

Cyber Security: A Federal Perspective



Office of the Chief Information Officer

U.S. Department of Education



Agenda



- Introduction
- Technology Equity and Cybersecurity
- Cybersecurity in a Telework Environment
- Securing Personal Information
- Federal Resources That Can Help
- Other Helpful Resources
- Questions

Introduction

- Steven Hernandez
- MBA, CISSP, CISA, CNSS, CSSLP, SSCP, CAP, ITIL
- Chief Information Security Officer (CISO)
- US Department of Education

- Prior Roles:
- Vice Chairman Board of Directors (ISC)²
- CISO HHS OIG
- Senior Official for Privacy, HHS OIG





Technology Equity and Cybersecurity

- Technology Equity critical for education delivery during COVID.
- Technology Equity can also push the boundaries for “acceptable” hardware/software/services
- Know your limits and requirements for services.
- Know how you can monitor and enforce devices and services.
 - Berkeley
 - <https://technology.berkeley.edu/STEP>
 - <https://security.berkeley.edu/policy/minimum-security-standards-networked-devices-draft>



Technology Equity and Cybersecurity

- [MINIMUM SECURITY STANDARDS FOR NETWORKED DEVICES - DRAFT](#)
- [Patching and Updates Guideline](#)
- [Anti-malware Software Guideline](#)
- [Host-based Firewall Software Guideline](#)
- [Use of Authentication Guidelines](#)
- [Passphrase Guidelines](#)
- [Campus Guidelines for Kiosk Workstations](#)
- [Unnecessary Services Guidelines](#)
- [Privileged Accounts Guidelines](#)



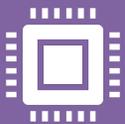
Cybersecurity in a Telework Environment



Organizations have transitioned to working in a remote capacity. Often this meant issuing equipment, realigning support solutions like the service desk, modifying contracts and standing up new capabilities such as increased VPN capacity.



Moving equipment between environments may introduce new risks to the environment. For example, when most equipment is routed through a VPN service or device a certain amount of web filtering takes place that isolates the system and prevents it from reaching out if compromised.



When infected devices are returned to the local area network back at the physical building they are often connected to a different interface that lacks the isolation of modern VPN solutions. In short, if the workforce is returning the building support should be ready for an increase in incidents and service tickets.



Cybersecurity in a Telework Environment

Organizations may not have deployed a fully capable technology stack when issuing equipment for COVID. Many devices may not have been patched for a long time, some devices may be locked out due to time away from the network. And in the worst cases the technology may be badly infected from being off the organization's network for prolonged periods.

Organizations should consider how they are going to reintegrate the devices back into their environment as folks return to facilities. Having a patching and scanning intake process ensuing devices are up to date with patches and scanning is a minimum step all organizations should consider.

If the organization has leveraged cloud services it is a good time to review the devices connected to those cloud services and purge unknown or potentially unauthorized devices.

Cybersecurity in a Telework Environment

Recent Phishing Alerts

- **Education**

- At least 28 universities, colleges and school districts were impacted by ransomware in 2020 Q1, disrupting operations at up to 422 individual schools. In 2019, 89 educational establishments were impacted disrupting operations at up to 1,233 individual schools for an average of 22.25/308.25 per quarter. Incidents in Q1 included:

- Fort Worth Independent School District, Texas
- Gadsden Independent School District, New Mexico
- Spartanburg County School District, South Carolina

- <https://www.threatshub.org/blog/fbi-warns-k12-schools-of-ransomware-attacks-via-rdp/>



July 1st FBI PIN regarding RYUK

The FBI released a Private Industry Notice on July 1st regarding targeted RYUK attacks towards K-12 institutions.

Technical Details

Ryuk has been around since 2018 in many shapes and forms. The Malware takes advantage of weak and insecure Remote Desktop Protocol connections. Ransoms typically range between 100k and 500k.

Cybersecurity in a Telework Environment

Attacking RDP

Scan for exposed RDP ports: The attacker uses free, simple-to-use port-scanning tools such as [Shodan](#) to scan the entire Internet for exposed RDP ports.

Attempt to log in: The attacker tries to gain access to the system (typically as an administrator) using stolen credentials that can be purchased on the black market, or more commonly, brute-force tools that systematically attempt to login using every possible character combination until the correct username and password are found.

