“Cybersecurity and the Broadcast Station”

Wayne M. Pecena CPBE, AMD, ATSC3, DRB, 8VSB, CBNE

Texas A&M University

“Cybersecurity and the Broadcast Station”

Advertised Presentation Scope:

The broadcast technical plant relies on Information Technology (IT) and the Internet Protocol (IP) infrastructure whether a small radio station or a state of the art ATSC 3 TV facility, Protecting the infrastructure against cyber threats grows more challenging each year for the broadcast IT engineer. Threats can vary from emailed ransomware to potential piracy of ATSC 3.0 signals to overall disruption of broadcast content. It is essential to know your vulnerabilities and potential exposure to cyber criminals and implement the necessary precautions. This presentation will outline key cybersecurity principles and provide practical prevention steps you can take to mitigate cyber threats to broadcast facilities of any size.

AGENDA:
Cybersecurity Principals & Foundation
Threats & Threat Actors (ransomware focus)
What About ATSC 3?
Mitigation & Prevention Tasks
Takeaway Thoughts & Resources

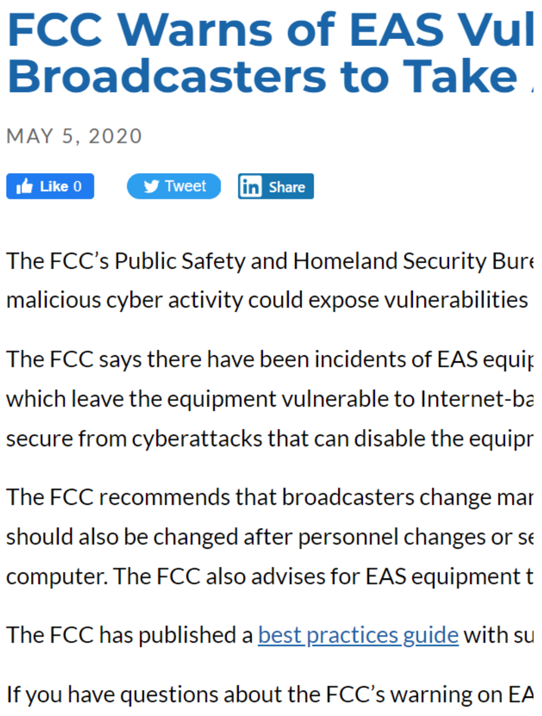
What is Cybersecurity

- ***Cybersecurity is focused upon the protection of computers, networks, programs and data from change, destruction, or disruption.***

Cyber attack focus areas:
System tampering
(network infrastructure, servers, hosts)
Sensitive information access / tampering / extortion
Operational disruption
Data encryption extortion

- Risks:
  - Dead Air
  - Impact Upon Resources
  - Loss of Revenue
  - Public Embarrassment
  - Breach of Data
  - Potential Liability
  - Lost Trust

Cybersecurity Rules & Regulation for Broadcast Stations



FCC Warns of EAS Vul
Broadcasters to Take

MAY 5, 2020

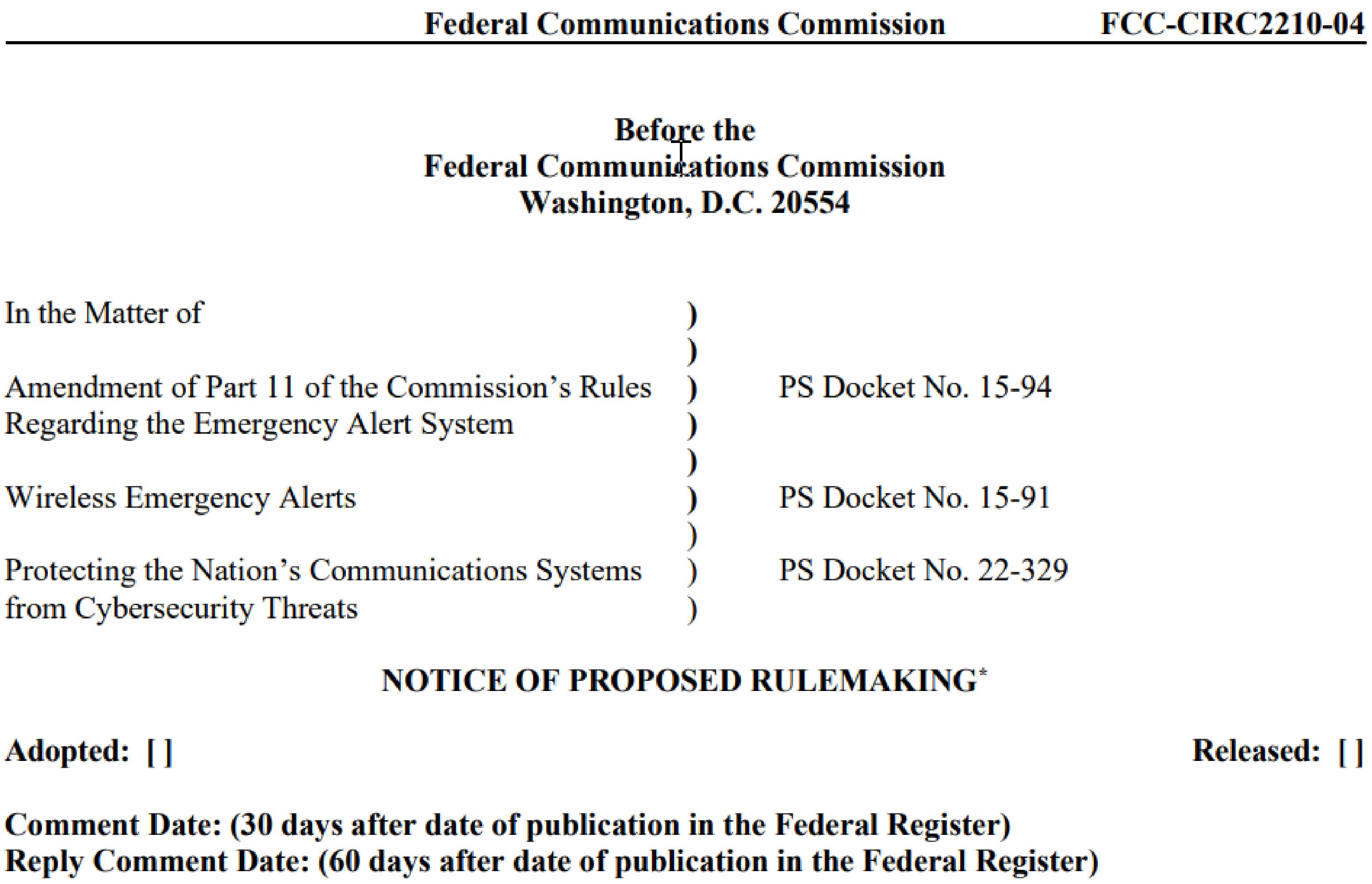
The FCC's Public Safety and Homeland Security Bure
malicious cyber activity could expose vulnerabilities

The FCC says there have been incidents of EAS equip
which leave the equipment vulnerable to Internet-ba
secure from cyberattacks that can disable the equipr

The FCC recommends that broadcasters change mar
should also be changed after personnel changes or se
computer. The FCC also advises for EAS equipment t

The FCC has published a best practices guide with su

If you have questions about the FCC's warning on EA



Federal Communications Commission **FCC-CIRC2210-04**

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System	)	PS Docket No. 15-94
	)	
Wireless Emergency Alerts	)	PS Docket No. 15-91
	)	
Protecting the Nation's Communications Systems from Cybersecurity Threats	)	PS Docket No. 22-329

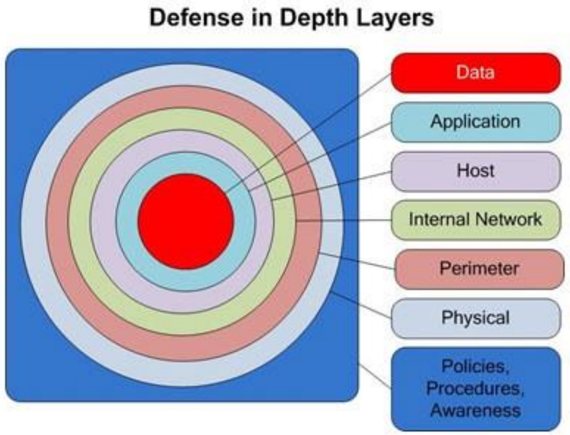
NOTICE OF PROPOSED RULEMAKING*

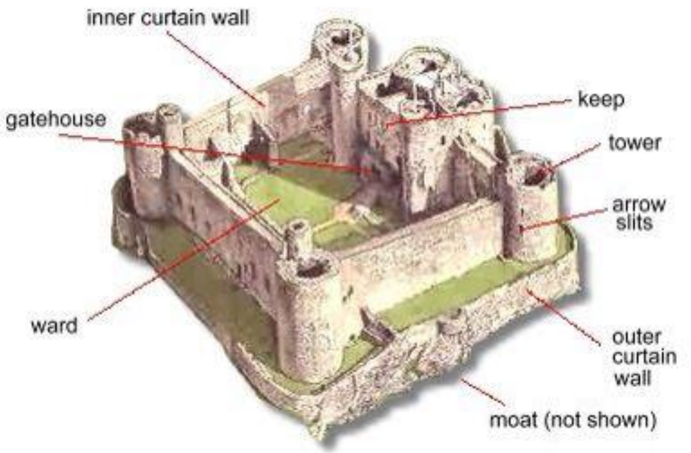
Adopted: [ ] **Released: [ ]**

Comment Date: (30 days after date of publication in the Federal Register)
Reply Comment Date: (60 days after date of publication in the Federal Register)

Key Cybersecurity Principals

Defense-in-Depth



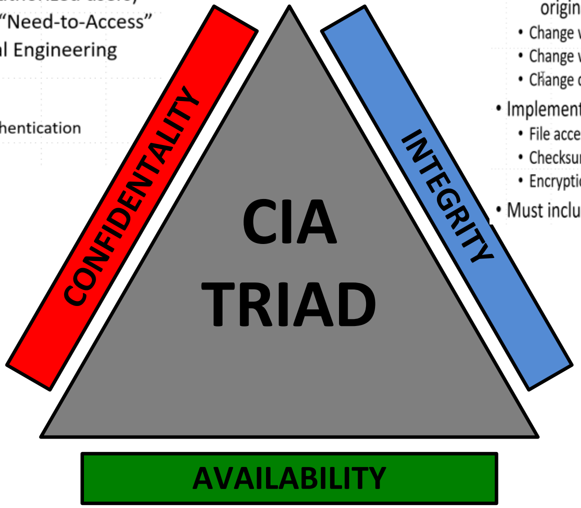


Harlech Castle, North Wales, built in 1283 AD

Least Privilege

CIA Triad

- Can be equated to Privacy!
  - Preventing information (data) to reaching the wrong hands (unauthorized users)
  - Restrict / Limit access – “Need-to-Access”
  - Often the target of Social Engineering
  - Implemented by:
    - Data encryption
    - Passwords / 2-factor authentication
    - Off-Line data storage



- Preventing information (data integrity) to be changed through an IT workflow and originating at a known source (source integrity)
  - Change when traversing a network
  - Change when stored
  - Change during processing
- Implemented by:
  - File access controls
  - Checksums
  - Encryption
- Must include detection mechanism(s)

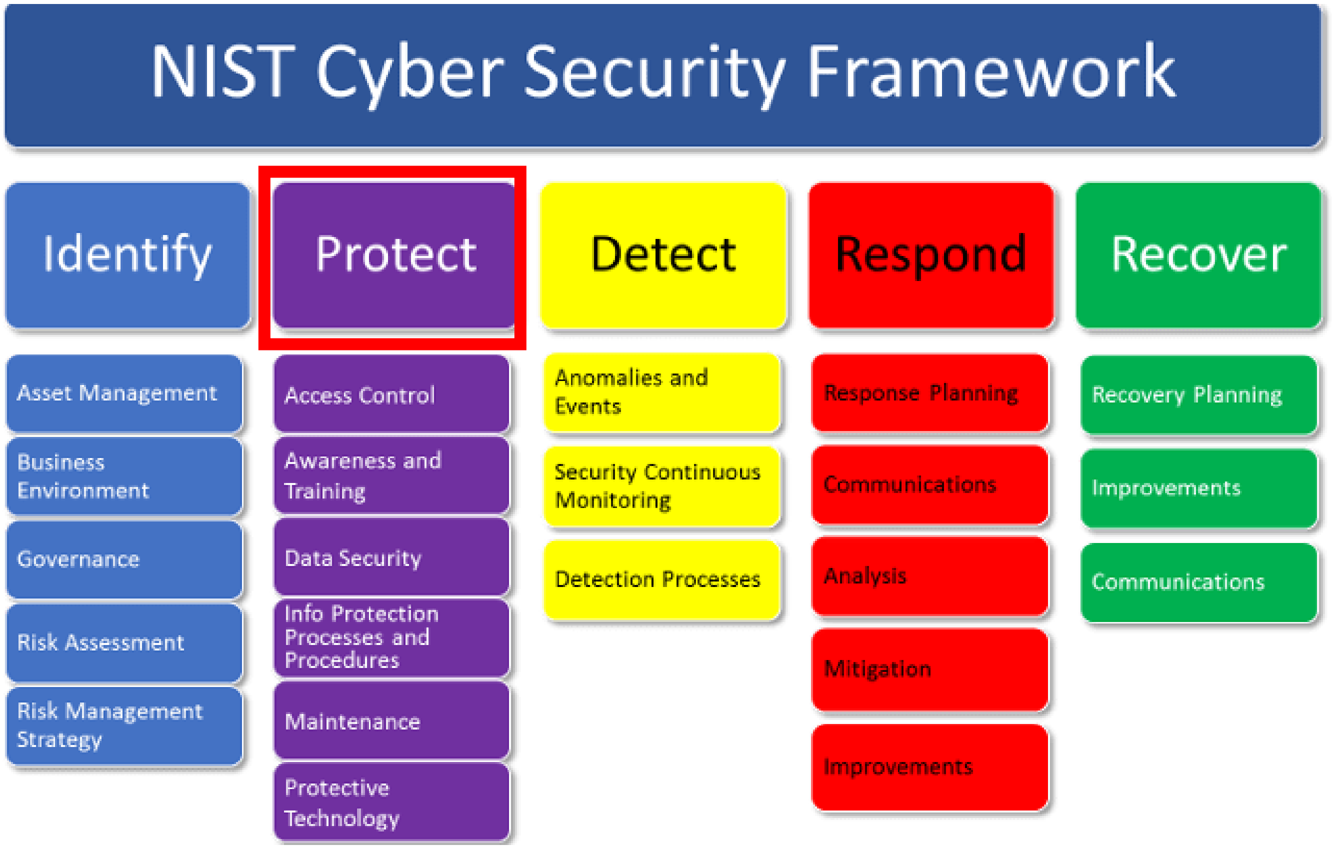
- Insuring resources are available!
  - Network
  - Servers (infrastructure)
  - Applications
- Often the target of:
  - “DoS” or “DDoS” attacks
  - Ransomware
- Implemented by:
  - Redundancy – network infrastructure
  - Redundancy – auto-failover servers
  - Intrusion detection

NIST Cybersecurity Framework

https://www.nist.gov/cyberframework/framework

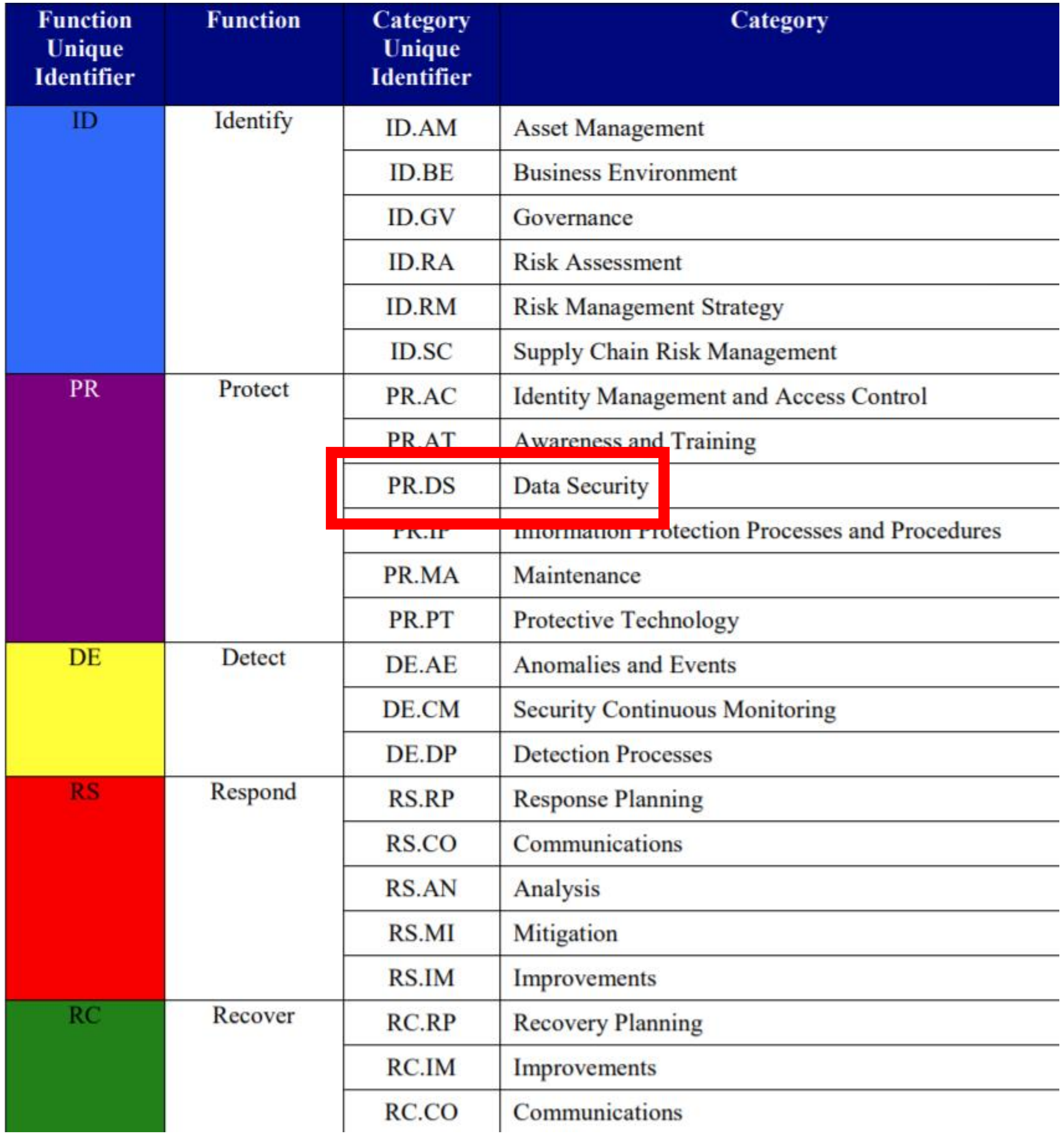
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

