LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Securely Teleworking in Healthcare

03/26/2020

Report #: 202003260918

Agenda

- Why this topic?
- Telework: Benefits vs. Risks
- Current healthcare telework jobs
- Healthcare services offered remotely
- Implementing a telework program
- Policy modification considerations
- Home office requirements and security
- Virtual Private Networks (VPNs)
- Multi-factor Authentication (MFA)
- PHI and ePHI and how to protect it
- Transitioning to the cloud
- Additional practical security recommendations
- References
- Questions

Slides Key:

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

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

Healthcare Telework: Why This Topic?

Why are we holding this presentation? Three reasons:

- **There's the obvious, immediate answer: The Coronavirus pandemic**
  - Currently, increased vulnerability and increased threat – increased risk.
- **There's a longer-term answer: This likely isn't the last event like this**
  - Continuity of operations (COOP) Plans for healthcare organizations should be in place, and include remote work provisions
- **There's a more permanent answer: Telework has inherent benefits to a healthcare organization and its employees**
  - Telework has the potential, in some instances, to make a healthcare organization more efficient and more effective
  - Telework can also raise employee morale, not only improving the quality of life for the individual but, as the saying goes, a happy employee is a productive employee

Bottom line:

- **Telework has immediate and long-term benefits for healthcare organizations…**
- **…but security becomes even more critical**

Image source: Federal Soup

Telework: Benefits vs. Risks

<u>Potential benefits of telework</u>

- Increase employee effectiveness
- Increase management achievement of goals
- Avoid delays associated with commute
- Reduce office distractions
- Reduce real estate costs/requirements
- Increased employee morale due to improved quality of life
  - Commute – saves time and money
  - Work environment – familiarity, comfort, relaxed dress code
  - Personal costs – Attire, purchasing meals
- Business continuity in the event of an emergency/disaster
- Decentralized and distributed work is becoming more common

One of the many benefits of telework is a relaxed dress code

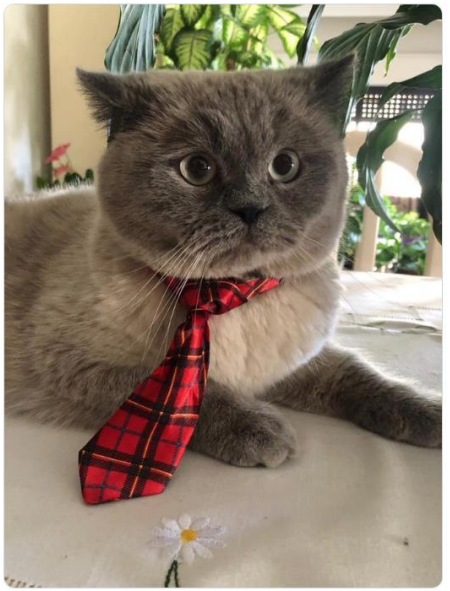


Image source: https://twitter.com/sighrolanna

<u>Potential risks when teleworking</u>

- Decreased employee effectiveness
- Increased costs
- Increased attack surface

Research that supports these observations:

<u>2014 PGi report: State of Telecommuting</u>
https://www.slideshare.net/PGi/state-of-telecommuting-2014-pgi-report/1

<u>2015 Stanford University study on Telework</u>
https://nbloom.people.stanford.edu/sites/g/files/sbiybj4746/f/wfh.pdf

<u>Office of Personnel Management: Telework Insights</u>
https://www.opm.gov/policy-data-oversight/worklife/federal-work-life-survey/telework-insights.pdf

Telework: Additional Benefits

Image source: fairfaxcounty.gov

Current Healthcare Telework Jobs

Many healthcare jobs are already offered remotely, such as:

- IT and information specialists
- Medical billing/coding
- Medical translator
- Nurse care manager
- Medical director
- Clinical Program Manager
- Healthcare recruiter
- Medical writer
- Insurance professional
- Patient advocate/customer service rep
- Medical transcriptionist
- Pharmaceutical representative
- Legal nurse consultant
- Physician