Disable security systems: Once the attacker has gained access to the target system, they focus on making the network as insecure as possible. Depending on the privileges of the compromised account, this might involve disabling antivirus software, deleting backups and changing configuration settings that are usually locked down.

Deliver the payload: After security systems have been disabled and the network is suitably vulnerable, the payload is delivered. This might involve installing ransomware on the network, deploying keyloggers, using compromised machines to distribute spam, stealing sensitive data, or installing backdoors that can be used for future attacks.

<https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/>

Cybersecurity in a Telework Environment

Secure RDP



Direct accessibility of systems on the public internet.



Vulnerability and patch management of exposed systems.



Minimize internal lateral movement after initial compromise.



Multi-factor authentication (MFA).



Session security.



Controlling, auditing, and logging remote access.

Cybersecurity in a Telework Environment

Best Practices for Combating the Phishing Threat



Here are some indicators that you can use to identify a phishing/spear phishing attack:

- You don't know the sender or the sender's email address doesn't match the "friendly" name displayed.
- The email is not similar to what you have received from the sender in the past.
- Includes a link or an attachment you weren't expecting or that is out of context for the sender, or both a link and attachment.
- Includes information that may have been found on social media or refers to a current news event.
- Immediate action is required.
- Requests sensitive information about yourself or the Department.
- Contains poor grammar, misspellings, and/or punctuation errors.

To avoid phishing attacks, take the following precautions.

- Slow down and analyze your email messages for common indications of a spear phishing attack.
- Pay attention to web sites' URLs. Malicious web sites may look identical to legitimate ones, but their URLs may use variations in spelling or different domains (e.g., .com vs. .net).
- Don't open an attachment in an email if you weren't expecting or access a web site by clicking links in emails or pop-up messages.
- Digitally sign emails you send and validate digital signatures on emails you receive. Digitally signing emails you send helps others be more efficient with emails containing links or attachments.

Cybersecurity in a Telework Environment

Virtual Private Network (VPN) Solutions



- Remote work options—or telework—require an enterprise virtual private network (VPN) solution to securely connect personnel to an organization’s information technology (IT) network.
- VPNs encrypt traffic between your computer and the internet, even on unsecured Wi-Fi networks.
- Personnel must use the authorized VPN to securely access the organization’s network, systems, and information when teleworking or working remotely. The VPN connection should be established as soon as possible once online.

Cybersecurity in a Telework Environment

Collaboration and Teleconference Tools



Communicate your organization's approved solutions for making calls, facilitating meetings, and collaborating with others to all end users. Consider blocking those that are unauthorized at network boundary points using the provider's IP address, domain, or both.

For Meeting Organizers:

- Require a password for entry or use a lobby to only allow known attendees
- For sensitive information consider a list of passwords sent via sms or another channel to the recipients. Remove those who will not confirm their identity
- If the solution supports "closing" or "locking" your conference do so after the start
- Understand how to remove participants if needed
- Ensure you limit your screenshare. Share in this order when possible: 1. File 2. Application 3. Desktop
- If on webcam blur/replace or be aware of your background
- You may want to inform folks if taking screenshots is ok.

For Meeting Attendees:

- Double check the URL of the meeting you think you are attending
- Make sure your client software is up to date
- Assume everything you share will be recorded and potentially made public. This is exceptionally true when joining free/no cost solutions.

Cybersecurity in a Telework Environment

Cyber Hygiene and The Internet of Things (IoT)



- Technology provides a level of convenience to our lives and connecting a device to the internet is extremely simple. After powering on a device, it requests to connect to your wireless network. Most people, eager to use the functionality, simply grant access without a second thought. But in doing so, the newly connected device may serve as a new point of entry for cybercriminals and other bad actors. For example, recently bad actors gained access to a popular brand of a home security camera and used that access to spy on and harass people.
- When teleworking, it is important to remember to use good cyber hygiene. Organization-furnished equipment must be kept safe, secure, and separated from personal property and information.
- Don't let others, even family members, use your laptop or other devices provided to you for organization.
- Don't use or connect to systems and applications that aren't approved for use by your organization. If you are not sure what is approved, contact your IT Help Desk for assistance.