- National Institute for Standards & Technology “NIST”
  - Provides a structured outline of best practices
  - Industry guideline baseline
- 5 Framework Core Areas:
  - Identify – all IT assets & create policy
  - Protect – control access, encrypt data
  - Detect – monitor network activity
  - Respond – business continuity plan
  - Recover – restore impacted areas

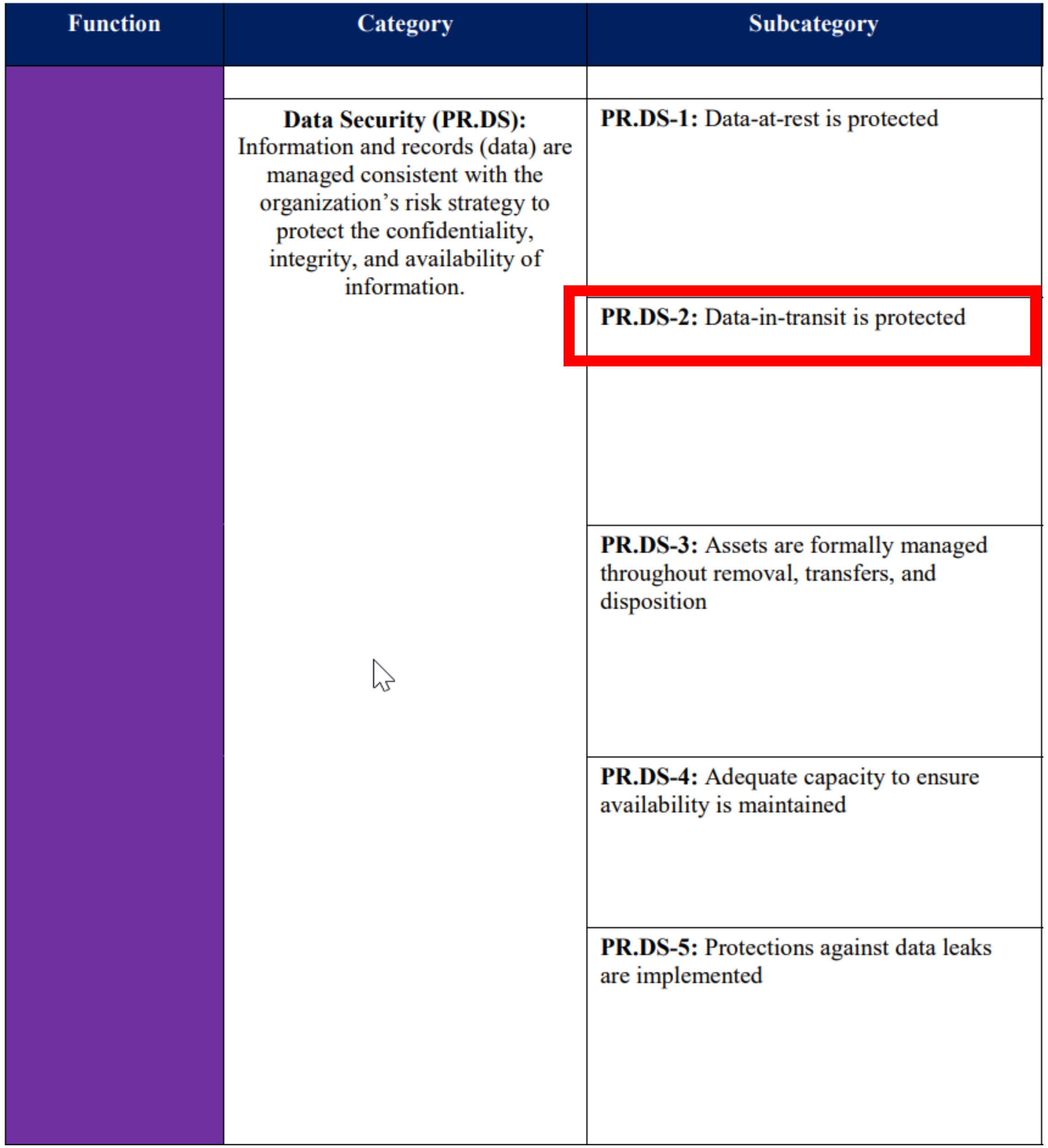


NIST Cyber Security Framework

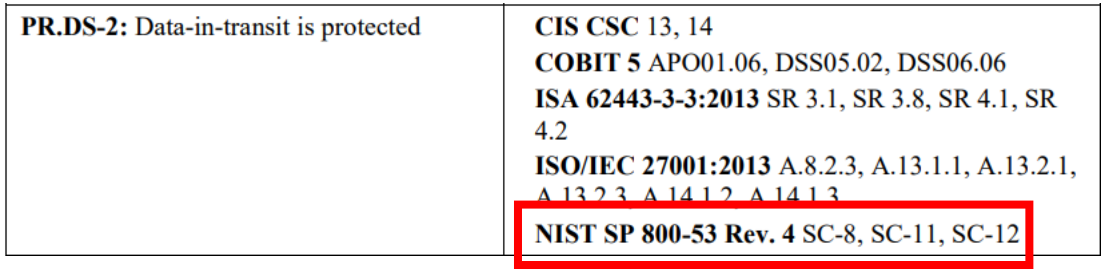
Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			



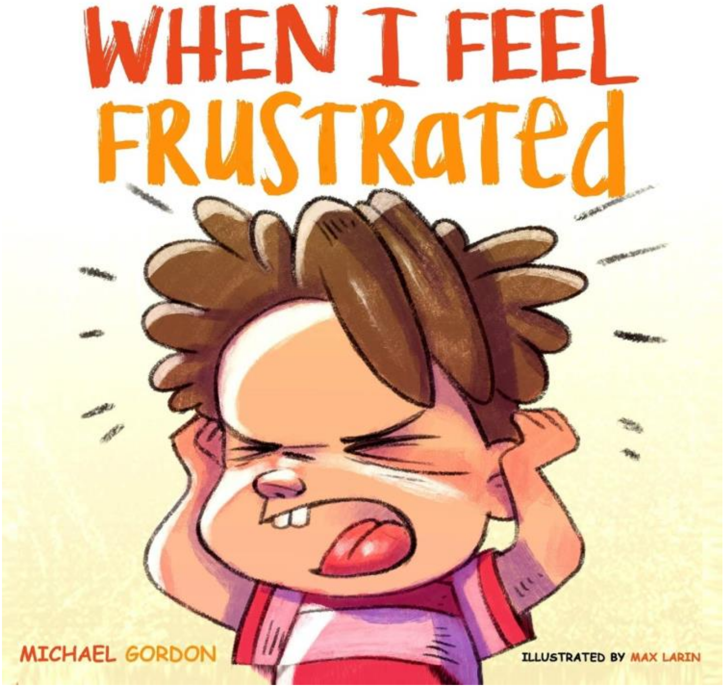
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

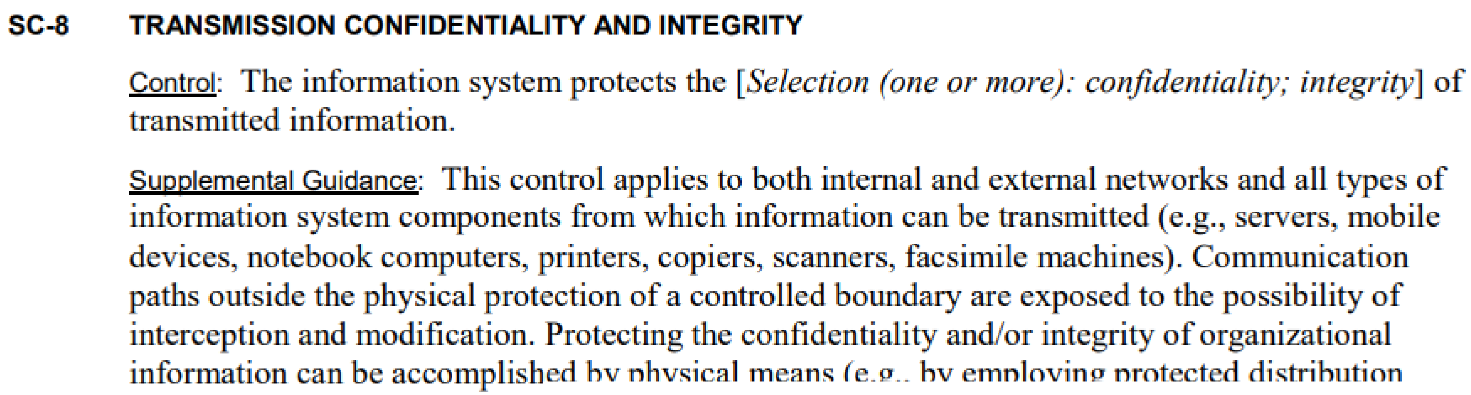


Function	Category	Subcategory
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
		PR.DS-4: Adequate capacity to ensure availability is maintained
		PR.DS-5: Protections against data leaks are implemented



PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12

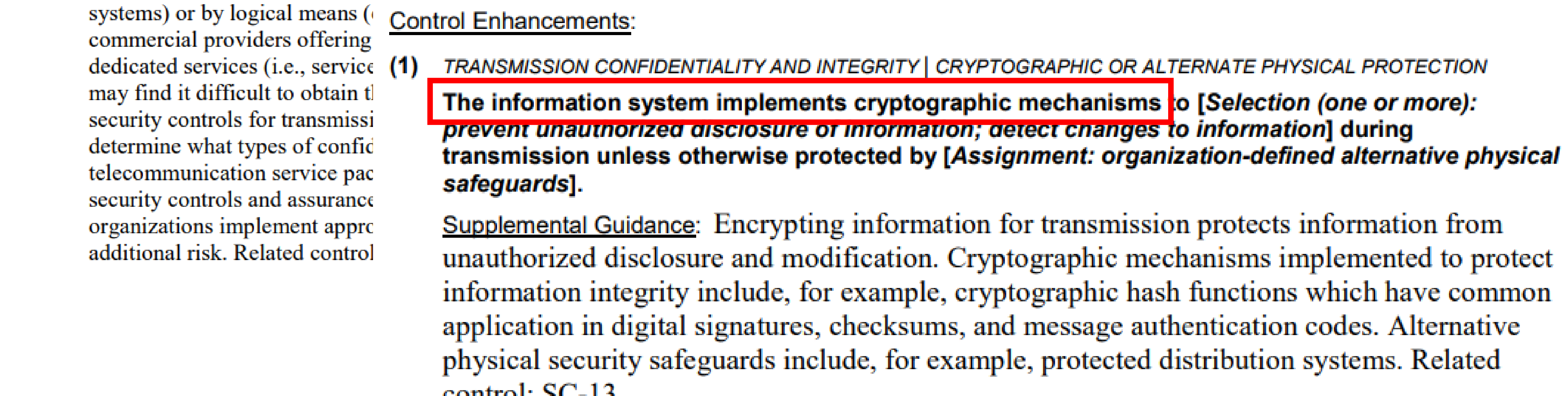




SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution



systems) or by logical means (
commercial providers offering
dedicated services (i.e., service
may find it difficult to obtain t
security controls for transmissi
determine what types of confid
telecommunication service pac
security controls and assurance
organizations implement appro
additional risk. Related control

Control Enhancements:

(1) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*

The information system implements cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.

Threats & Threat Actors

(ransomware focus)

Cybersecurity Sources & Threats

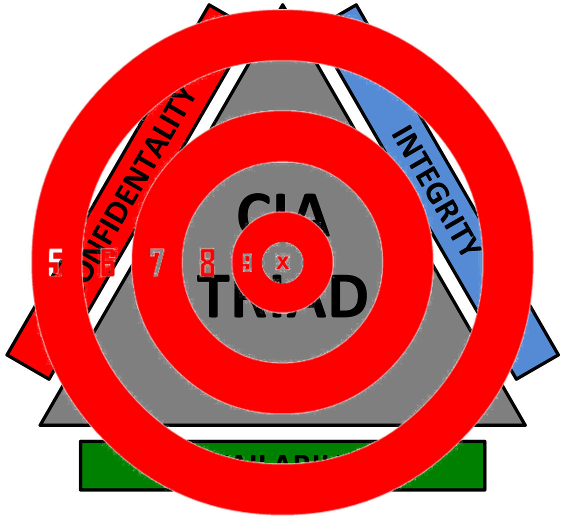
- Malicious Source:
  - Hacktivist
  - Nation states
  - Terrorist groups
  - "Black Hat" malicious hacker
  - Script "kiddies"
  - Cyber Gangs / organized crime
  - Disgruntled employee
- Non-Malicious Source:
  - Accidental actions
  - Natural disasters

BlackCat (ALPHV)
Black Basta
Hive

Cybersecurity Preparation helps recovery!

- Malware:
  - Ransomware
  - Virus
  - Worms
  - Trojan
  - Spyware (key logger)
  - Rootkit
- Infrastructure / Network:
  - DHCP Snooping
  - ARP Spoofing (IP Address Spoofing)
  - Rogue Router Advertisements
  - Denial of Service Attacks - DoS
  - Distributed Denial of Service Attacks - DDoS
  - Application Layer Attacks

“CIA” Triad & the “Hacker”



Confidentiality

- Breaching organization’s data
- Decoding encryption
- Exposing sensitive information
- Social engineering attacks

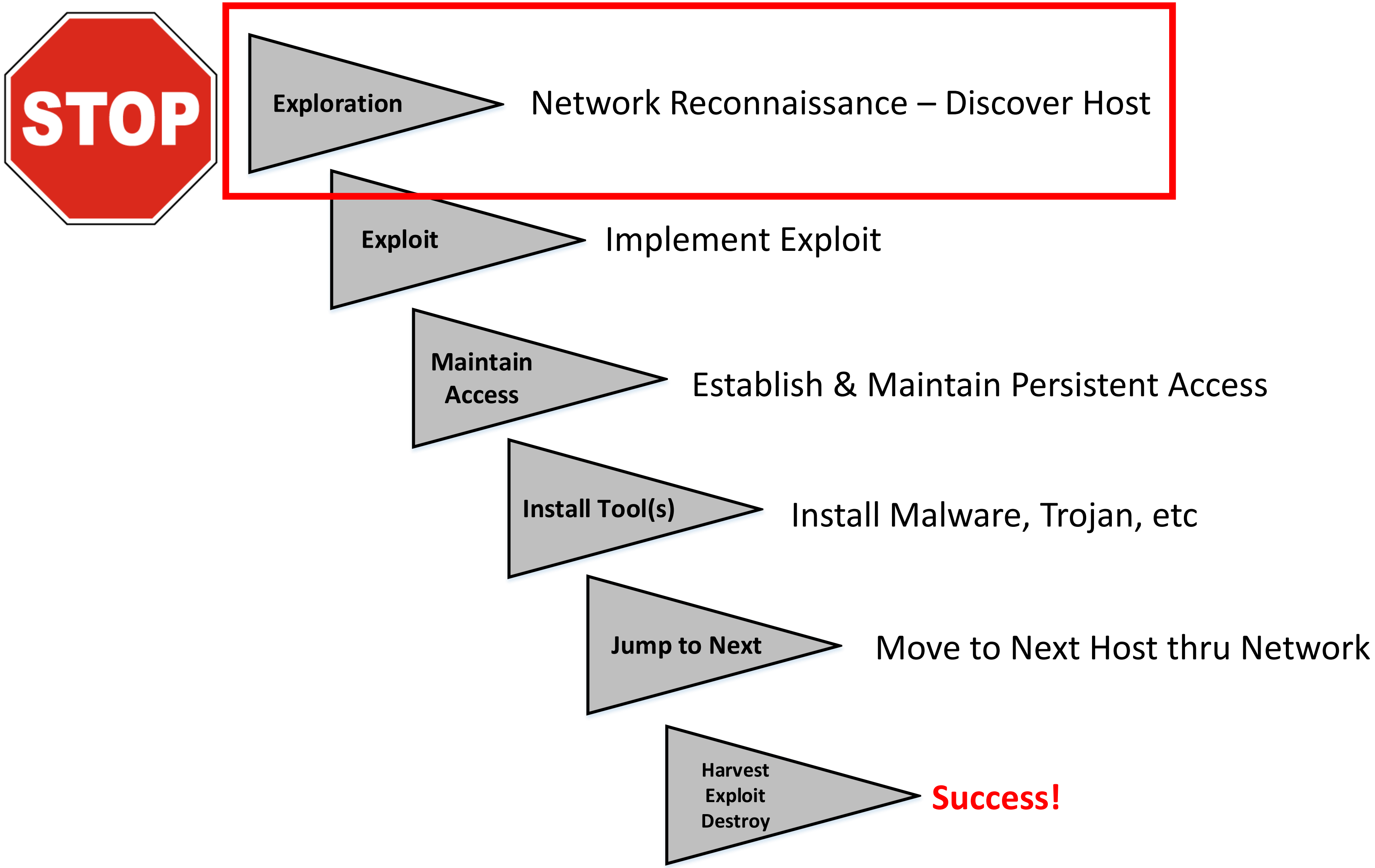
Integrity

- Man-in-the Middle attacks
- Embedded malware
- Data record manipulation
- Social engineering attacks

Availability

- Denial of Service (DoS) attack
- Distributed DoS (DDoS) attack
- Network outages
- Ransomware
- Viruses / Malware
- Infrastructure damage

The Cybersecurity Attack



Exploration — Network Reconnaissance – Discover Host

Exploit — Implement Exploit

Maintain Access — Establish & Maintain Persistent Access

Install Tool(s) — Install Malware, Trojan, etc

Jump to Next — Move to Next Host thru Network

Harvest Exploit Destroy — **Success!**

1st Step in Network Security

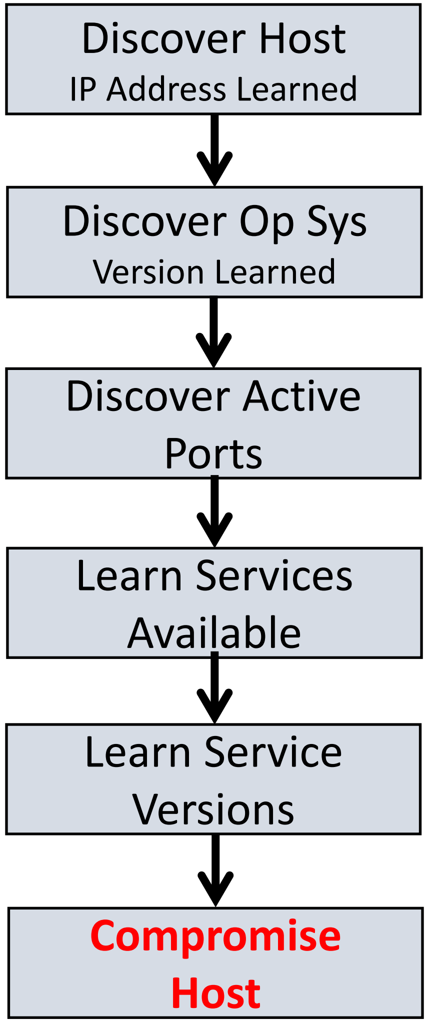
Prevent Reconnaissance
Exploration or Probing
of the Network

1st Step in Network Security

Network Reconnaissance

What Can You Learn?

