rather than shrink its attack surface." – Frost & Sullivan**
- 5G capabilities and increased demand for remote healthcare drive adoption of IoMT devices
- According to the Open Source Cybersecurity Intelligence Network and Resource (OSCINR), 60% of all medical devices are unpatchable.
  - At the end-of-life stage with no security patches or upgrades available
  - Patching medical devices may also require taking them offline
    - Potentially deprives patients of medical care
- Rise in IoMT devices will also open HPH entities to attacks and potential compromise

Cybersecurity Spending in the HPH Sector

- PWC survey of CISOs and security buyers
- For the HPH sector, spending is set to increase under the pressure imposed by COVID-19
- However, HPH entities that have had to significantly invest in adjusting to a digital/virtual environment may have overextended their budgets and may “cut back on cybersecurity spending as a result”
    - Budgets may be squeezed by revenue reductions caused by cancellation of elective surgeries/COVID-19-based restrictions
- HPH industry is estimated to spend $18 billion on cybersecurity in 2021

The COVID-19 crisis is expected to shift cybersecurity spending by industry and product category.



- Industries hardest hit by pandemic (eg, retail, energy) expect budgets to drop; small businesses will be more affected than large ones will
- Vendors could use customers’ need for new services to recommend shifting cybersecurity tech stack to cloud rather than patching new features onto legacy systems

The following is not a complete list of mitigations for these potential threats, and should be treated as a starting point.

Phishing

- Train employees to recognize phishing emails

Ransomware:

- Maintain an incident response plan
- Maintain backups of data (3-2-1 rule)
- Patch vulnerabilities

Supply Chain Attacks:

- Ask vendors what mechanism they have in place to protect their software from compromise
- Apply policy of least-privilege to applications and software

VPN Vulnerabilities:

- Consider shifting to Zero Trust security framework

IoMT:

- Knowing is half the battle: identify all devices and vulnerabilities
- Initiate micro-segmentation
- Establish manageable and realistic network security parameters
- Maintain existing network assets and infrastructure

Reference Materials

References

- Axios. “Ransomware Trends You Need to Know in 2021.” February 11, 2021. Security Boulevard. https://securityboulevard.com/2021/02/ransomware-trends-you-need-to-know-in-2021/
- “A GLOBAL RESET: Cyber Security Predictions 2021.” 2020. FireEye. https://content.fireeye.com/predictions/rpt-security-predictions-2021
- “The SolarWinds Hack and The Arrival of Software Supply Chain Attacks.” December 18, 2020. BreachLock. https://www.breachlock.com/the-solarwinds-hack-and-the-arrival-of-software-supply-chain-attacks/
- Cimpanu, Catalin. “Some ransomware gangs are going after top execs to pressure companies into paying.” January 9th, 2021. Zero Day. https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/
- Landi, Heather. “CISOs, CIOs Not Confident in Their Medical Device Security Strategy, New KLAS Research Finds.” October 9th, 2018. Healthcare Innovation Group. https://www.hcinnovationgroup.com/cybersecurity/article/13030781/cisos-cios-not-confident-in-their-medical-device-security-strategy-new-klas-research-finds
- Mitran, Sarah. “Medical Device and Network Security – Coming to Terms with the Internet of Medical Things” Frost & Sullivan. 2019. https://www.extremenetworks.com/resources/white-paper/medical-device-and-network-security-coming-to-terms-with-the-internet-of-medical-things/
- Venky Anant, Jeffrey Caso, and Andreas Schwarz. “COVID-19 crisis shifts cybersecurity priorities and budgets.” July 21, 2020. McKinsey. https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets
- Sentonas, Michael. “Ransomware attackers now have their sights set on the biggest prize.” Wired. January 2, 2020. https://www.wired.co.uk/article/ransomware-trends-2021

References

- “Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands” February 1st, 2021. Coveware. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
- Dixon, Brian. “Why ransomware attacks will explode in 2021” January 12, 2021. Cyber News. https://cybernews.com/security/ransomware- attacks-will-explode-in-2021/
- “Cybersecurity comes of age as industries transform” PriceWaterhouseCooper. https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights/sector-analysis.html#health
- Lohrmann, Dan. “The Top 21 Security Predictions for 2021.” December 22, 2020. GovTech. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html
- “Turning the Tide: TrendMicro Security Predictions for 2021.” December 08, 2020. TrendMicro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021
- Abousselham et al. “Data Security Predictions for 2021.” 2020. Splunk. https://www.splunk.com/pdfs/ebooks/splunk-security-predictions-2021.pdf
- “Advanced Threat predictions for 2021.” November 19, 2020. SecureList. https://securelist.com/apt-predictions-for-2021/99387/
- Kahol, Anurag. “Seven cybersecurity predictions for 2021. November 10, 2020. Security Magazine. https://www.securitymagazine.com/articles/93887-seven-cybersecurity-predictions-for-2021?
- Qi An Xin Group. “Zero Trust Architecture and Solutions.“ 2020. Gartner. https://www.gartner.com/teamsiteanalytics/servePDF?g=/imagesrv/media-products/pdf/Qi-An-Xin/Qi-An-Xin-1-1OKONUN2.pdf

Upcoming Briefs

- HPH Supply Chain Risk Management (3/18)

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday between 9am-5pm (EST) at **202-691-2110.**

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

Products

Sector & Victim Notifications

Directs communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, and general notifications to the HPH about currently 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 document and presentation that provides 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 call us Monday-Friday between 9am-5pm (EST) at **202-691-2110.**

Questions

Contact

Health Sector Cybersecurity Coordination Center (HC3)

202-691-2110

HC3@HHS.GOV