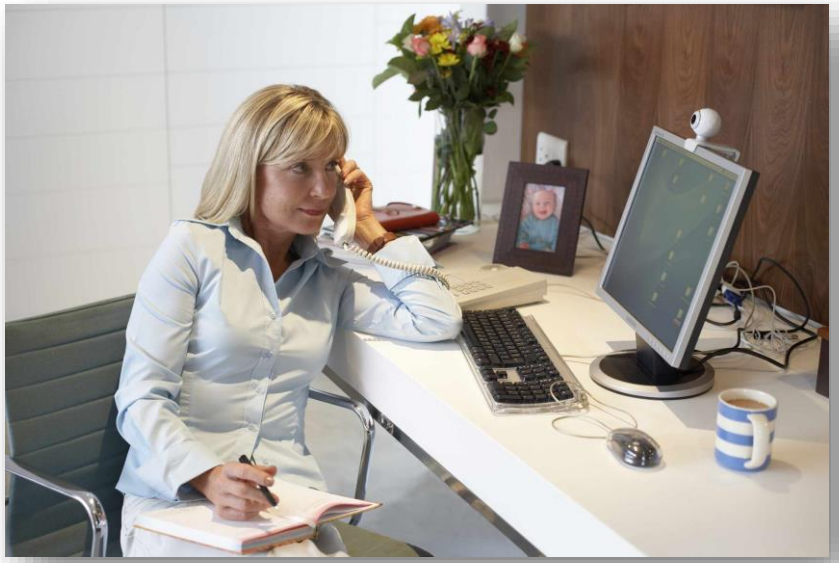


Image source: Lifewire

Therefore, many healthcare organizations already have the basic technology and policy infrastructure in place to support telework, and expansion is simply a matter of managed scaling of those capabilities

How to Implement/Expand a Telework Program

Implementing/expanding a telework program

- **Training (Both individual contributors and managers)**
  - Individual contributors need to receive training in working securely (VPN use, PII/PHI handling, collaboration tools, etc…)
  - Managing telework employees can be a challenge
  - Managers need to be familiar with the same tools their employees are using (see above) not only for their own use but to ensure their employees remain well-trained and are utilizing them to the best of their ability
  - Communication and organization are key
- **Devices – Allocated, tracked, and secured:**
  - Endpoints – enterprise and/or BYOD (laptops, tablets, cellphones, etc…)
  - Security (protecting PII and PHI in all forms)

Image source: Thrive Global

How to Implement/Expand a Telework Program

- **Scalable infrastructure**
  - Internet service (adequate bandwidth for the organization)
  - Out-of-band communication methods
  - Virtual Private Network (VPN) technology
  - Multi-factor Authentication (MFA) technology
  - Bandwidth monitoring and management (internal and external)

- **Policy**
  - Describes how an employee requests, utilizes and terminates regular remote access to an organization's information resources (systems, networks and data)
  - Includes acquisition, use and maintenance of mobile system
  - May also include bring your own device (BYOD) requirements
  - An IT helpdesk will need to be adequately staffed to support increased teleworkers

Image Source: Flickr

Policy Modification Considerations

Implementation/Expansion of BYOD policy:

- **Reevaluation of BYOD policies – Expansion may require:**
  - Additional training
    - Security for BYOD devices
    - Managers will need to plan and proactively manage remote workers to be sure they are providing the support to the organization their position requires
  - Additional security (VPN accounts, endpoint security implementation)
  - Must include all devices (laptops, tablets, phones, etc…)

Image source: Wikipedia

- **Security implications go beyond individual devices:**
  - If multi-factor authentication is not already in place, this is a good opportunity
  - Scalable VPN services may require additional IT resources and personnel to support
  - Management of VPN accounts becomes even more important

Policy Modification Considerations

- **Enterprise security policy**
  - All decisions must be made with the understanding that the attack surface increases as more employees telework.
    - Intrusion detection and real-time incident handling becomes even more important
    - Security Information and Event Management (SIEM) tools become even more important
- **Telework policy also fits into the overall risk mitigation strategy and as such, should be part of any COOP plan**

Home Office Requirements

What does an employee need in their residence to telework?