Prevent Reconnaissance
Exploration or Probing
of the Network


Discover Host
IP Address Learned

Discover Op Sys
Version Learned

Discover Active Ports

Learn Services Available

Learn Service Versions

Compromise Host

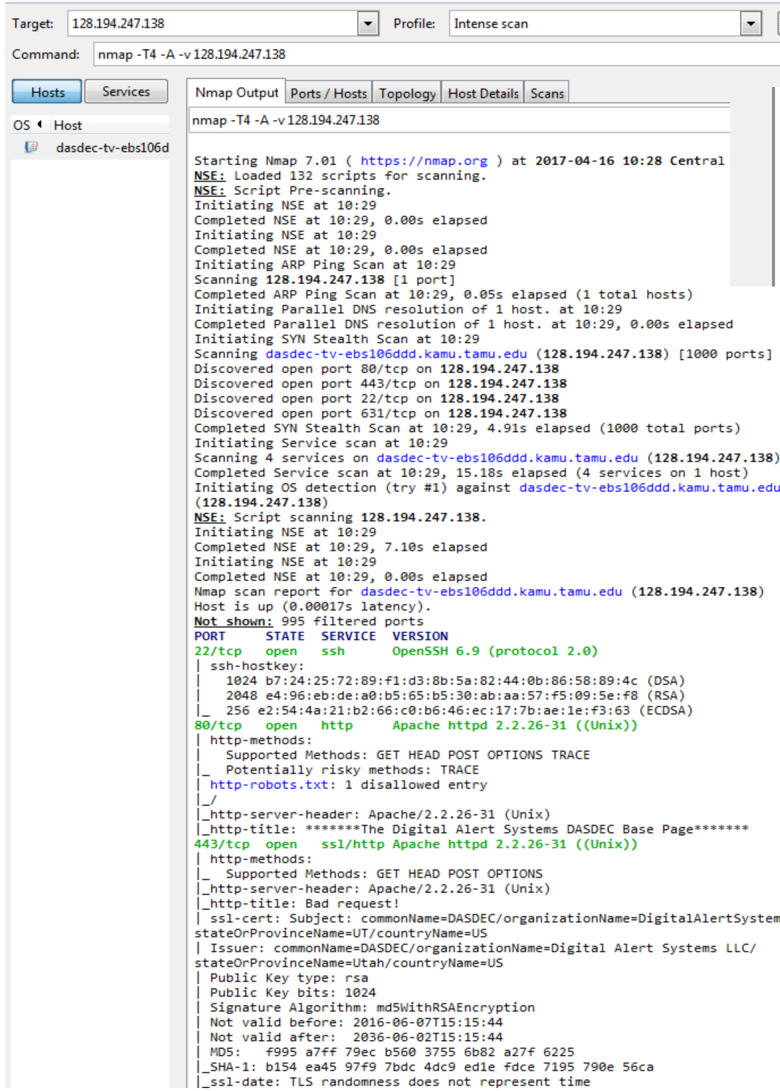
Vulnerability?

Vulnerability?

Insight to Compromise Host

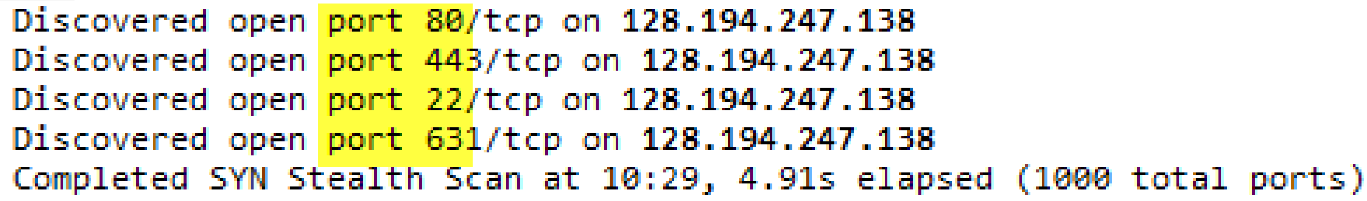
Vulnerability?
Default login?

Port:
80 - HTTP
443 - HTTPS
22 - SSH
631 - IPP

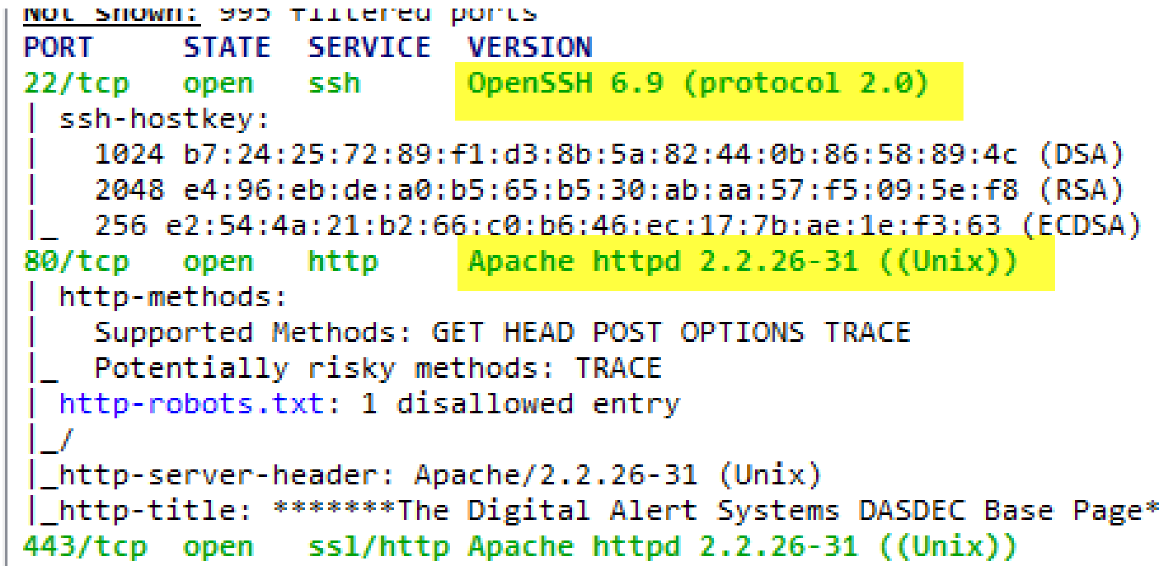


Target: 128.194.247.138
Profile: Intense scan
Command: nmap -T4 -A -v 128.194.247.138

```
nmap -T4 -A -v 128.194.247.138

Starting Nmap 7.01 ( https://nmap.org ) at 2017-04-16 10:28 Central
NSE: Loaded 132 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:29
Completed NSE at 10:29, 0.00s elapsed
Initiating NSE at 10:29
Completed NSE at 10:29, 0.00s elapsed
Initiating ARP Ping Scan at 10:29
Scanning 128.194.247.138 [1 port]
Completed ARP Ping Scan at 10:29, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:29
Completed Parallel DNS resolution of 1 host. at 10:29, 0.00s elapsed
Initiating SYN Stealth Scan at 10:29
Scanning dasdec-tv-ebs106ddd.kamu.tamu.edu (128.194.247.138) [1000 ports]
Discovered open port 80/tcp on 128.194.247.138
Discovered open port 443/tcp on 128.194.247.138
Discovered open port 22/tcp on 128.194.247.138
Discovered open port 631/tcp on 128.194.247.138
Completed SYN Stealth Scan at 10:29, 4.91s elapsed (1000 total ports)
Initiating Service scan at 10:29
Scanning 4 services on dasdec-tv-ebs106ddd.kamu.tamu.edu (128.194.247.138)
Completed Service scan at 10:29, 15.18s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against dasdec-tv-ebs106ddd.kamu.tamu.edu
(128.194.247.138)
NSE: Script scanning 128.194.247.138.
Initiating NSE at 10:29
Completed NSE at 10:29, 7.10s elapsed
Initiating NSE at 10:29
Completed NSE at 10:29, 0.00s elapsed
Nmap scan report for dasdec-tv-ebs106ddd.kamu.tamu.edu (128.194.247.138)
Host is up (0.00017s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 6.9 (protocol 2.0)
| ssh-hostkey:
|   1024 b7:24:25:72:89:f1:d3:8b:5a:82:44:0b:86:58:89:4c (DSA)
|   2048 e4:96:eb:de:a0:b5:65:b5:30:ab:aa:57:f5:09:5e:f8 (RSA)
|_  256 e2:54:4a:21:b2:66:c0:b6:46:ec:17:7b:ae:1e:f3:63 (ECDSA)
80/tcp   open   http     Apache httpd 2.2.26-31 ((Unix))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.2.26-31 (Unix)
|_http-title: *******The Digital Alert Systems DASDEC Base Page*******
443/tcp  open   ssl/http Apache httpd 2.2.26-31 ((Unix))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.26-31 (Unix)
|_http-title: Bad request!
| ssl-cert: Subject: commonName=DASDEC/organizationName=DigitalAlertSystemsLLC/
stateOrProvinceName=UT/countryName=US
| Issuer: commonName=DASDEC/organizationName=Digital Alert Systems LLC/
stateOrProvinceName=Utah/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2016-06-07T15:15:44
| Not valid after:  2036-06-02T15:15:44
| MD5:   f995 a7ff 79ec b560 3755 6b82 a27f 6225
|_SHA-1: b154 ea45 97f9 7bdc 4dc9 ed1e fdce 7195 790e 56ca
|_ssl-date: TLS randomness does not represent time
```



```
Discovered open port 80/tcp on 128.194.247.138
Discovered open port 443/tcp on 128.194.247.138
Discovered open port 22/tcp on 128.194.247.138
Discovered open port 631/tcp on 128.194.247.138
Completed SYN Stealth Scan at 10:29, 4.91s elapsed (1000 total ports)
```

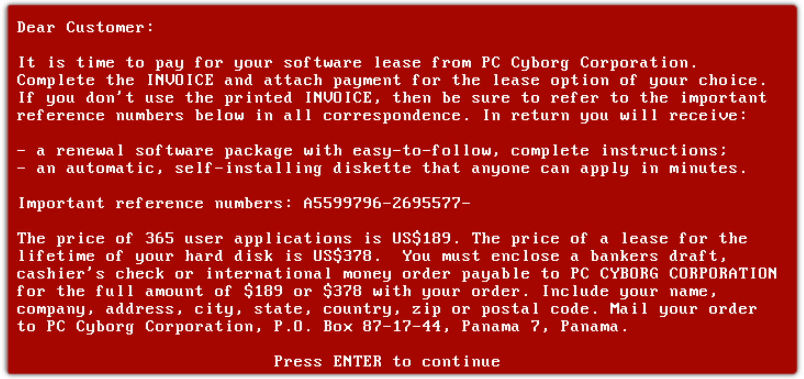


```
Not shown: 995 filtered ports
PORT     STATE  SERVICE  VERSION
22/tcp   open   ssh      OpenSSH 6.9 (protocol 2.0)
| ssh-hostkey:
|   1024 b7:24:25:72:89:f1:d3:8b:5a:82:44:0b:86:58:89:4c (DSA)
|   2048 e4:96:eb:de:a0:b5:65:b5:30:ab:aa:57:f5:09:5e:f8 (RSA)
|_  256 e2:54:4a:21:b2:66:c0:b6:46:ec:17:7b:ae:1e:f3:63 (ECDSA)
80/tcp   open   http     Apache httpd 2.2.26-31 ((Unix))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.2.26-31 (Unix)
|_http-title: *******The Digital Alert Systems DASDEC Base Page*
443/tcp  open   ssl/http Apache httpd 2.2.26-31 ((Unix))
```

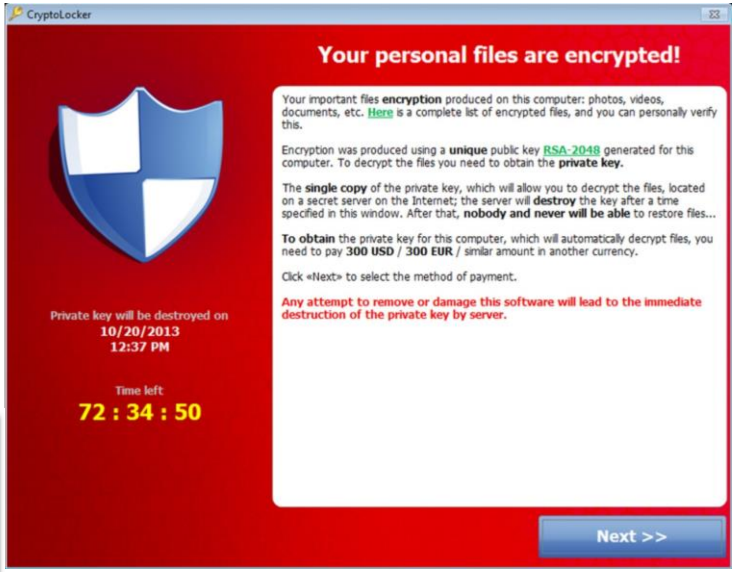
A Focus on Ransomware

- What is Ransomware?
- Evolving malicious malware:
  - Encrypts files
  - May block system access
  - May disclose sensitive information
- Ransom demand ($$$ bitcoins $$$):
  - De-encrypt (restore) files
  - Not disclose information
- Generic types:
  - Locker ransomware – impact to host functions
  - Crypto ransomware – individual files encrypted
- Many variants today – continues to evolve!

