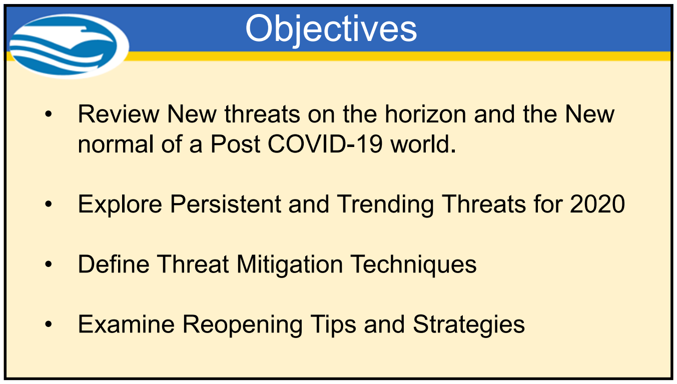
The site ahead contains malware

Attackers currently on **malware.testing.google.test** might attempt to
programs on your Mac that steal or delete your information (for examp
passwords, messages and credit cards).

IT Threats and Risks Associated with the Pandemic

Division of Technology



Objectives

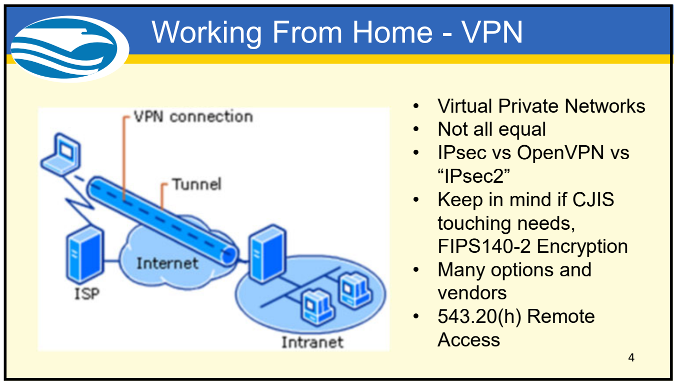
- Review New threats on the horizon and the New normal of a Post COVID-19 world.
- Explore Persistent and Trending Threats for 2020
- Define Threat Mitigation Techniques
- Examine Reopening Tips and Strategies

Socially Distant Tech Concerns

- How are you distancing?
- Variance checks
- Signature checks

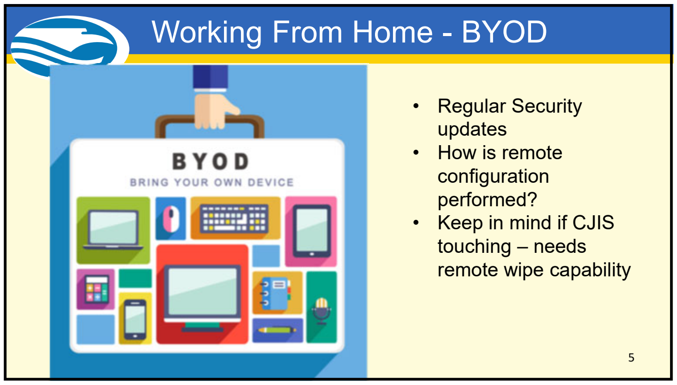
- Surveillance concerns?
- Working socially distant

3



Working From Home - VPN

- Virtual Private Networks
- Not all equal
- IPsec vs OpenVPN vs “IPsec2”
- Keep in mind if CJIS touching needs, FIPS140-2 Encryption
- Many options and vendors
- 543.20(h) Remote Access



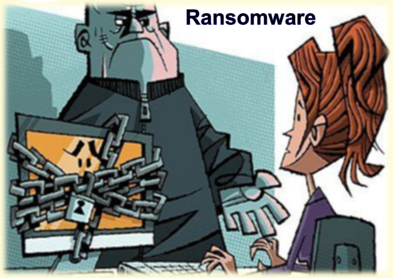
Working From Home - BYOD

- Regular Security updates
- How is remote configuration performed?
- Keep in mind if CJIS touching – needs remote wipe capability

Working From Home - Conferencing

- How secure is it?
- What configuration is needed to create or join? (543.20(e) Logical Security)
- “Zoombombing”
- Where and what kind of data are stored?

Persistent Threats

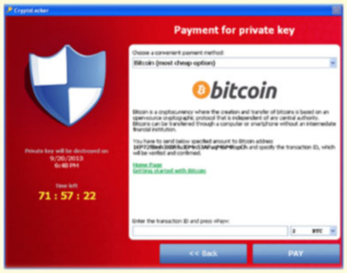


- Increase of over 77% 2018 vs 2019 Q1/Q2
- Decrease in variety of code
- WannaCry (MS17-10)
- More targeting of research and communication

Source: TrendMicro

7

What is Ransomware?



CryptoLocker

Payment for private key

Choose a convenient payment method:

Bitcoin (most cheap option)

bitcoin

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.

You have to send below specified amount to Bitcoin address [illegible] and specify the transaction ID, which will be verified and confirmed.