- **Physical space**
  - Preferably an area that is dedicated to work and not used for anything else
- **Reliable (speed and consistent availability) of communications**
  - Internet access via Internet Service Provider (ISP)
  - Cellular signal via local cell tower
    - May consider cell extender
- **Modem and router**
  - Modem usually provided by ISP
  - Routers can be bought locally or online
    - Newer routers are more secure
- **Isolation from distractions**
- **Office supplies**
  - The usual: pens, notebooks, etc…
  - Desk and comfortable chair
  - Filing cabinet
  - Fire safe box

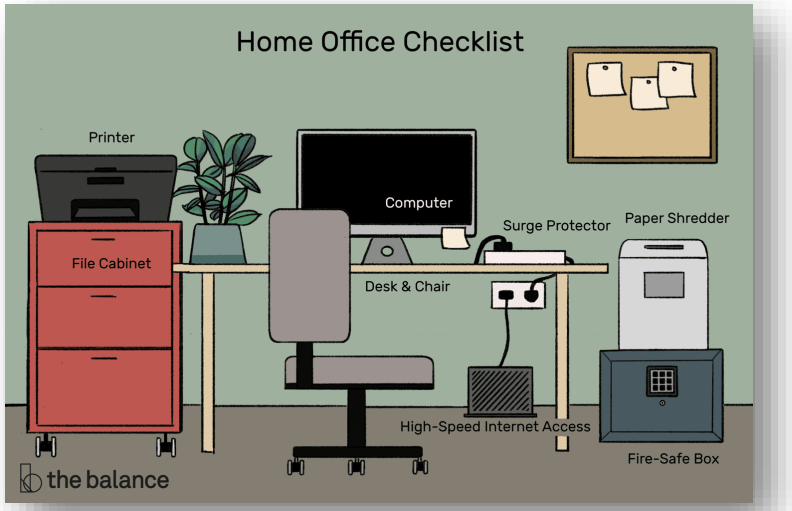


Image source: The Balance Small Business

Home Office Needs: Security is Critical!

Home office IT components:

- **Modem**
  - Point of demarcation
  - Receives/Sends directly to/from Internet Service Provider (ISP)
- **Router/Firewall**
  - Can provide access to both wired and wireless devices
  - Often includes integrated firewall
    - Firewall acts as digital security guard for network/internet traffic
  - Devices can include laptops, desktops, tablets, wired and cellular phones
  - Extenders can allow wireless router signal to extend throughout a large home/building
- **Endpoint security**
  - Installed and updated

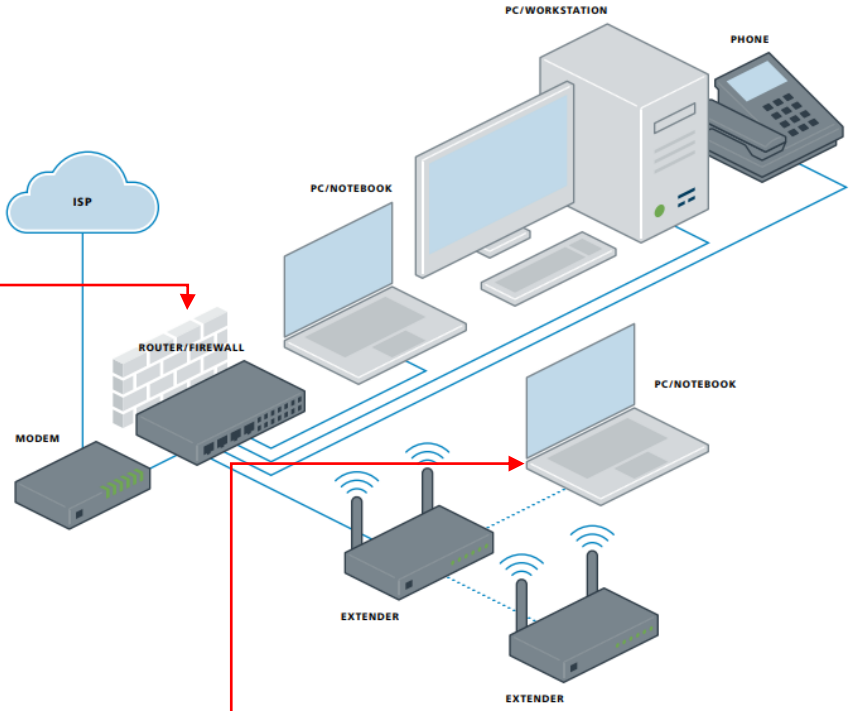
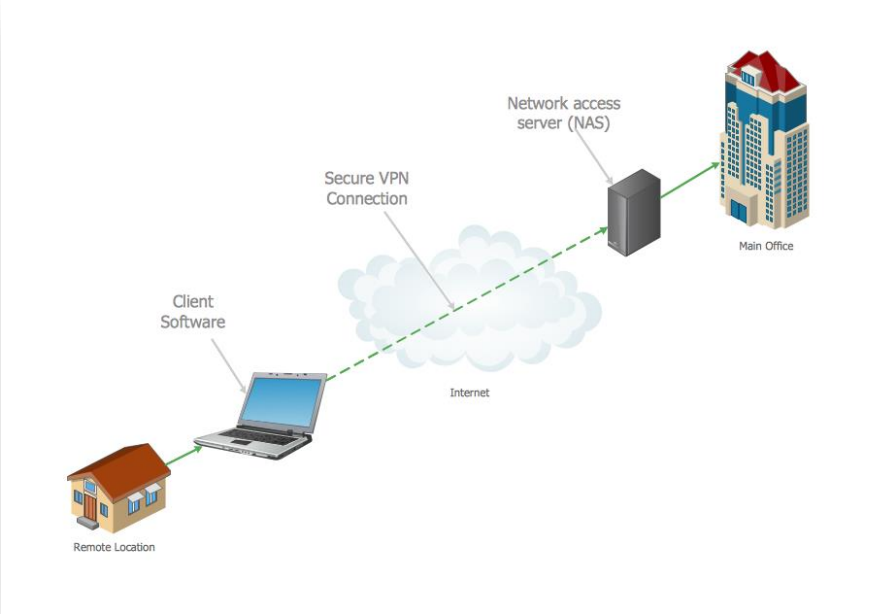