Cryptolocker



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                          Press ENTER to continue
```



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt the files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

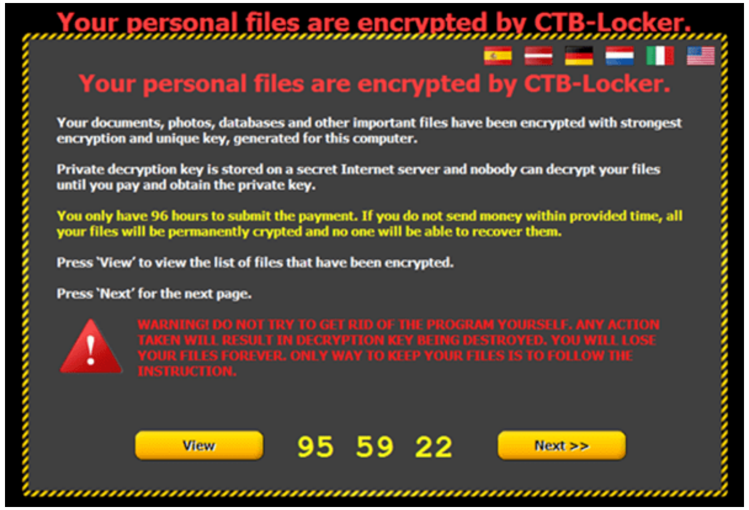
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

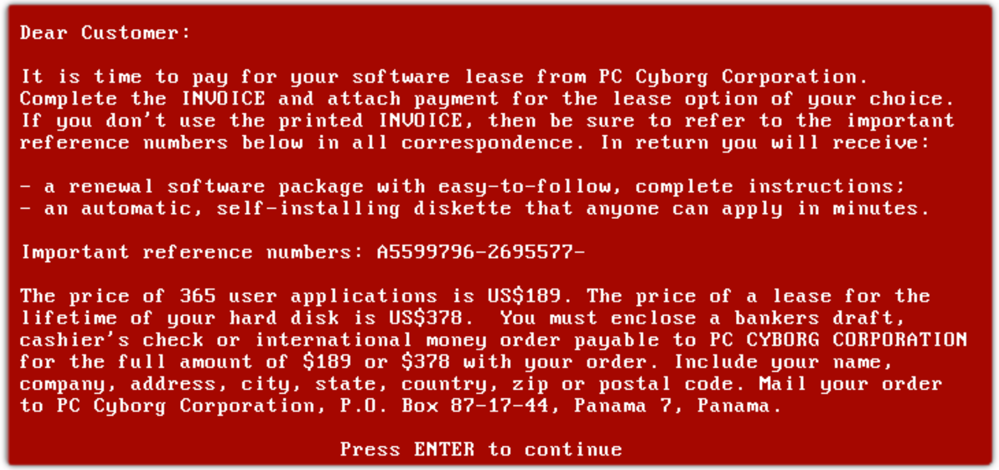
Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

95 59 22

Ransomware Variants



```
Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378.  You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