Cybersecurity in a Telework Environment

Cyber Hygiene and The Internet of Things (IoT) – Digital Assistants



- Digital assistants like Siri on iPhones and iPads and smart speakers such as Amazon Echo and Google Home are configured to constantly listen for commands. When you participate in a conference call from home, your digital assistant may hear and record the sensitive information discussed. Do you know where information you have shared with your digital assistant is stored and who may have access to that information?
- To keep virtual work discussions private and secure, turn off or disable your digital assistant prior to joining any conference calls or virtual meetings where sensitive information may be discussed. Using some basic precautions can help ensure that your meetings are an opportunity to collaborate and work effectively—and not cause a data breach or other embarrassing and costly security or privacy incidents.

Secure Information Sharing



- While teleworking most users focus first on convenience and may unintentionally place sensitive information at risk. To comply with records management requirements and prevent a security or privacy breach:
 - Remember to encrypt email messages containing sensitive information and refrain from including sensitive information in voice mail messages.
 - Organizational information should only be processed, stored or transmitted to authorized organizational devices and services.
 - Official email should not be forwarded to personal accounts (Gmail, Yahoo, MSN, etc.).
 - Only organization authorized alternate storage options such as the use of USB, DVD, or other portable media devices may be used to store or transfer organizational information. These devices must be encrypted using organizational approved encryption methods.

Mobile Apps and Information Sharing



- On August 6, 2020, the President released Executive Order 13942 and 13943 to address the threats posed by TikTok and WeChat. To comply with these orders, TikTok and WeChat applications and services are no longer authorized for use on the Federal networks and government furnished equipment (GFE).
- You should use caution when downloading and using mobile apps. Some popular mobile apps, including TikTok and WeChat, automatically capture vast swaths of information from users, including Internet and other network activity information such as location data and browsing and search histories. This data collection threatens to allow unauthorized access to Americans' personal and proprietary information—potentially allowing the locations of Federal employees and contractors to be tracked with personal information used for blackmail and to conduct corporate espionage.

Social Media and Information Sharing



- As the COVID-19 pandemic continues, many people have turned to social media for distraction and social media quizzes and games have become more prolific. Some encourage you to share information such as the names of all the streets you've lived on, all the cars you've owned, or the song that was popular the year you were born. Or how about the one suggesting you post your senior-year high school photo?
- Although these may seem harmless and fun, many of the questions listed match up with passwords you use or security questions you have set to protect your online accounts. That's because cybercriminals, hackers, scammers and other bad actors use them to collect, use and profit from the personal information you share. The more information a bad actor can trick you into divulging, the easier it is for them to impersonate you or gain access to your passwords and accounts.
- Passwords are the most common means of authentication, but many systems and services have been successfully breached because of non-secure and inadequate passwords. Once a system is compromised, it is open to exploitation by other unwanted sources. No matter how long and strong your password is, a breach is always possible.
- When possible, enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for accounts and services which requires logging in. If MFA is an option, enable it by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. When MFA is not available, be sure to select a strong, complex, memorable password that complies with organizational Password Standards.

Helpful Federal Resources



- US Department of Education
 - <https://studentprivacy.ed.gov/>
 - <https://nces.ed.gov/programs/ptac/>
- FBI
 - Internet Crime Compliant Center (<https://www.ic3.gov/default.aspx>)
 - Local Field Offices (Establish a relationship sooner than later!) <https://www.fbi.gov/contact-us/field-offices>
 - InfraGard (<https://www.infragard.org/>)
- MS-ISAC (<https://www.cisecurity.org/ms-isac/>)
 - Connects back to the US Department of Homeland Security
- Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml)
 - Electronic Crimes Task Forces (ECTFs) (<http://www.secretservice.gov/ectf.shtml>)
- US CERT National Cyber Awareness System <https://us-cert.cisa.gov/ncas>

Other Helpful Resources



- MITRE ATT&CK
 - <https://attack.mitre.org/>
- National Cybersecurity Alliance
 - <https://staysafeonline.org/stay-safe-online/>
 - DHS CISA State and Local NCATS services
 - <https://us-cert.cisa.gov/resources/ncats>
 - <https://us-cert.cisa.gov/resources/slts>

THANKS!!!!



Questions??

Contact me:

Steven G Hernandez

Steven.Hernandez@ed.gov