Diagram source: Center for Internet Security

Virtual Private Networks (VPNs)

What is a VPN?

- Virtual Private Network
- Creates an encrypted “tunnel” enabling secure, end-to-end communications; extends a private network beyond traditional physical boundaries
- Commonly used for teleworkers or workers on travel
- Protects confidentiality and prevents interception of data; Allows for use of public infrastructure without exposing sensitive information
- Does not defend against denial-of-service attacks; doesn’t protect availability
- A VPN server must be operated and maintained – these demands will increase as the number of users increases
- Malicious individuals will attempt to exploit the VPN server as it can present an attractive target



DVPN diagram source: Conceptdraw.com

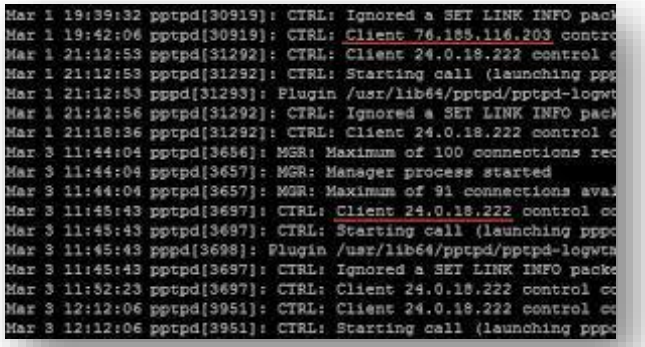
Virtual Private Networks (VPNs)

What to be concerned about regarding VPNs?

- **Critical to keep a VPN server patched and properly configured! Why?**
  - Unlike other IT resources, it is necessarily exposed to the public Internet
  - By its very function, it allows access to the internal network
  - It is a glaring target for malicious individuals

- **What to do to keep VPN services and the enterprise IT infrastructure safe?**
  - VPN accounts must be properly managed and monitored
    - Tracking which accounts login and when (review logs)
    - Abnormal behavior should be monitored
      - Did the account for a “M-F, 9-5” worker login at 3AM Sunday morning?
      - Investigate as appropriate
    - Access restrictions per account can (and should!) be implemented
      - When?
      - How often?
      - Failed login attempts
    - Security Incident and Event Management tools
      - Thorough coverage of VPN server and demilitarized zone (DMZ)

Example VPN server logs



Multi-Factor Authentication

Multifactor authentication (MFA)