                         Press ENTER to continue
```

- First ransomware appears in 1989
- Revil / Sodinokibi
  - File encryption – increasing ransom over time
- Maze
  - File encryption & threat of public release of sensitive information
- Ryuk
  - File encryption & system access blocked
- Tycoon
  - File encryption - targets VPN encryption
- NetWalker
  - File encryption – targets network connected Windows hosts

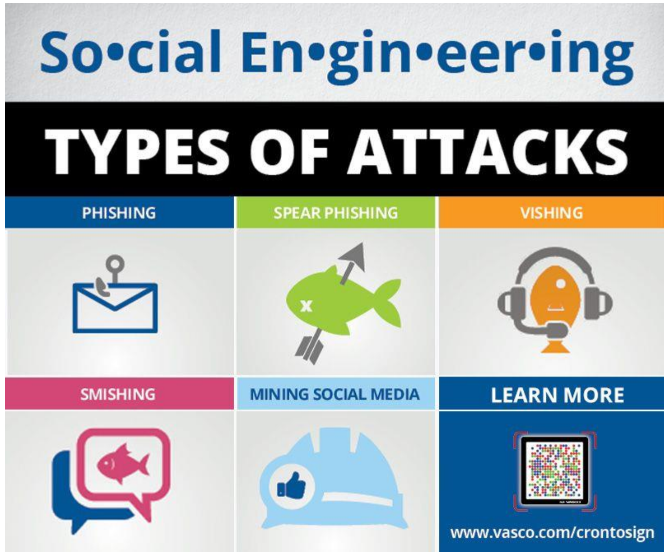
LockBit 3.0
Most Popular
Today

- Satan
- Netwalker
- Cerber
- Egregor
- Hostman
- WannaCry
- Philadelphia
- MacRansom
- Atom
- FLUX
- Tox
- REvil
- Ryuk
- Encryptor
- Fakben
- ORX Locker
- Alpha Locker
- Hidden Tear
- Janus
- Ransom3

Delivering Ransomware

- email Phishing
  - email attachments (malicious)
  - email links (malicious)
- “Drive-By” file download
  - Exploit kit downloaded
- Protocol (RDP) exploit
- Macro execution
- External USB “candy drop”
- Pirated software

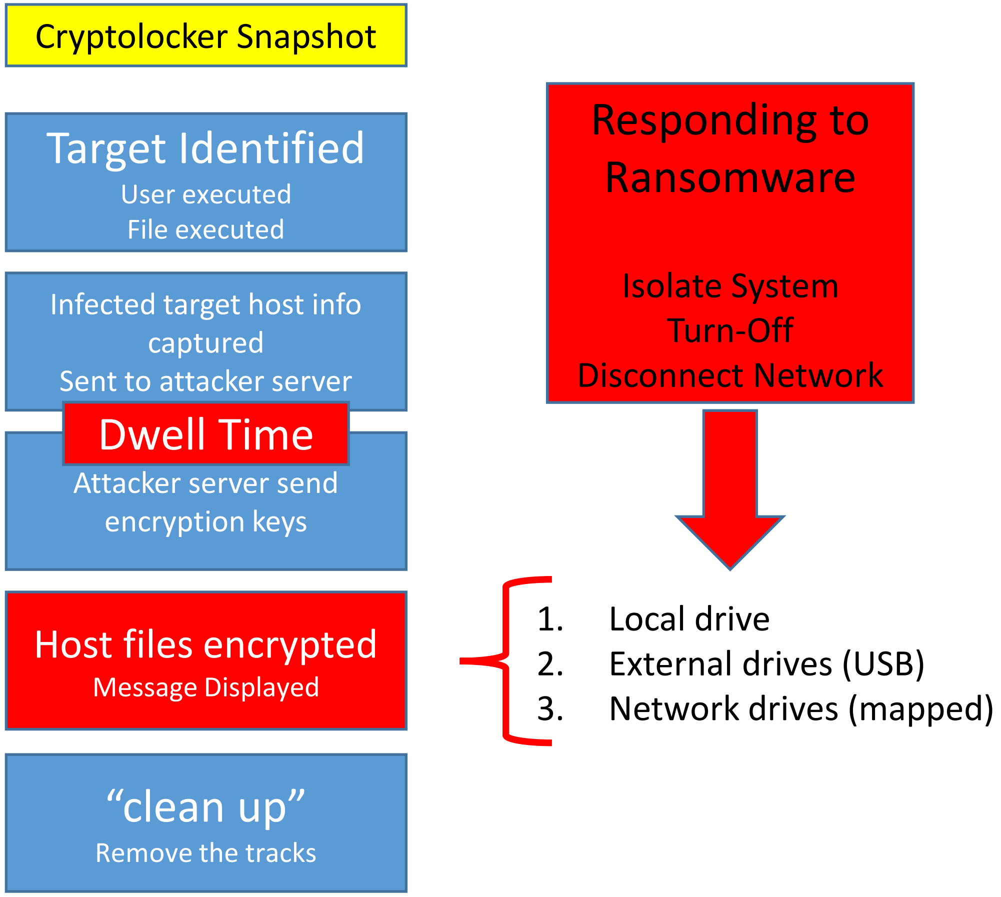
- Popular tactics:
  - Spear-phishing – target specific audience
  - Whaling – spear-phishing target at upper level (C suite)
  - Smishing/vishing – SMS based focused on personalization & urgency
- Popular tricks:
  - Playing off emotions (establish trust)
  - Pretexting
  - Wide-net phishing (common service based)



Social Engineering

- Use of deception to obtain information
- Actors prey upon human “willingness to be helpful”
  - Persuasive tactics
  - Psychological manipulation
- Has become a successful technique:
  - System exploits often more difficult
  - Often easier to exploit human weakness
- Based upon principals of influence:
  - Reciprocity
  - Commitment
  - Social Proof
  - Authority
  - Liking
  - Scarcity

Ransomware Workflow Example



Cryptolocker Snapshot

Target Identified
User executed
File executed

Infected target host info captured
Sent to attacker server

Dwell Time
Attacker server send encryption keys

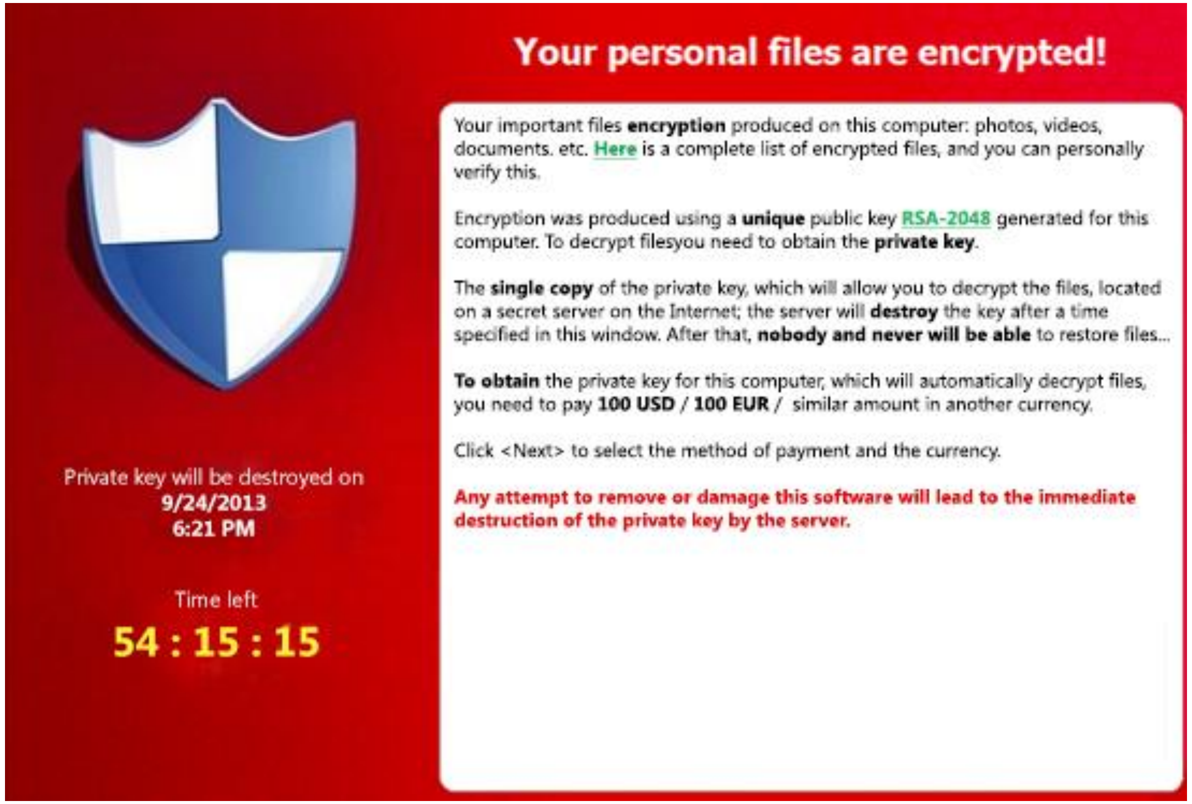
Host files encrypted
Message Displayed

“clean up”
Remove the tracks

Responding to Ransomware

Isolate System
Turn-Off
Disconnect Network

1. Local drive
2. External drives (USB)
3. Network drives (mapped)



Your personal files are encrypted!

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 15

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

SBE

What About ATSC 3.0 ?

ROAD TO ATSC 3.0

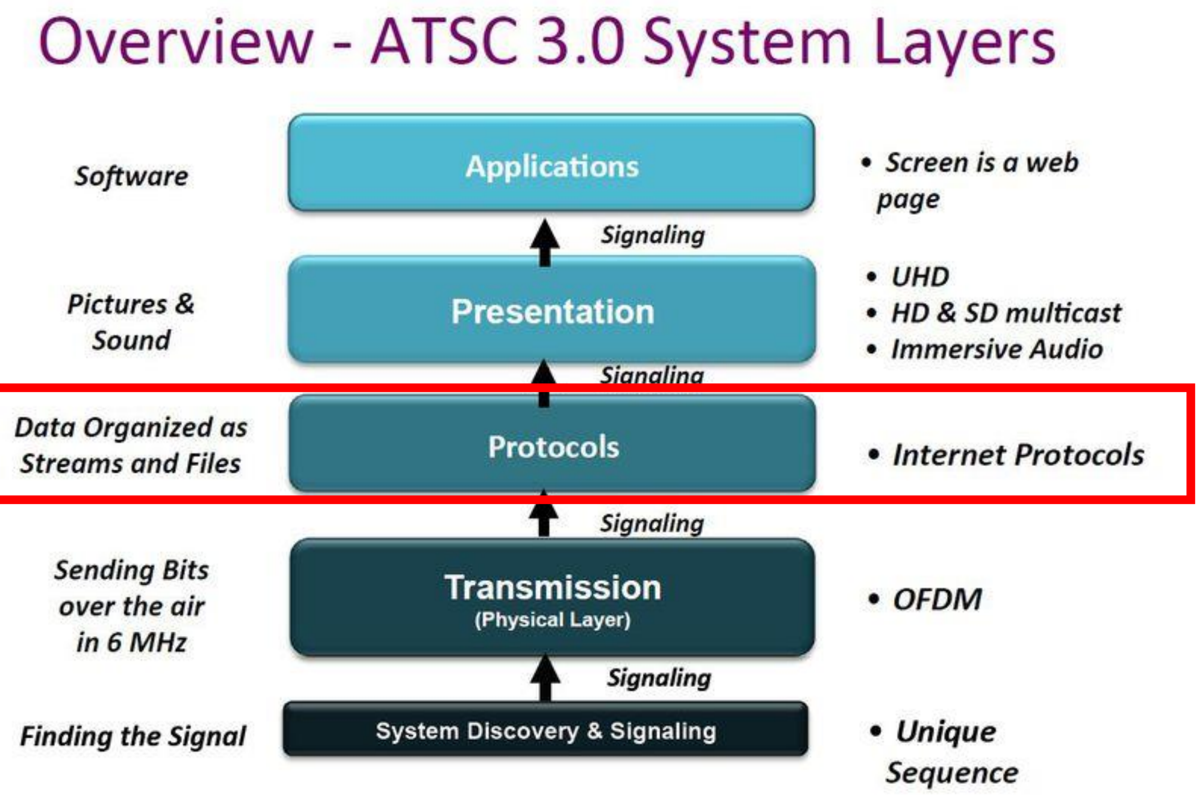
MIDWEST BROADCAST & MULTIMEDIA TECHNOLOGY CONFERENCE

Network Models & ATSC 3.0 Layer Architecture

ROAD TO ATSC 3.0

OSI Model	DoD Model	TCP/IP Model
Application	Application	Application
Presentation		
Session		
Transport	Host to Host	Transport
Network	Internet	Internet
Data Link	Network	Network Interface
Physical		

TCP/IP Focused



Overview - ATSC 3.0 System Layers

Software — Applications — *• Screen is a web page*

Signaling

Pictures & Sound — Presentation — *• UHD • HD & SD multicast • Immersive Audio*

Signaling

Data Organized as Streams and Files — Protocols — *• Internet Protocols*

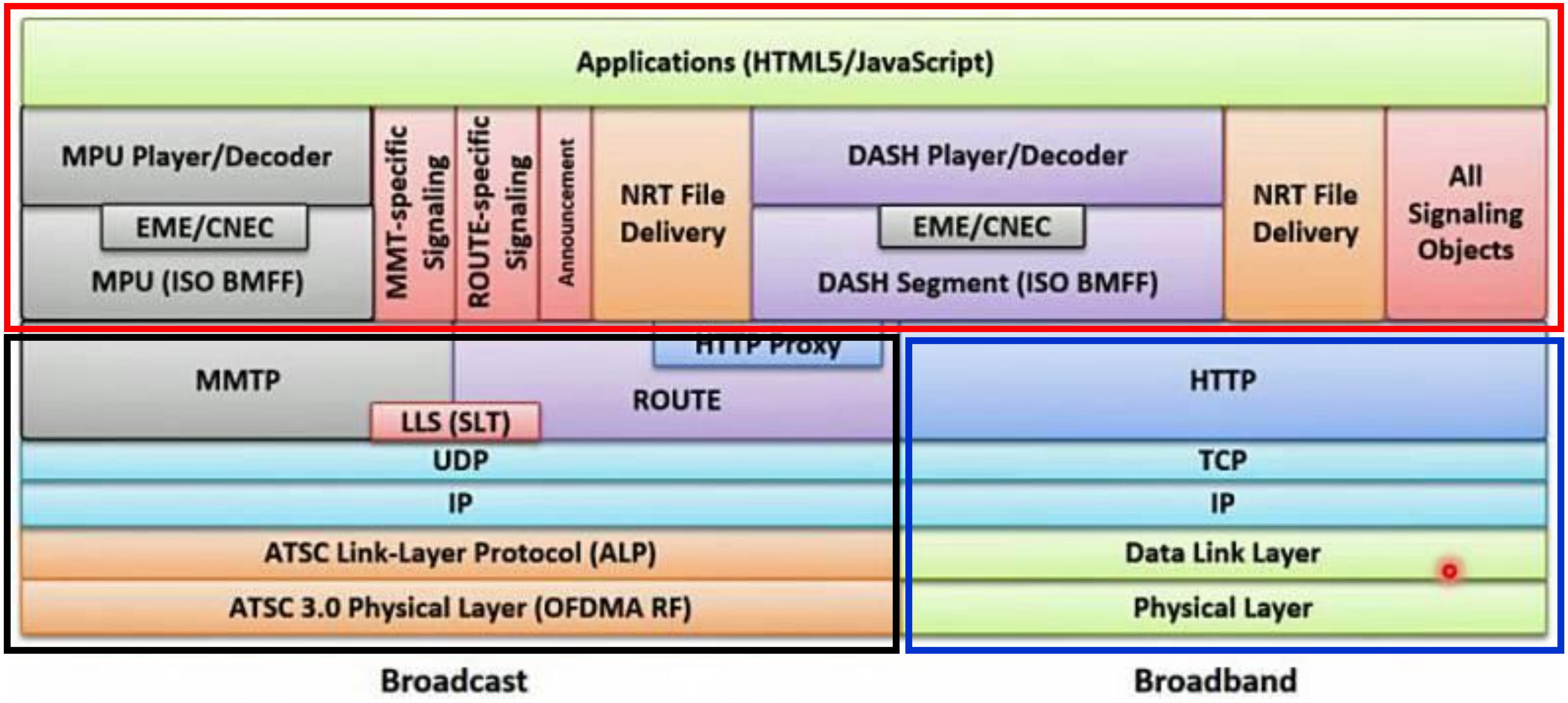
Signaling

Sending Bits over the air in 6 MHz — Transmission (Physical Layer) — *• OFDM*

Signaling

Finding the Signal — System Discovery & Signaling — *• Unique Sequence*

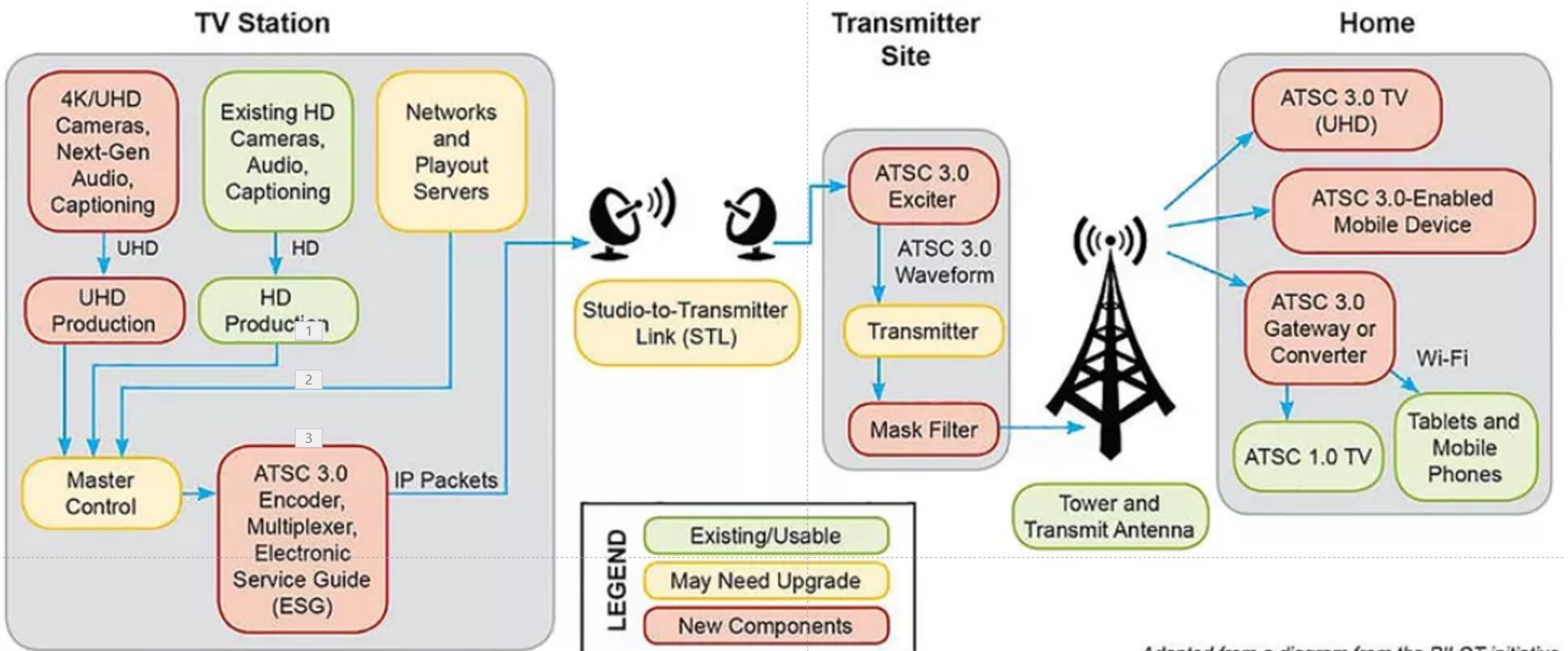
The ATSC 3.0 “stack” in detail



The ATSC 3.0 End-to-End Ecosystem

ROAD TO ATSC 3.0

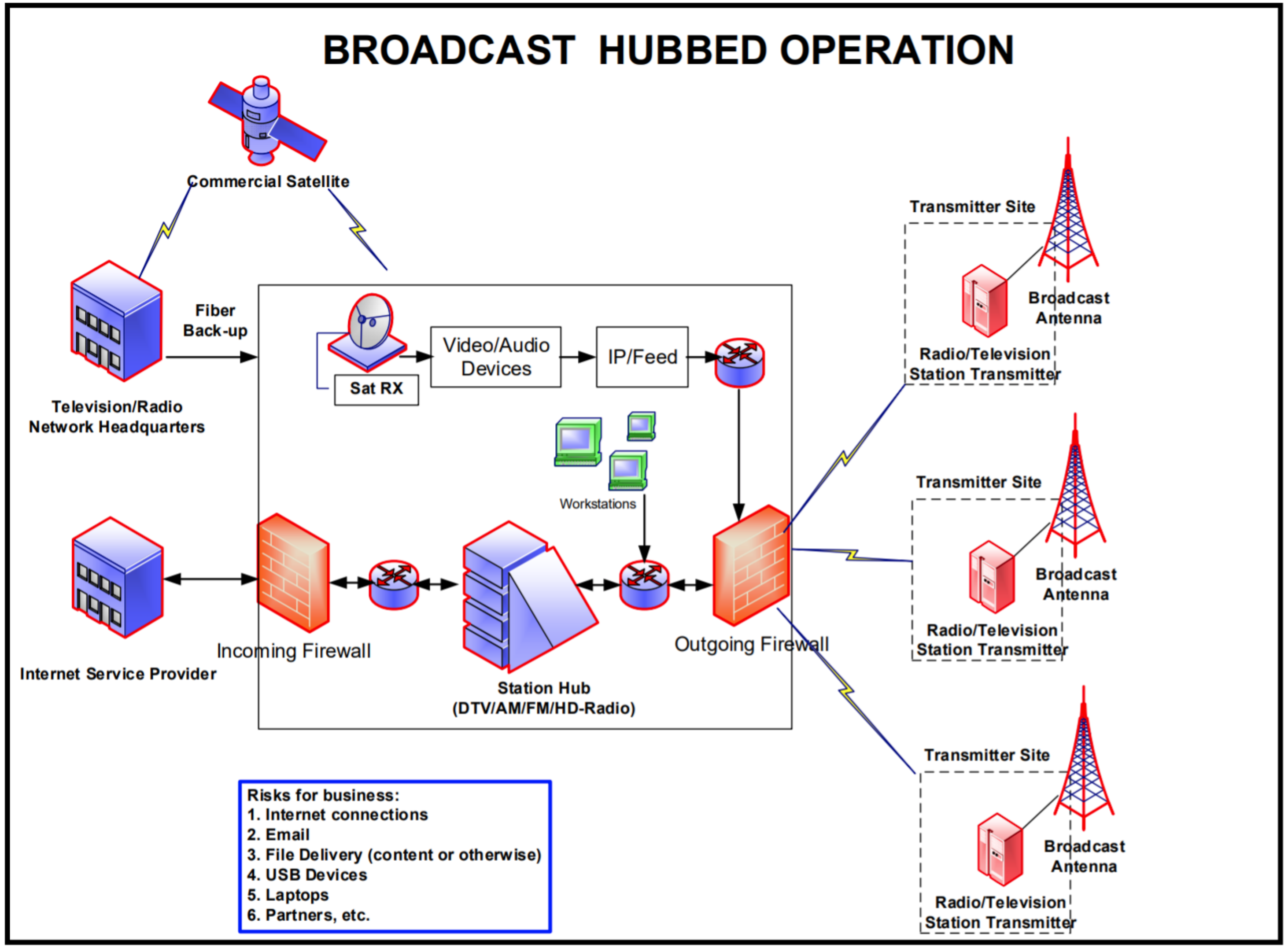
- Broadcast Station
- Transmission
- Home Environment



TV Station
4K/UHD Cameras, Next-Gen Audio, Captioning
UHD
UHD Production
Existing HD Cameras, Audio, Captioning
HD
HD Production
Networks and Playout Servers
Master Control
ATSC 3.0 Encoder, Multiplexer, Electronic Service Guide (ESG)
IP Packets
Studio-to-Transmitter Link (STL)
Transmitter Site
ATSC 3.0 Exciter
ATSC 3.0 Waveform
Transmitter
Mask Filter
Tower and Transmit Antenna
Home
ATSC 3.0 TV (UHD)
ATSC 3.0-Enabled Mobile Device
ATSC 3.0 Gateway or Converter
Wi-Fi
ATSC 1.0 TV
Tablets and Mobile Phones
LEGEND
Existing/Usable
May Need Upgrade
New Components

Adapted from a diagram from the PILOT initiative

Securing The Broadcast System


BROADCAST HUBBED OPERATION
Commercial Satellite
Television/Radio Network Headquarters
Fiber Back-up
Sat RX
Video/Audio Devices
IP/Feed
Workstations
Internet Service Provider
Incoming Firewall
Station Hub (DTV/AM/FM/HD-Radio)
Outgoing Firewall
Transmitter Site
Broadcast Antenna
Radio/Television Station Transmitter
Transmitter Site
Broadcast Antenna
Radio/Television Station Transmitter
Transmitter Site
Broadcast Antenna
Radio/Television Station Transmitter

Risks for business:

1. Internet connections
2. Email
3. File Delivery (content or otherwise)
4. USB Devices
5. Laptops
6. Partners, etc.

Securing The Transmission System

- ATSC 3.0 Inherent Mitigations - ATSC A/360:2018
  - TLS
    - Transport Layer Security v1.2 / 1.3
    - IETF RFC 8446
  - DNSSEC
    - Domain Name Service Security Extensions
    - IETF RFC 6840
  - Cryptographically Signing
    - IETF RFC 5751
  - DRM Encryption

ATSC Standard:
ATSC 3.0 Security and Service Protection

A/360 Security and Service Protection
*Recommended Practice
© Copyright 2018 - Advanced Television Systems Committee Inc.

Securing the Home System

- ATSC 3.0 Presents a Diverse Environment:
  - SmartTV
  - OTT STB
  - Dongle
  - The “Home Gateway”
- Gateway Device
  - ATSC 3 Tuner
  - Broadband “Internet” Router
  - WiFi AP

The Home Network

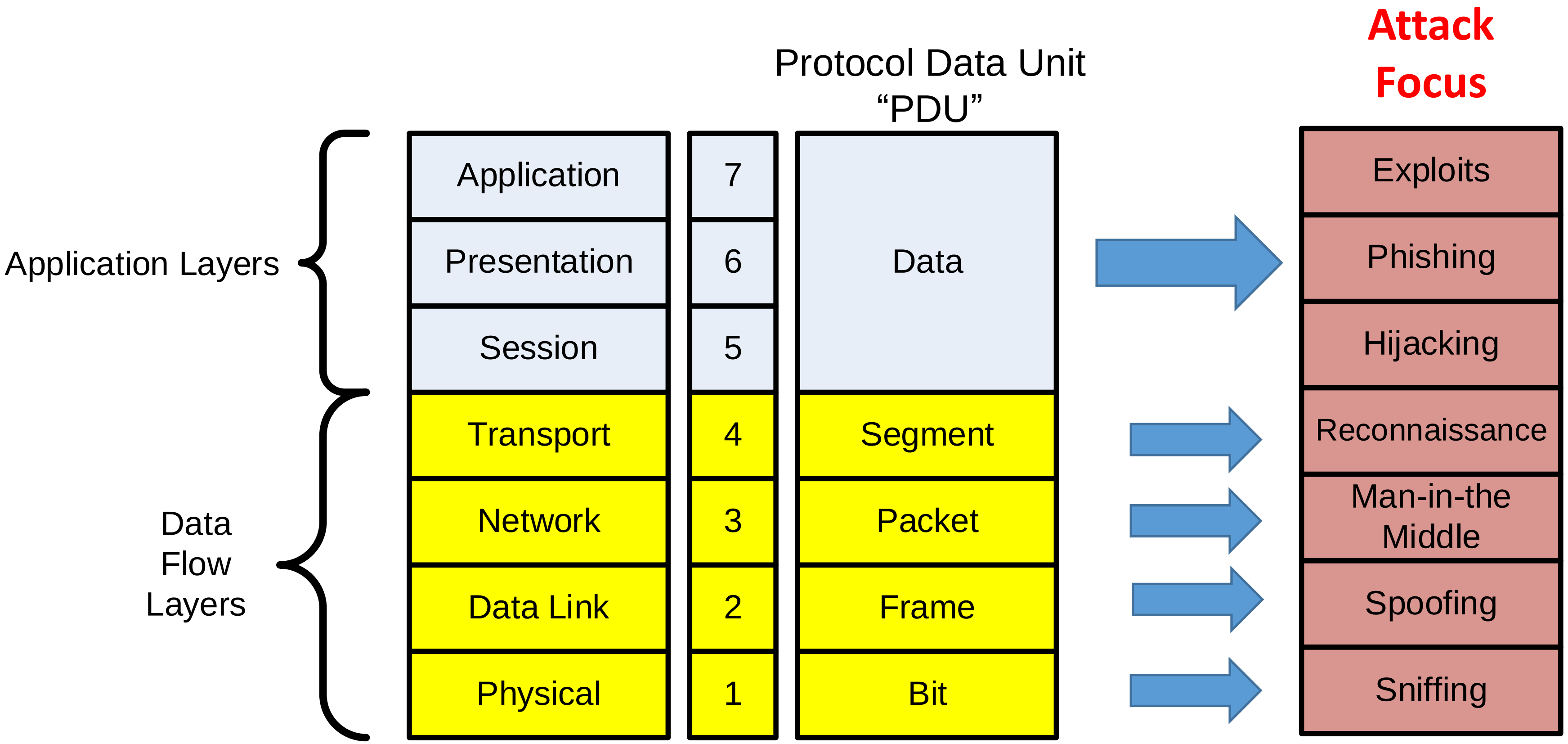
Owner Responsibility

- Only Connect Devices That Need Internet
- Change Default Device Passwords - Use Strong Passwords – Unique for Each Device
- Segment Network – Separate Networks (Media net / General Use net / Control net
- Keep Device Firmware Updated
- Disable uPnP (universal Plug & Play)
- Understand Cloud Service Based Apps
- Monitor Network Activity – Know What is Connected – Be Cautious of Open Ports

Not Likely to Happen

Mitigation & Prevention Tasks

OSI Model Layers & Attack Focus



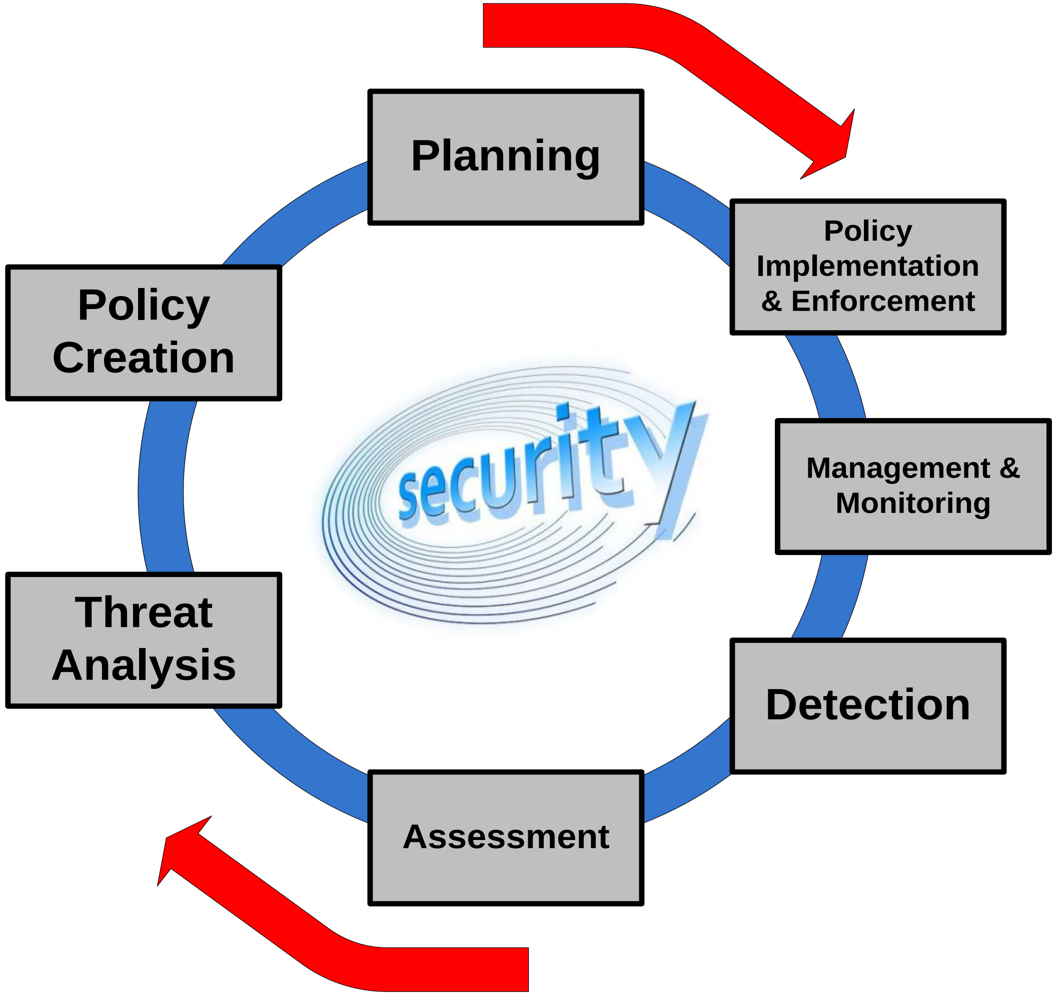
			Protocol Data Unit “PDU”	Attack Focus
Application Layers	Application	7	Data	Exploits
	Presentation	6		Phishing
	Session	5		Hijacking
Data Flow Layers	Transport	4	Segment	Reconnaissance
	Network	3	Packet	Man-in-the Middle
	Data Link	2	Frame	Spoofing
	Physical	1	Bit	Sniffing

The Open Systems Interconnection (OSI) model is an abstract, conceptual model created by the International Organization for Standardization which enables diverse communication systems to communicate using standardized protocols. The OSI provides a standard for host – host communications over diverse network types.

Cybersecurity Mitigation - Where Do You Begin?

Securing the Broadcast IT System

- Securing the Network
  - Architecture
  - Harding devices
  - Protecting transmission paths:
    - Wired
    - Wireless
- Securing the Hosts
  - Operating System
  - Storage
  - Applications
- Recovery & Incident Response
  - Business continuity plan
  - Recovery:
    - Redundancy
    - Data backups

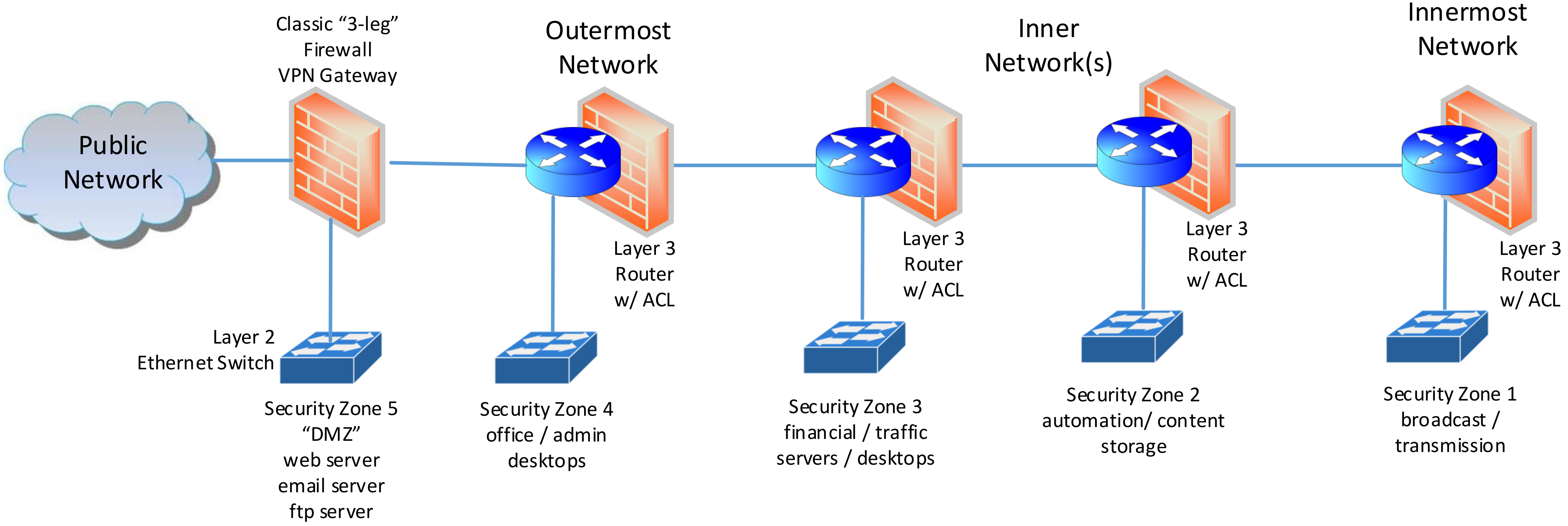


Securing the Network

- Security Begins With Network Architecture
- Segment Networks to Minimize Attack Surface
- Apply Best Practices - Structured & Coordinated
- Follow the OSI Model for the Structure

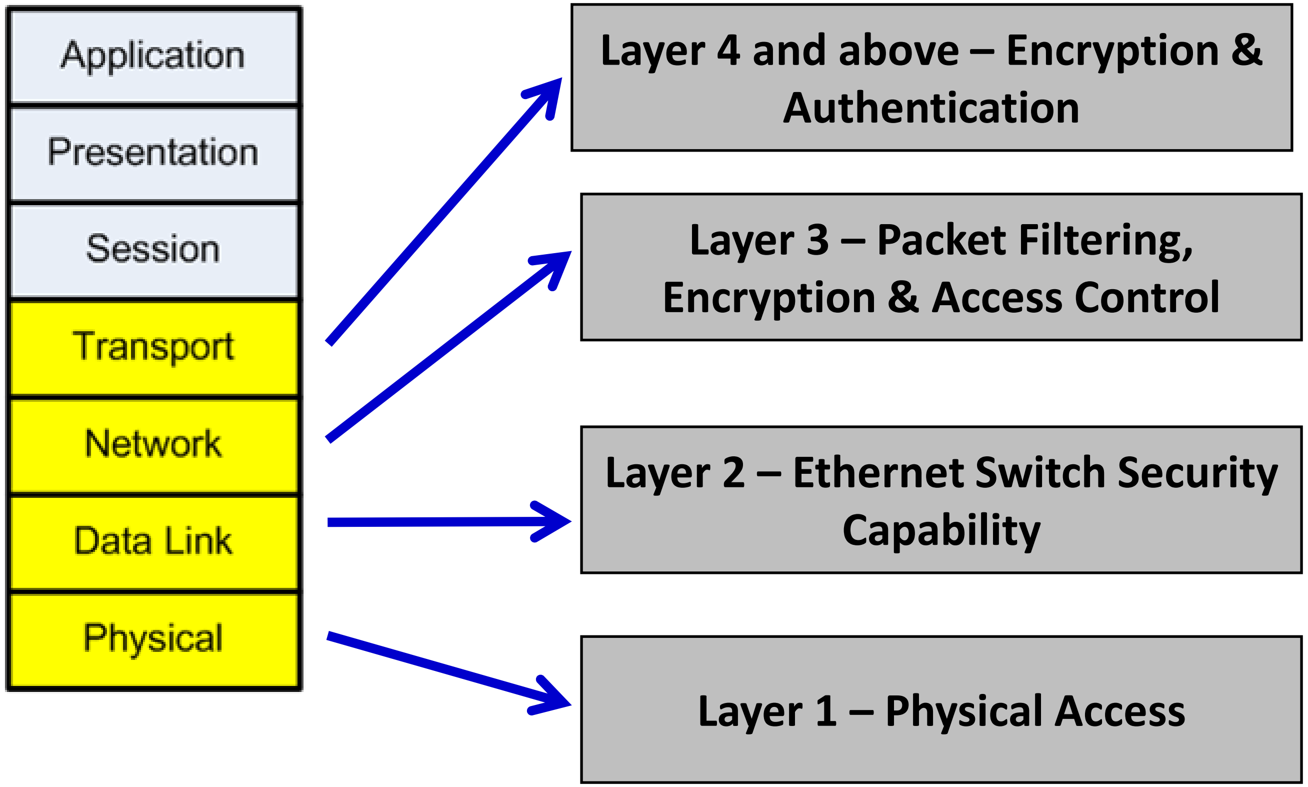
Why segment?

- Performance enhancement
- Improved Security:
  - Attack plane minimized
  - Containment
  - Endpoint protection
  - Resource access minimized
  - Minimized "east-west" (lateral) movement


Public Network
Classic "3-leg" Firewall VPN Gateway
Layer 2 Ethernet Switch
Security Zone 5 "DMZ" web server email server ftp server
Outermost Network
Layer 3 Router w/ ACL
Security Zone 4 office / admin desktops
Layer 3 Router w/ ACL
Security Zone 3 financial / traffic servers / desktops
Inner Network(s)
Layer 3 Router w/ ACL
Security Zone 2 automation/ content storage
Innermost Network
Layer 3 Router w/ ACL
Security Zone 1 broadcast / transmission

OSI Model for Structure & Coordination

“Defense in Depth principal: Approach based upon **coordinated** “multiple layered” security protections



Layer 4 and above – Encryption & Authentication

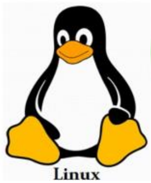
Layer 3 – Packet Filtering, Encryption & Access Control

Layer 2 – Ethernet Switch Security Capability

Layer 1 – Physical Access

Securing the Host Devices

- Hardening is a process to reduce the attack surface of a host device operating system
- Implementation activities typically include:
  - Changing default passwords
  - Removing un-used applications / services (de-bloating)
  - Deleting un-used accounts
  - Adjusting / changing default configurations
  - Strong password management
  - Keeping updates & patches up-to-date
  - Closing network "back doors"



Windows Op System

- Separate user and admin account(s
- Obfuscate local admin account (rename)
- Disable "guest" account(s)
- Insure "drivers" are patched up-to-date
- Disable "un-needed" services
- Utilize "domain controller" to administer multiple hosts with "caution"

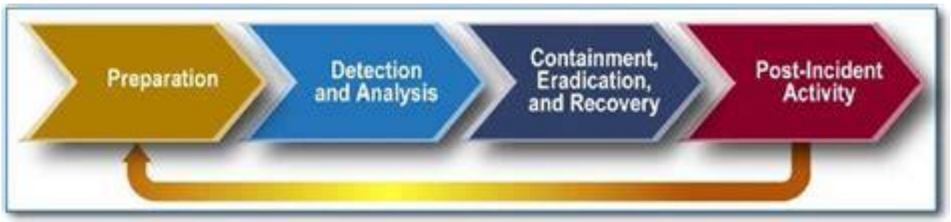
Linux Op System

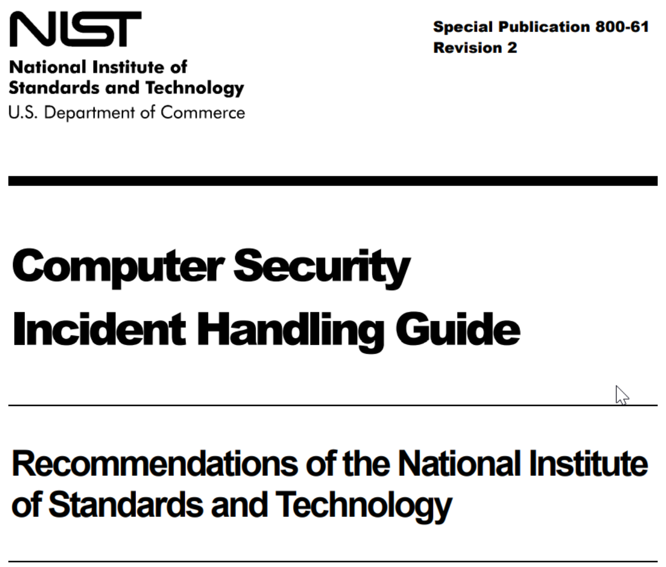
- Password protect the host BIOS
- Enable disk encryption
- Lock boot directory (read-only)
- Maintain system (kernel) updates & patches
- Disable / remove any un-used services (ie telnet, tftp, etc)
- Check for open ports (pen test)
- Secure SSH (change port, disable root login)
- Disable network parameters:
  - IP Forwarding
  - ICMP Re-Directs
  - Send Packet Re-Directs
- Set a "strong" password hashing algorithm (SHA512)
- Lock accounts after x failed login attempts (3-5)

Recovery & Incident Response

“Pre-determined course of action for a cybersecurity event”

- Have a recovery plan in place (proactive)
- Instructions to detect, respond & recover
  - Can be beneficial to recovering from a catastrophic event
- Incident Response Plan (NIST):
  - Preparation
  - Detection & analysis
  - Containment, eradication and recovery
  - Post-event activity
- Maintain data backups





NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

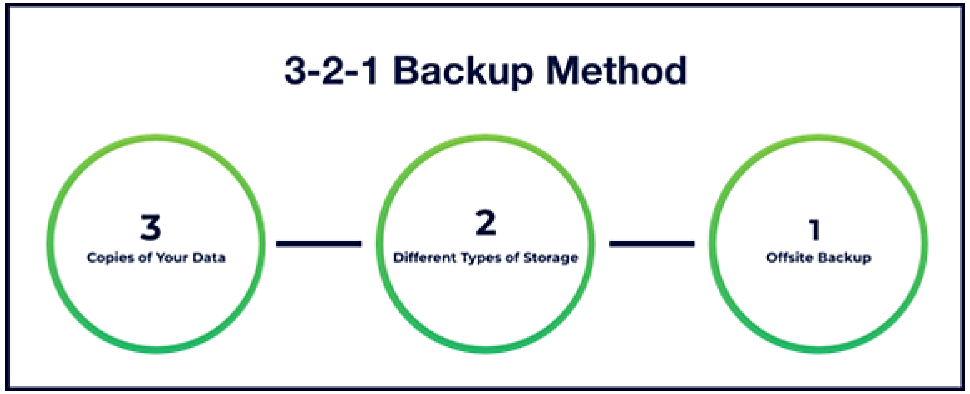
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Data Backup & Practices

- Often is the last resort course of action!

- Backup “best practices”:
  - Maintain offline – isolate backups
    - Mount target drive when required
    - Set backup drive as “RO”
  - Use “immutable” storage “WORM”
  - Mount drives only when necessary
  - Consider “intelligent” backup solutions
  - Match backup frequency to your business
  - Keep multiple backups – multiple locations - “3-2-1” rule

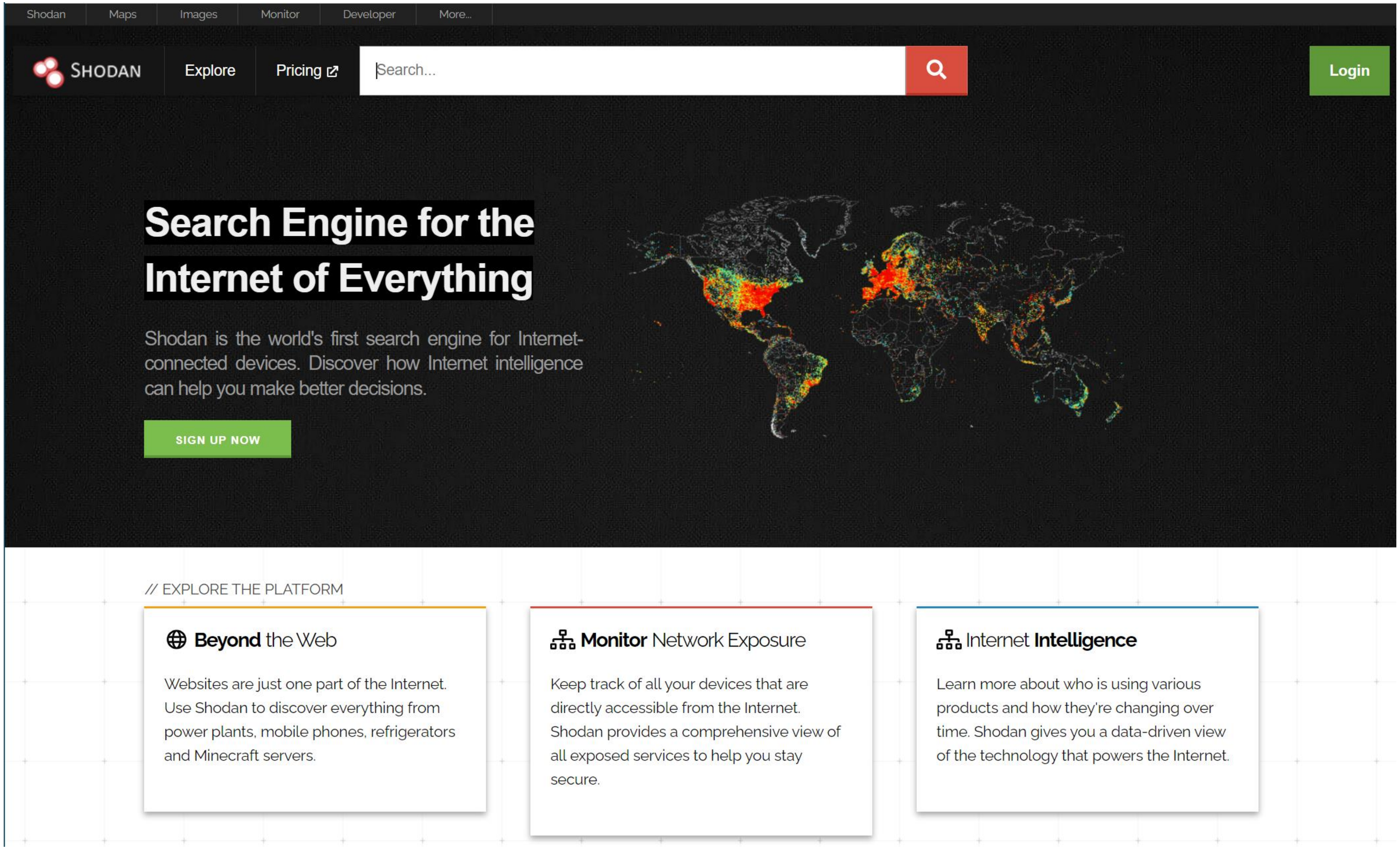
- Restoration practices
  - Know the restoration time required
  - Know the restoration priority – dependencies
  - TEST, TEST, TEST restoration



Takeaway Thoughts & Resources

SHODAN

https://www.shodan.io



Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

// EXPLORE THE PLATFORM

Beyond the Web

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Monitor Network Exposure

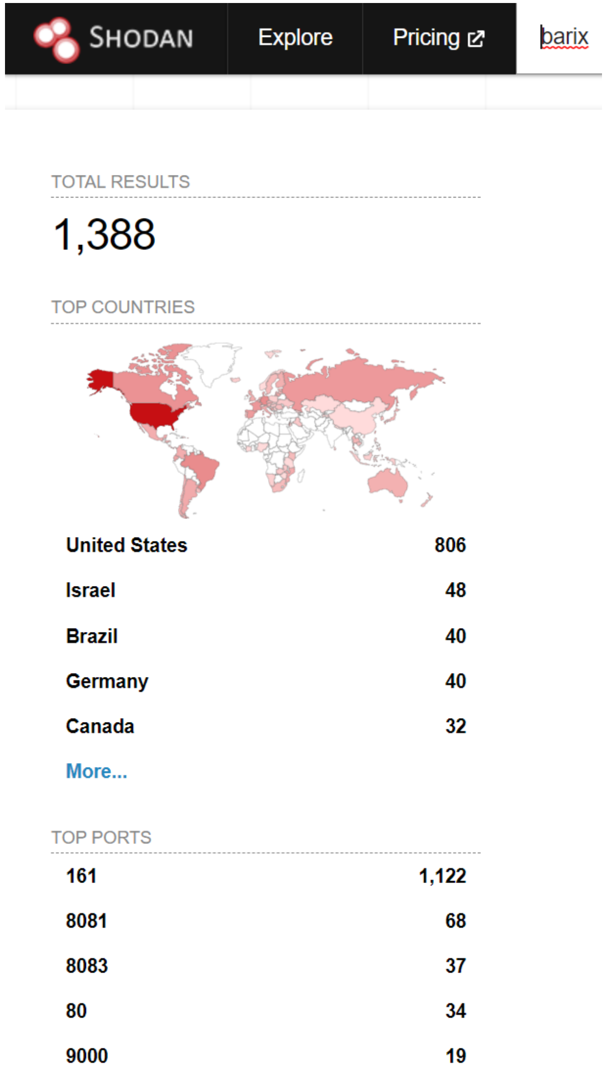
Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

Internet Intelligence

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

SHODAN

https://www.shodan.io



barix

TOTAL RESULTS

1,388

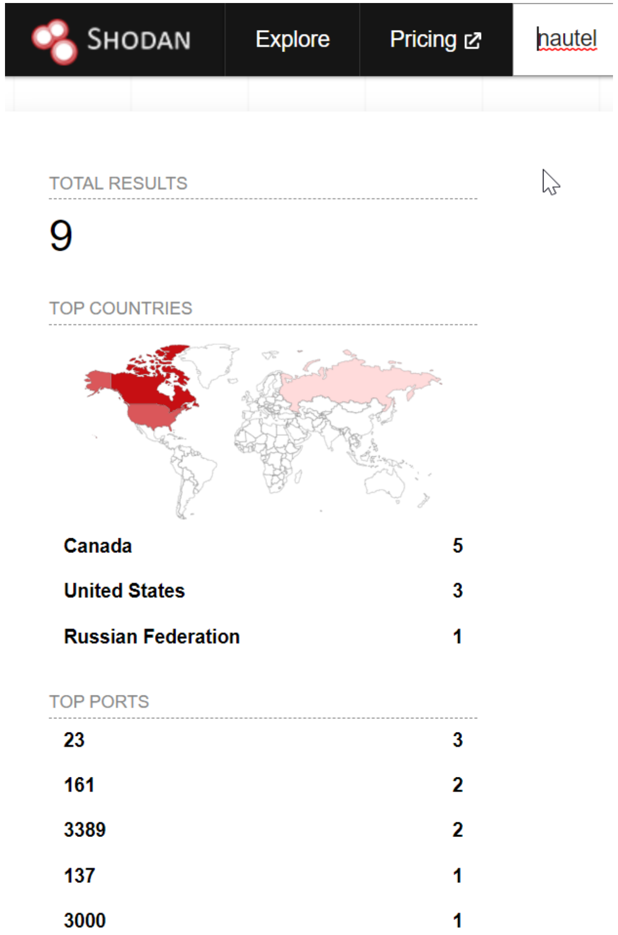
TOP COUNTRIES

United States	806
Israel	48
Brazil	40
Germany	40
Canada	32

More...

TOP PORTS

161	1,122
8081	68
8083	37
80	34
9000	19



nautel

TOTAL RESULTS

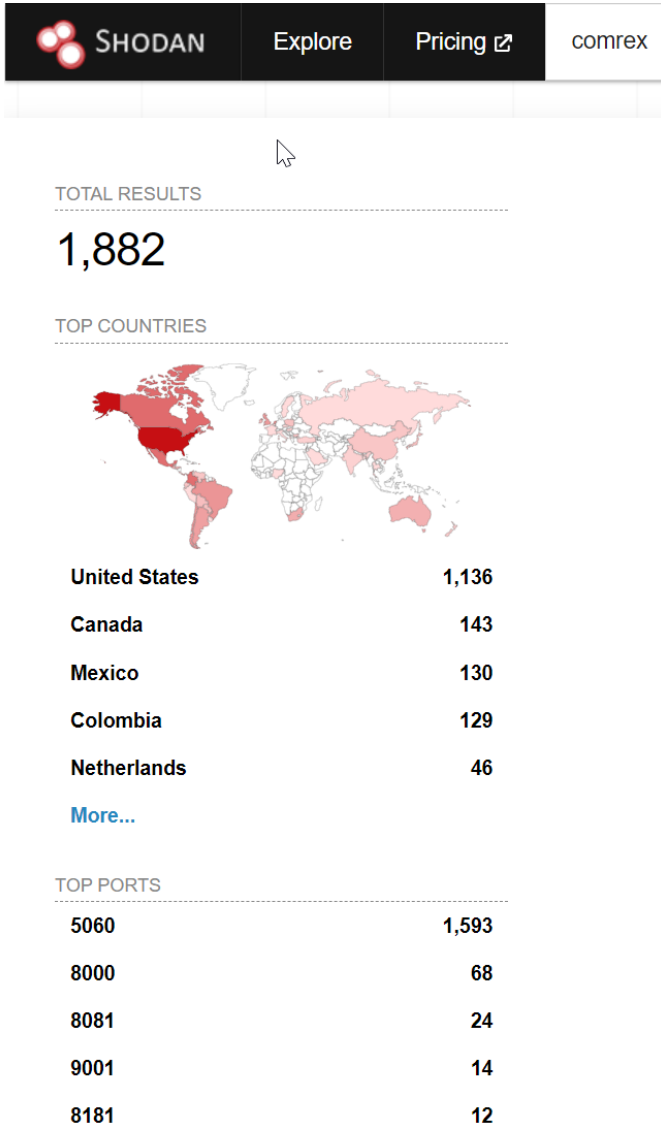
9

TOP COUNTRIES

Canada	5
United States	3
Russian Federation	1

TOP PORTS

23	3
161	2
3389	2
137	1
3000	1



comrex

TOTAL RESULTS

1,882

TOP COUNTRIES

United States	1,136
Canada	143
Mexico	130
Colombia	129
Netherlands	46

More...

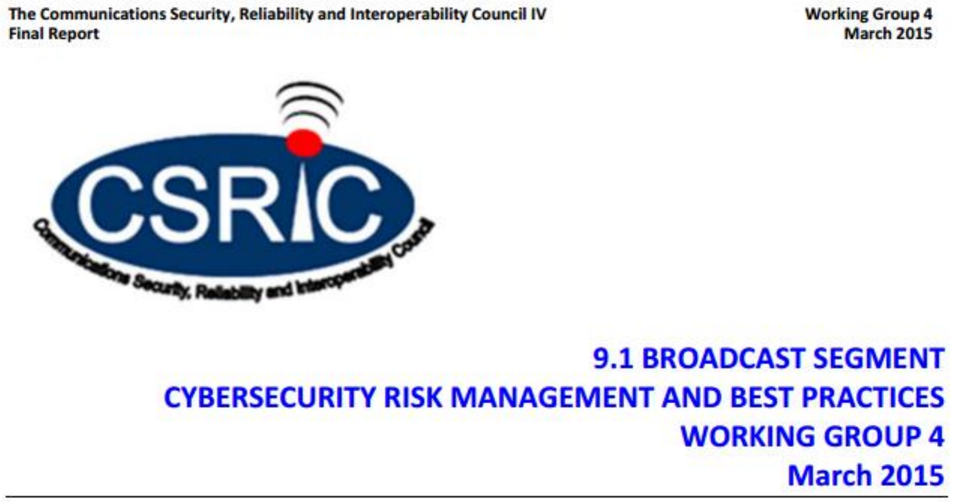
TOP PORTS

5060	1,593
8000	68
8081	24
9001	14
8181	12

10/25/2022 collected data

FCC Working Group 4

CSRIC IV Working Group 4 (WG4) was given the task of developing *voluntary mechanisms* that give the Federal Communications Commission (FCC) and the public assurance that communication providers are taking the necessary measures to manage cybersecurity risks across the enterprise.[1] WG4 also was charged with providing implementation guidance to help communication providers use and adapt the voluntary NIST Cybersecurity Framework[2] (hereinafter "NIST CSF").

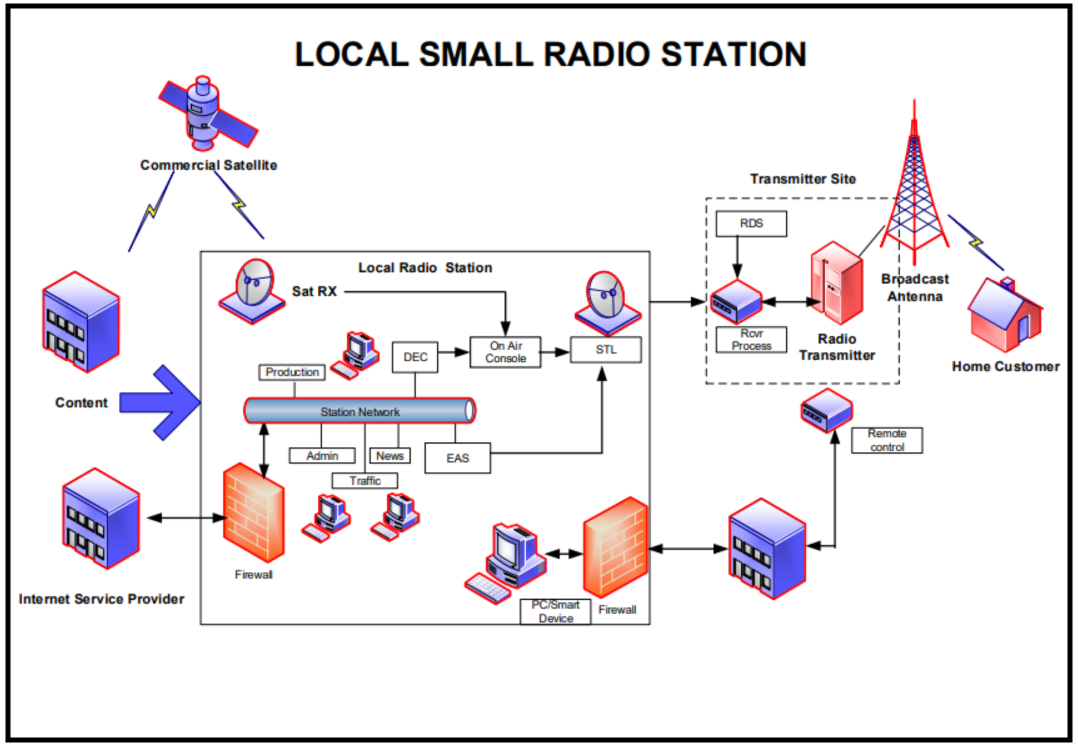


The Communications Security, Reliability and Interoperability Council IV
Final Report

Working Group 4
March 2015

CSRIC
Communications Security, Reliability and Interoperability Council

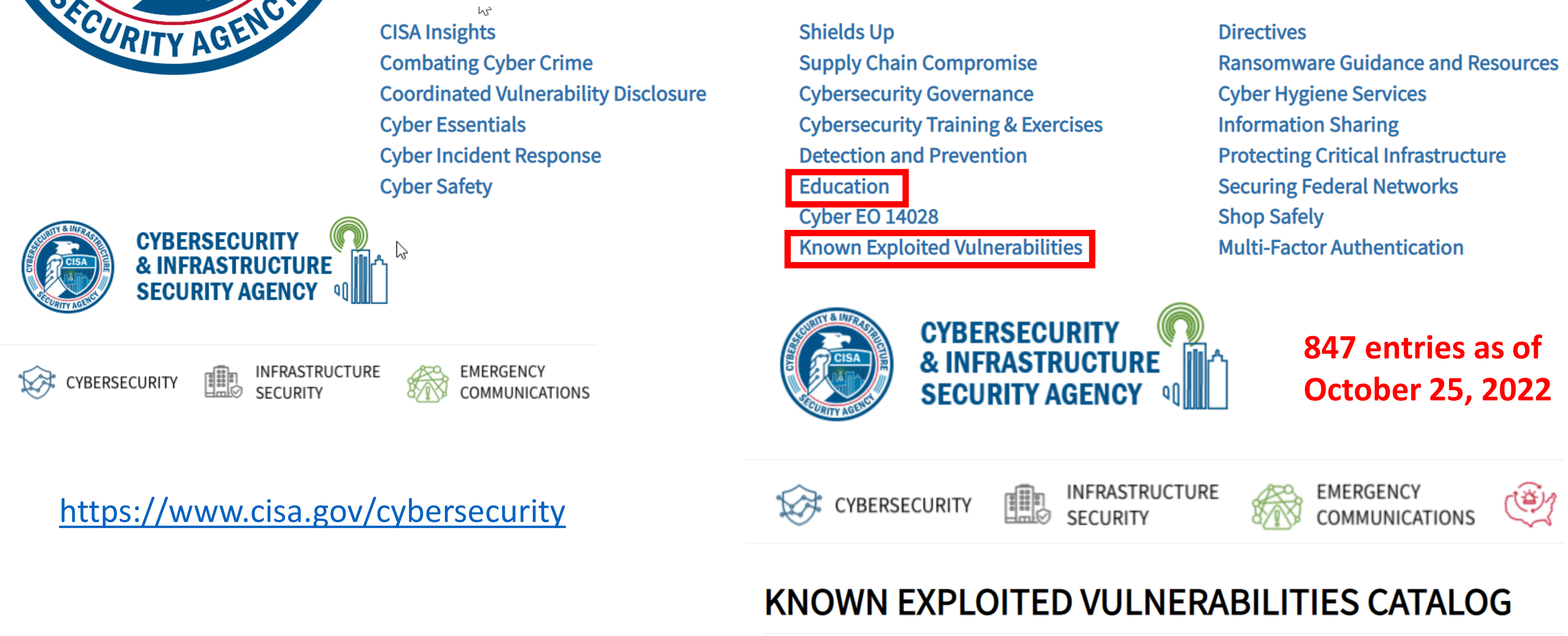
9.1 BROADCAST SEGMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015



LOCAL SMALL RADIO STATION

https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

The Cybersecurity and Infrastructure Security Agency is a United States federal agency, an operational component under Department of Homeland Security oversight. Its activities are a continuation of the National Protection and Programs Directorate.

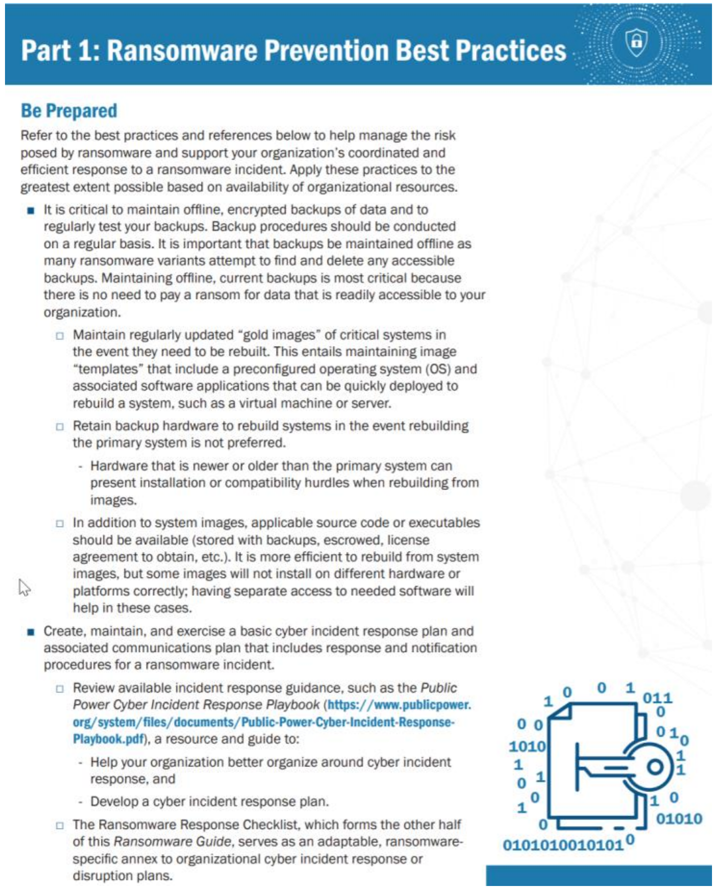


KNOWN EXPLOITED VULNERABILITIES CATALOG

847 entries as of October 25, 2022

https://www.cisa.gov/cybersecurity

MS-ISAC Ransomware Guide

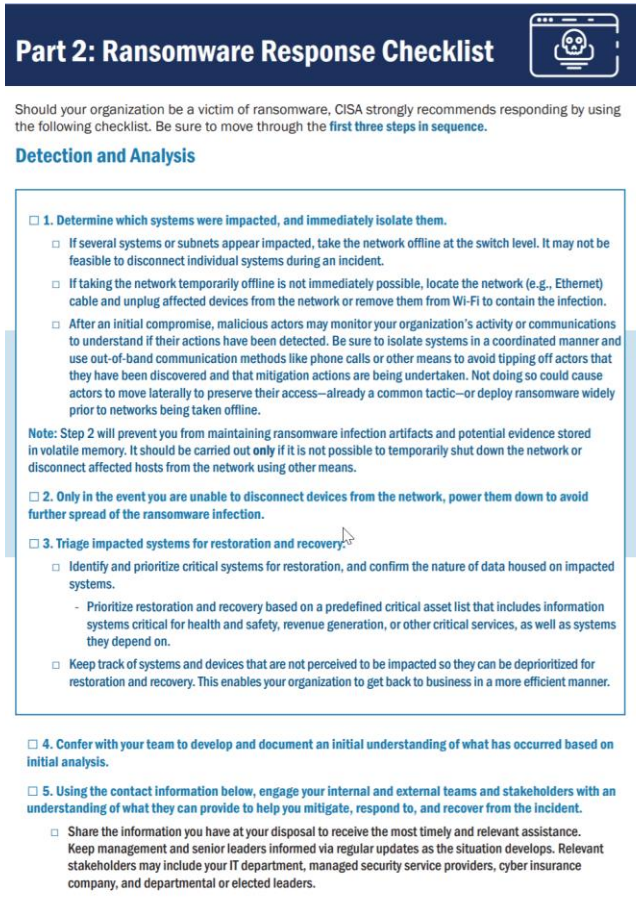


Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - □ Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - □ Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - □ In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - □ Review available incident response guidance, such as the *Public Power Cyber Incident Response Playbook* (**https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf**), a resource and guide to:
    - Help your organization better organize around cyber incident response, and
    - Develop a cyber incident response plan.
  - □ The Ransomware Response Checklist, which forms the other half of this *Ransomware Guide*, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.



Part 2: Ransomware Response Checklist

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

Detection and Analysis

□ 1. Determine which systems were impacted, and immediately isolate them.

- □ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
- □ If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- □ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out **only** if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

□ 2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

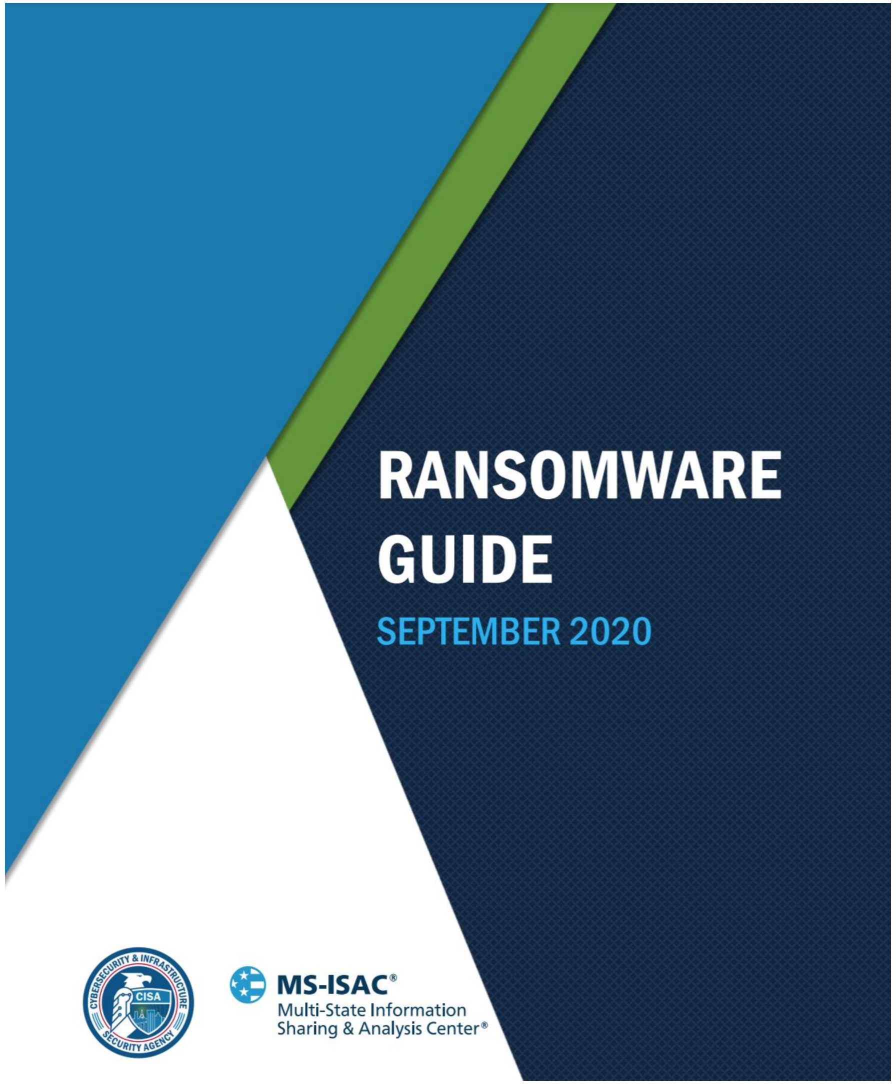
□ 3. Triage impacted systems for restoration and recovery.

- □ Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems.
  - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- □ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

□ 4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.

□ 5. Using the contact information below, engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.

- □ Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.

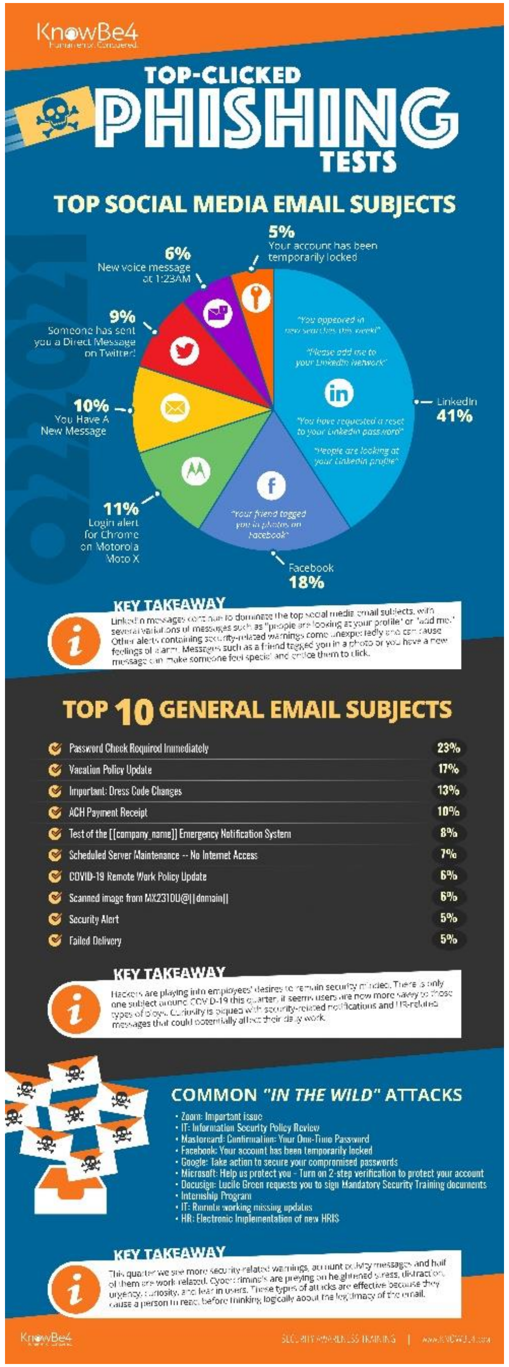


RANSOMWARE GUIDE

SEPTEMBER 2020

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf



KnowBe4
Human error. Conquered.

TOP-CLICKED PHISHING TESTS

TOP SOCIAL MEDIA EMAIL SUBJECTS

Q2 2021
5% Your account has been temporarily locked
6% New voice message at 1:23AM
9% Someone has sent you a Direct Message on Twitter!
10% You Have A New Message
11% Login alert for Chrome on Motorola Moto X
Facebook 18%
LinkedIn 41%
"You appeared in new searches this week!"
"Please add me to your LinkedIn Network"
"You have requested a reset to your LinkedIn password"
"People are looking at your LinkedIn profile"
"Your friend tagged you in photos on Facebook"

KEY TAKEAWAY

LinkedIn messages continue to dominate the top social media email subjects, with several variations of messages such as "people are looking at your profile" or "add me." Other alerts containing security-related warnings come unexpectedly and can cause feelings of alarm. Messages such as a friend tagged you in a photo or you have a new message can make someone feel special and entice them to click.

TOP 10 GENERAL EMAIL SUBJECTS

✓ Password Check Required Immediately	23%
✓ Vacation Policy Update	17%
✓ Important: Dress Code Changes	13%
✓ ACH Payment Receipt	10%
✓ Test of the [[company_name]] Emergency Notification System	8%
✓ Scheduled Server Maintenance -- No Internet Access	7%
✓ COVID-19 Remote Work Policy Update	6%
✓ Scanned image from MX2310U@[[domain]]	6%
✓ Security Alert	5%
✓ Failed Delivery	5%

KEY TAKEAWAY

Hackers are playing into employees' desires to remain security minded. There is only one subject around COVID-19 this quarter, it seems users are now more savvy to those types of ploys. Curiosity is piqued with security-related notifications and HR-related messages that could potentially affect their daily work.

COMMON *"IN THE WILD"* ATTACKS

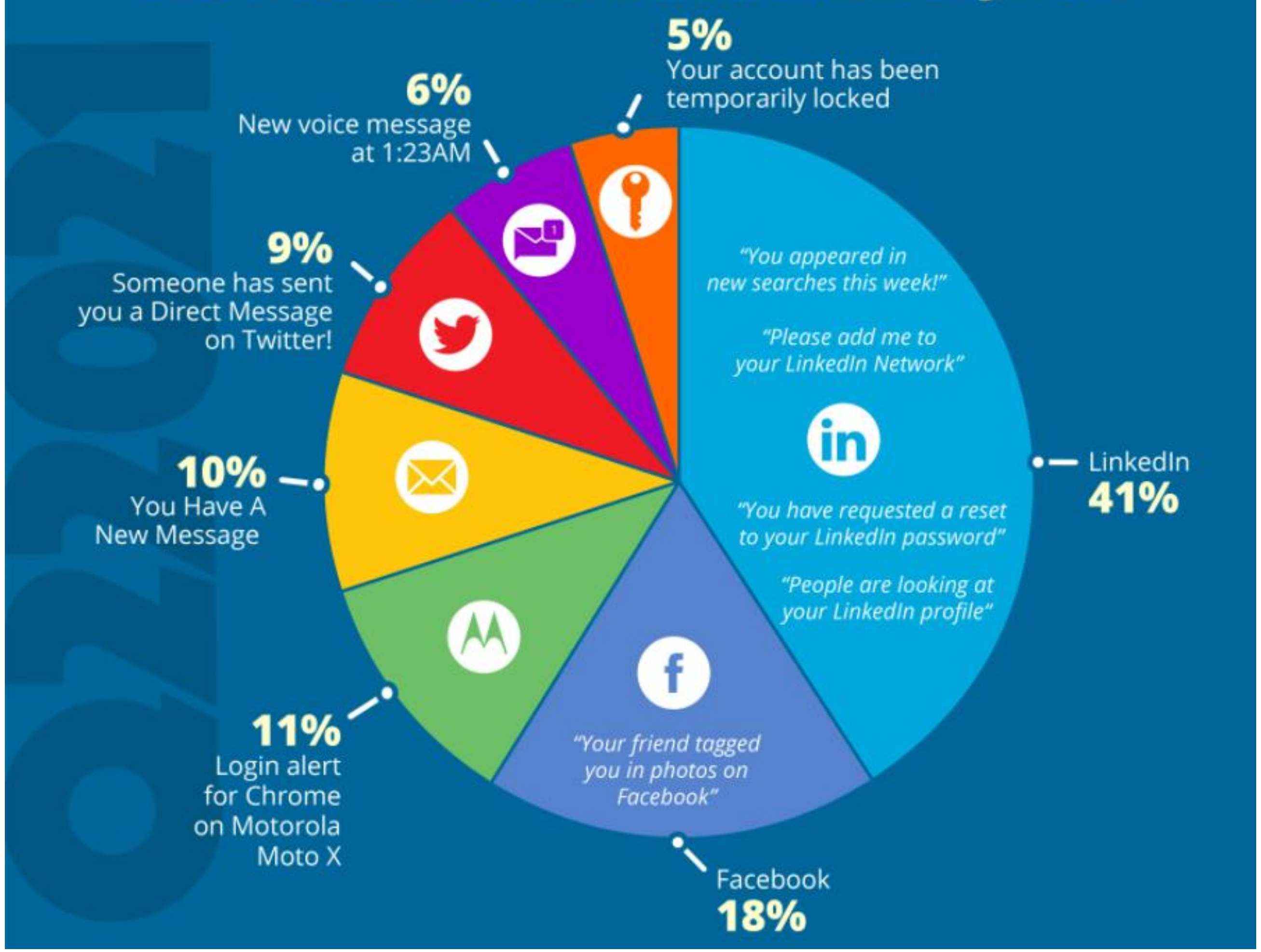
- Zoom: Important issue
- IT: Information Security Policy Review
- Mastercard: Confirmation: Your One-Time Password
- Facebook: Your account has been temporarily locked
- Google: Take action to secure your compromised passwords
- Microsoft: Help us protect you - Turn on 2-step verification to protect your account
- Docusign: Lucile Green requests you to sign Mandatory Security Training documents
- Internship Program
- IT: Remote working missing updates
- HR: Electronic Implementation of new HRIS

KEY TAKEAWAY

This quarter we see more security-related warnings, account activity messages and half of them are work related. Cybercriminals are preying on heightened stress, distraction, urgency, curiosity, and fear in users. These types of attacks are effective because they cause a person to react before thinking logically about the legitimacy of the email.

KnowBe4 SECURITY AWARENESS TRAINING | www.KnowBe4.com

TOP SOCIAL MEDIA EMAIL SUBJECTS

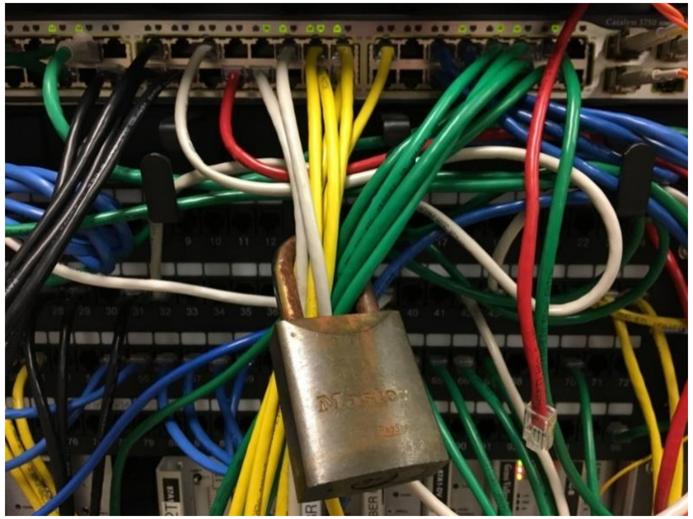


https://blog.knowbe4.com/infographic-q2-2021-users-falling-for-security-hr-phishing-attacks

Do These 13 Things

(if nothing else)

- Accept - Their is **NO SINGLE** Solution! - Implement multiple protections **“DiD”**
- **Segment** your network (VLAN) – reduce attack surface & east-west movement - enhance performance
- Utilize Ethernet switch **port security** features
- Change **default** login credentials - Use **unique** & **strong** passwords (paraphrases)
- **Separate** Admin & User accounts on hosts (WIN)
- **Limit** access (users & applications) – apply principal of “**least privilege**”
- Control access - use packet **filtering** - (ACL and/or firewall) – **deny by default** – SSH & MFA
- **Disable / minimize** services not required – close/block ports – **minimize** macros / RDP use
- **Monitor** you IT infrastructure / network – know what is normal
- Use “**intelligent**” host backup solutions – **test** backup restoration – follow “**3-2-1**” rule
- Keep systems **updated** / **patched –** use **KEV** to guide priorities
- Utilize **signature based** deep-packet inspection antivirus/malware – keep updated (often daily)
- Don’t overlook **social engineering** – engage & educate users – **phishing** is alive and effective



A single “phishing” attempt can instantly negate your efforts!

The Cybersecurity Challenge

Ultimate Network Security

Air
Gap
GATESAIR

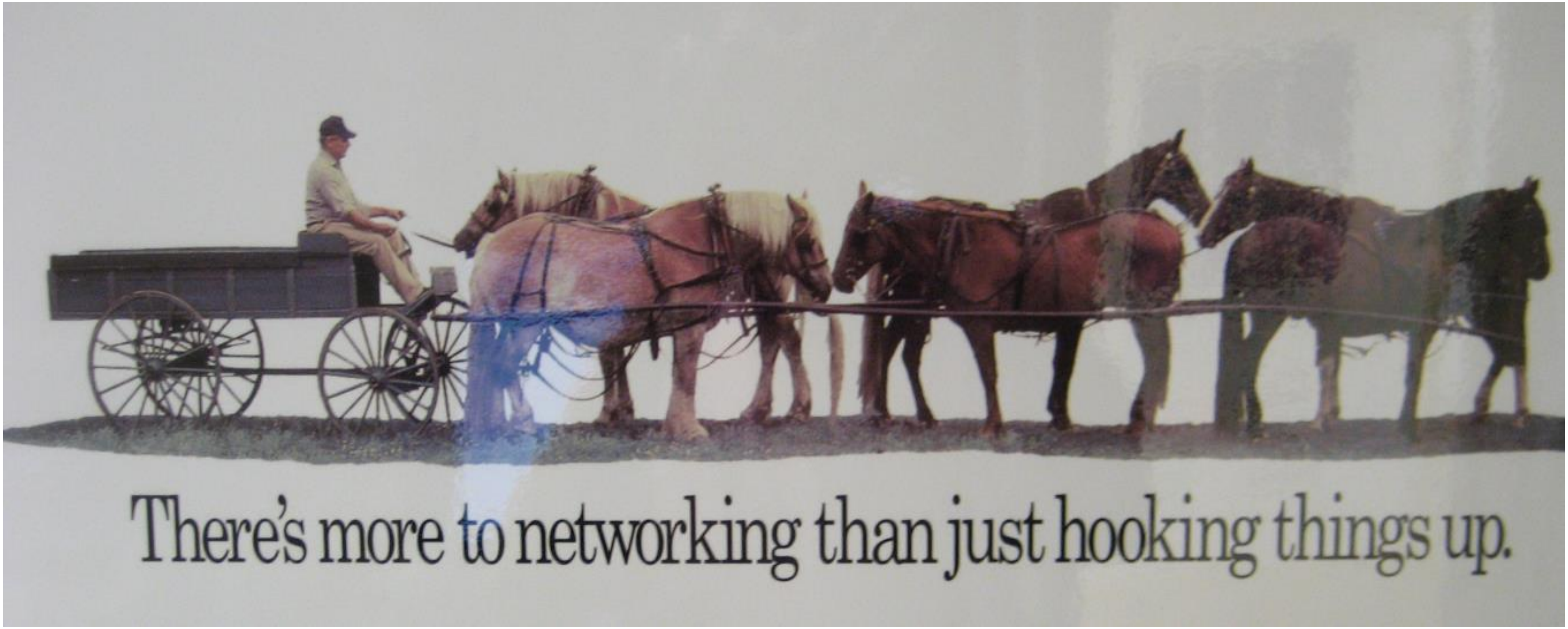
Question if a “critical” host device needs public network access!

Recognize remote access is not the same as public network access!

Closing Thoughts ....

- Cybersecurity is an ongoing process – use routine cyber hygiene
- Have the proper segmented network design
- Follow OSI model to implement structured / coordinated approach:
  - Physical security
  - Utilize layer 2 Ethernet switch port security features
  - Utilize layer 3 packet filtering & encryption
- Use authenticated encrypted remote access (2-factor & VPN)
- Use packet filtering - Firewall "housekeeping" is essential
- Use of the Internet Protocol Brings Unique Features to ATSC 3
  - IP Opens Door to Cybersecurity Threats
  - ATSC 3 - Too New to Understand Real Threats
  - Beware of the Home Network!
- Be Careful Out There – The Weakest Link Determines System Security!

A single successful "phishing" attempt can instantly negate your all your cybersecurity efforts!


There’s more to networking than just hooking things up.

Questions ?

Wayne M. Pecena CPBE, AMD, ATSC3, DRB, 8VSB, CBNE
Texas A&M University
w-pecena@tamu.edu
wpecena@sbe.org
979.845.5662

ATM KAMU PBS npr

BTS IEEE Broadcast Technology Society **Distinguished Lecturer**

SBE **Immediate Past President**