Home Page
Getting started with Bitcoin

Private key will be destroyed on
9/20/2013
6:40 PM

Time left
71 : 57 : 22

Enter the transaction ID and press «Pay»:

2 BTC

<< Back

PAY

- Malicious software is executed remotely
- Critical files are encrypted
- Payment is demanded to decrypt files
- Attackers can wait months to strike.

8

Why is Ransomware so common?

- Phishing and other social engineering attacks
- Poor user controls
- Poor logical security
- Insufficient data backups
- User education

543.20(f) 543.20(e) 543.20(j)

9

Persistent Threats (Continued)

"Any act that influences a person to take an action that may or may not be in their best interest." – Social Engineer Inc.

Many Types:
- Phishing
- Spear phishing
- Baiting
- Quid Pro Quo
- BEC (Business Email Compromise)
- Vishing (Voice phishing)

"Social engineering is the act of tricking someone into divulging information or taking action, usually through technology." - NortonLifeLock

10

Social Engineering Example 1

Credit: Youtube

11

Social Engineering Targets/Tools

Many Types of Info. Targets
- Who handles IT
- What browser is used
- What OS is in use
- How do they open PDFs
- Who does food service, janitor, pest-control, trash service
- Rem: Social Media, Job Sites, Hacker sites.

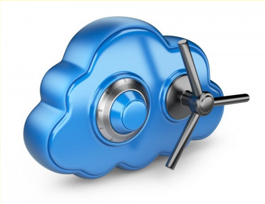
12

Social Engineering Example 2

WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES

Credit: Youtube

Mitigating Risk



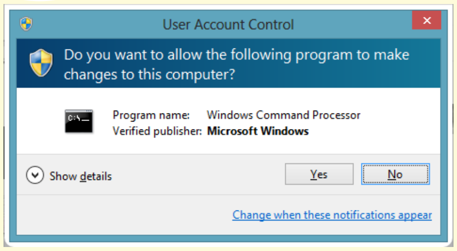
Data Backups
- 543.20(j)
- Recovery procedures
- Tested Procedures

Incident Management
- 543.20(i)
- BCP (Backup Continuity Plan)

Backup Continuity Plans

- ITIL Continuity Management
- ISO 22301
- Identify critical areas
- Identify responsible parties
- Identify recovery procedures
- Annual Testing - 543.20(j)(3)

Mitigate Risks (Continued)


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**

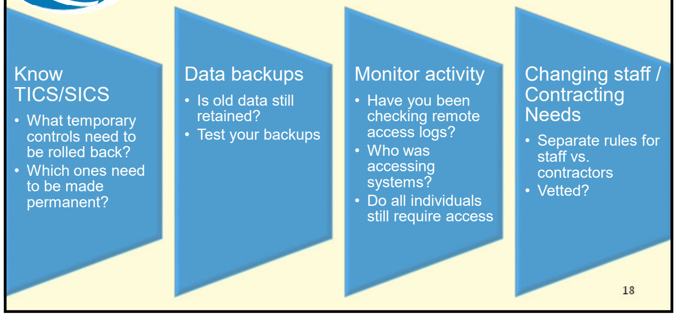
- Limit user access
- Segregate networks
- 543.20(f) User Controls

Mitigating Risks (Continued)

Change Management
- Patch Management
- 543.20(g)

User Education
- Awareness training
- NIST SP 800-50

Reopening Strategy/Tips

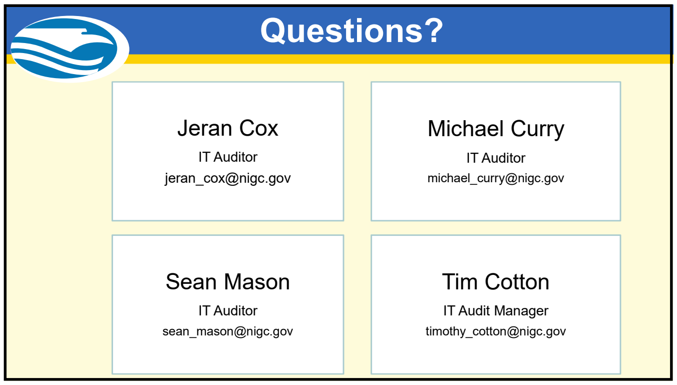


Know TICS/SICS
- What temporary controls need to be rolled back?
- Which ones need to be made permanent?

Data backups
- Is old data still retained?
- Test your backups

Monitor activity
- Have you been checking remote access logs?
- Who was accessing systems?
- Do all individuals still require access

Changing staff / Contracting Needs
- Separate rules for staff vs. contractors
- Vetted?



Questions?

Jeran Cox
IT Auditor
jeran_cox@nigc.gov

Michael Curry
IT Auditor
michael_curry@nigc.gov

Sean Mason
IT Auditor
sean_mason@nigc.gov

Tim Cotton
IT Audit Manager
timothy_cotton@nigc.gov