- **Three categories of authentication methods**
  - Something you have (e.g. ID card, physical token, cell phone)
  - Something you are (fingerprint, iris features, signature)
  - Something you know (password, pin number, combination)
- **MFA leverages two (or more!) categories**
  - Simply called two-factor authentication (2FA) when it leverages two
  - Examples:
    - Login to your bank with password, PIN # sent to phone to also be entered
    - Need to insert ID card into computer and enter PIN when logging in
- **MFA can go a long way in keeping enterprise accounts, e-mail and VPN accounts secure and is highly recommended for teleworkers**

PHI and ePHI

PHI – "Protected Health Information" – Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Definition (Per 45 CFR 160.103)

- Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:
  - (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  - (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
    - (i) That identifies the individual; or
    - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

PHI and ePHI

18 HIPAA identifiers:

- Patient name
- Dates (birth, treatment, death)
- Physical addresses
- E-mail addresses
- Fax numbers
- Social security numbers
- Telephone numbers
- URLs/Web addresses
- Full face photos/other pictures
- Health plan beneficiary information
- Certificate/License numbers
- Device identifiers and serial #s
- Vehicle identification information
- Internet Protocol (IP) addresses
- Biometric (finger, voice, etc..) info
- Medical record #s
- Account number
- Any other uniquely identifying info

ePHI is PII that is "produced, saved, transferred or received in an electronic form."

ePHI leaks are one of the biggest concerns for modern day healthcare cybersecurity, especially with regards to telemedicine

Transitioning to the Cloud

- **Transitioning to the cloud facilitates telework for two reasons:**
  - You will need less IT staff to manage assets and resources
  - Cloud capabilities allow for remote access to assets and resources
- **Four options**
  - On-premises: Internal management of everything
  - Infrastructure-as-a-service: On-demand access to IT resources which allow an organization from having to purchase hardware outright
  - Platform-as-a-service: Provides infrastructure, some software and a framework for developers to build upon; Applications managed in house
  - Software-as-a-service: Delivers applications that are managed by a third-party vendor; Also known as cloud application services (most common option)

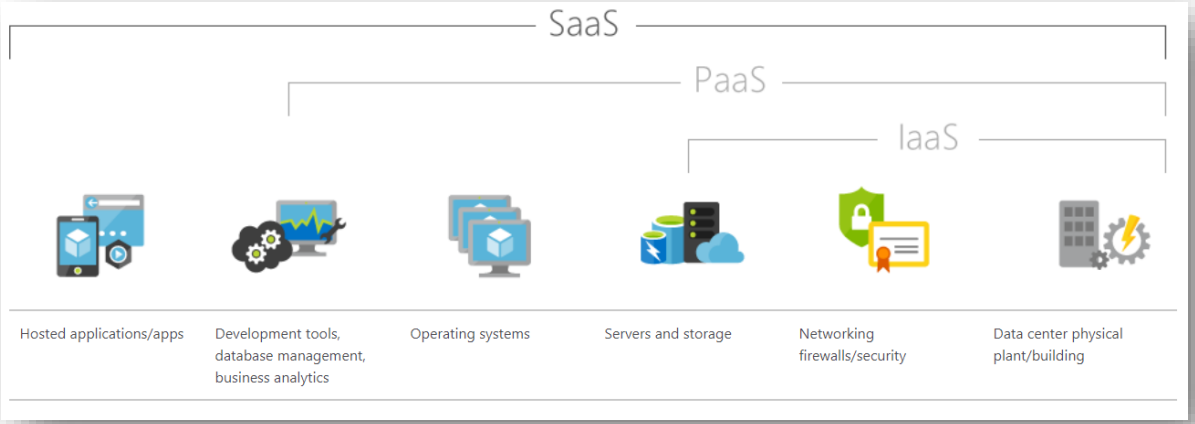


Diagram source: Microsoft

Transitioning to the Cloud (Continued)

- **Moving to software-as-a-service (SaaS) might help any transition to telework**
  - Complete software solution
  - Pay-as-you-go
  - Reduce need for IT staff
- **Outsourcing…**
  - Management of servers and applications
  - Data storage
  - Uptime requirements
  - Bandwidth and overall availability
  - Some security capabilities
- **Security**
  - Storage and transmission security outsourced
- **Other options besides SaaS could also lighten the burden of a transition to telework**

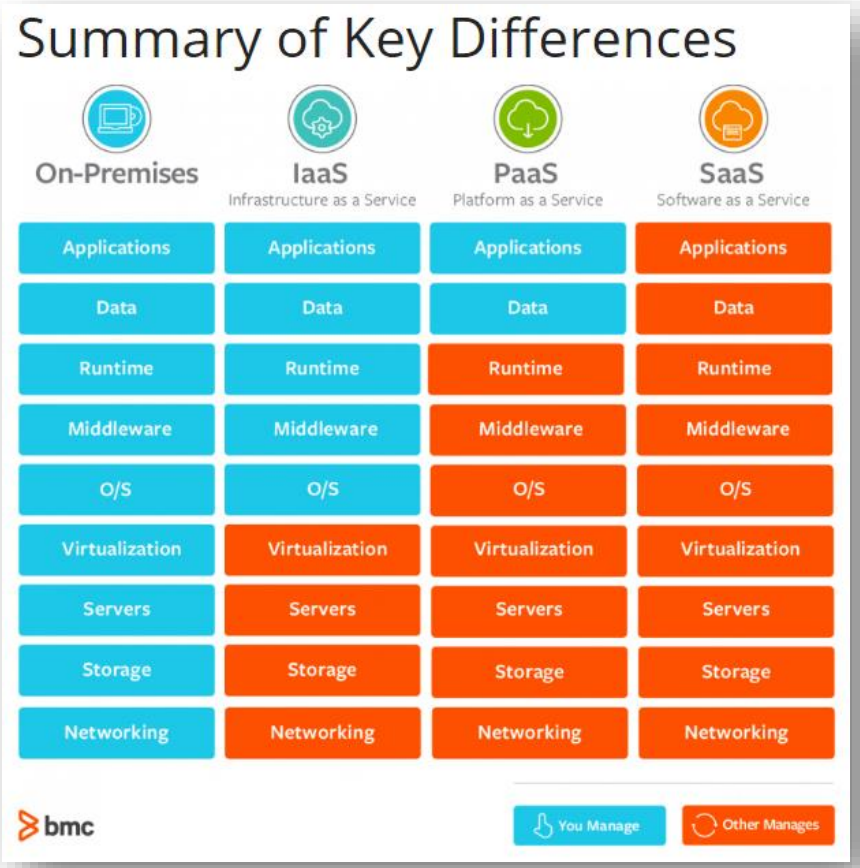
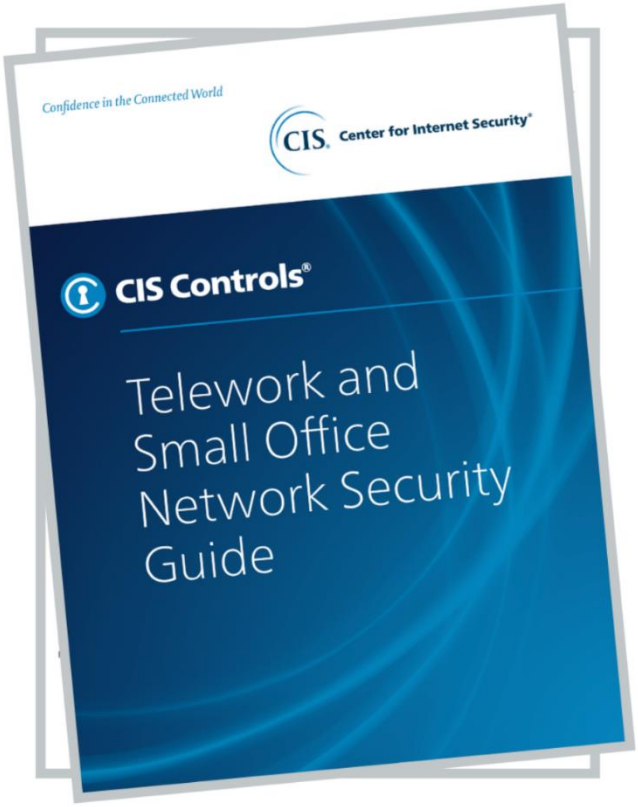


Diagram source: BMC

Practical Steps to Minimize Attack Surfaces

The Center for Internet Security (CIS)

- Non-profit organization dedicated to promoting cybersecurity, cyberdefense and an environment of trust in cyberspace
- They released a guide for small offices and home office network security that we recommend as part of an approach to securing a telework environment
  - The guide includes:
    - Purchasing, setting up and managing equipment
      - Devices and networks
    - Common data encryption algorithms (WEP, WPA, WPA2, WPA3 and WPS)
      - Note that, as the guide explains, WEP and WPA are obsolete and insecure encryption algorythms
    - Network security configuration best practices
    - An action checklist
    - Mapping to CIS controls
- The guide can be found at:
  - https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/



Reference Materials

References

- Agencies expand, loosen telework requirements amid coronavirus spread
  - https://federalnewsnetwork.com/workforce/2020/03/uscis-to-launch-nationwide-telework-program-amid-coronavirus-spread/
- Management Checklist for Teleworking Surge During COVID-19 Response
  - https://healthsectorcouncil.org/covid-checklist/
- CIS Controls Telework and Small Office Network Security Guide
  - https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/
- Telework.gov
  - https://www.telework.gov/
- 7 Steps IT Departments Need to Take Now to Manage a Telecommuting Spike
  - https://www.pcmag.com/news/7-steps-it-departments-need-to-take-now-to-manage-a-telecommuting-spike
- Implementing Effective Security Measures for Your Remote Workforce
  - https://blog.checkpoint.com/2020/03/11/implementing-effective-security-measures-for-your-remote-workforce/
- Hackers find new target as Americans work from home during outbreak
  - https://thehill.com/policy/cybersecurity/487542-hackers-find-new-target-as-americans-work-from-home-during-outbreak
- Security News This Week: Elite Hackers Are Using Coronavirus Emails to Set Traps
  - https://www.wired.com/story/coronavirus-phishing-ad-fraud-clearview-security-news/

References

- https://thehill.com/policy/cybersecurity/487542-hackers-find-new-target-as-americans-work-from-home-during-outbreak
- https://blog.trendmicro.com/suddenly-teleworking-securely/
- https://www.csoonline.com/article/3531963/8-key-security-considerations-for-protecting-remote-workers.html
- https://www.infosecurity-magazine.com/opinions/coronavirus-home-policies/
- https://www.zdnet.com/article/working-from-home-cybersecurity-tips-for-remote-workers/
- https://www.networkworld.com/article/3532440/coronavirus-challenges-remote-networking.html
- https://www.forbes.com/sites/enriquedans/2020/03/17/as-more-people-need-to-work-from-home-companies-need-to-ask-themselves-if-their-it-managers-are-up-to-thetask/
- https://securityboulevard.com/2020/03/securely-work-from-home-during-covid-19/
- https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html
- https://www.zdnet.com/article/covid-19-with-everyone-working-from-home-vpn-security-has-now-become-paramount
- https://securityboulevard.com/2020/03/securely-work-from-home-during-covid-19/
- https://www.infosecurity-magazine.com/opinions/coronavirus-home-policies
- https://www.opm.gov/policy-data-oversight/worklife/federal-work-life-survey/telework-insights.pdf

References

- How coronavirus COVID-19 is accelerating the future of work
- https://www.zdnet.com/article/how-coronavirus-may-accelerate-the-future-of-work/
- https://www.darkreading.com/operations/covid-19-drives-rush-to-remote-work-is-your-security-team-ready/d/d-id/1337294
- https://www.marketwatch.com/story/working-from-home-because-of-coronavirus-dont-give-your-company-a-different-kind-of-virus-2020-03-11
- https://www.pcmag.com/news/7-steps-it-departments-need-to-take-now-to-manage-a-telecommuting-spike
- https://techcrunch.com/2020/03/12/companies-secure-work-from-home-coronavirus/
- Securing Email Data When the Office Computer Comes Home
  - https://www.cisomag.com/securing-microsoft-outlook/
- Agencies expand, loosen telework requirements amid coronavirus spread
  - https://federalnewsnetwork.com/workforce/2020/03/uscis-to-launch-nationwide-telework-program-amid-coronavirus-spread/
- *https://www.pcmag.com/news/att-lifts-data-caps-on-broadband-during-coronavirus-outbreak*

Questions

Questions

Upcoming Briefs

- 2019 Threats posed to Healthcare Sector by use of Third-Party Services
- Access Control on Health Information Systems
- State of the Healthcare Industry: Cybersecurity Edition

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.**

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

Directed 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.**

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV