American Hospital Association.

# The Cyber Threat Landscape – Threats and Risk Mitigation

NATIONAL COUNCIL
FOR BEHAVIORAL HEALTH

American Hospital Association™

Advancing Health in America

Cybersecurity and Risk Advisory Services

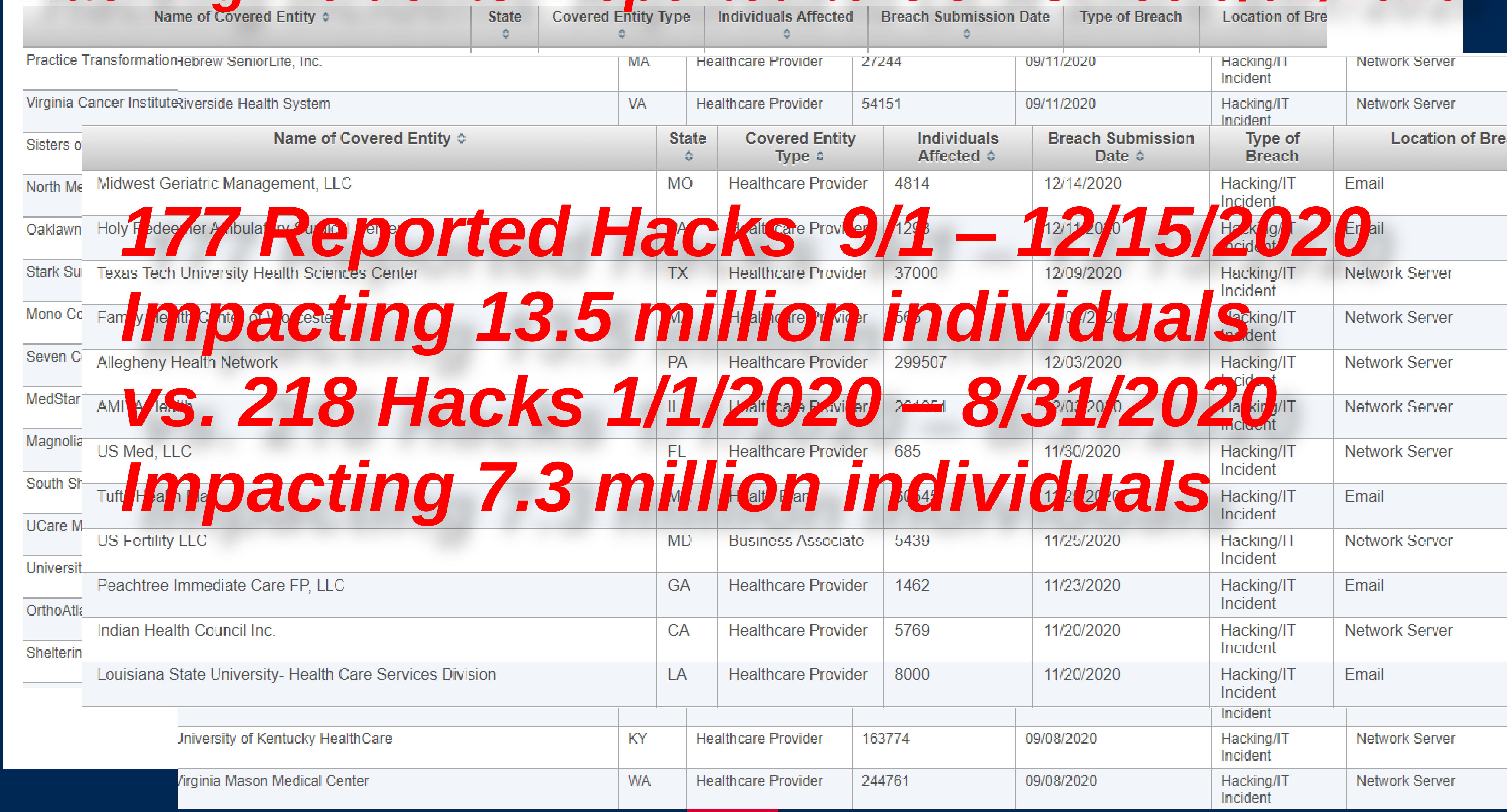
Presented by John Riggi, Senior Advisor for Cybersecurity and Risk Advisory Services, AHA
12/17/2020

American Hospital Association™
Advancing Health in America

AHA CENTER FOR HEALTH INNOVATION

# Hacking Incidents Reported to OCR Since 9/01/2020

**177 Reported Hacks 9/1 – 12/15/2020**
**Impacting 13.5 million individuals**
**vs. 218 Hacks 1/1/2020 – 8/31/2020**
**Impacting 7.3 million individuals**



| Name of Covered Entity ⇕ | State ⇕ | Covered Entity Type ⇕ | Individuals Affected ⇕ | Breach Submission Date ⇕ | Type of Breach | Location of Bre |
|---|---|---|---|---|---|---|
| Hebrew SeniorLife, Inc. | MA | Healthcare Provider | 27244 | 09/11/2020 | Hacking/IT Incident | Network Server |
| Riverside Health System | VA | Healthcare Provider | 54151 | 09/11/2020 | Hacking/IT Incident | Network Server |
| | | | | | Incident | |
| University of Kentucky HealthCare | KY | Healthcare Provider | 163774 | 09/08/2020 | Hacking/IT Incident | Network Server |
| Virginia Mason Medical Center | WA | Healthcare Provider | 244761 | 09/08/2020 | Hacking/IT Incident | Network Server |

Practice Transformation
Virginia Cancer Institute
Sisters o
North Me
Oaklawn
Stark Su
Mono Co
Seven C
MedStar
Magnolia
South Sh
UCare M
Universit
OrthoAtl
Shelterin

| Name of Covered Entity ⇕ | State ⇕ | Covered Entity Type ⇕ | Individuals Affected ⇕ | Breach Submission Date ⇕ | Type of Breach | Location of Bre |
|---|---|---|---|---|---|---|
| Midwest Geriatric Management, LLC | MO | Healthcare Provider | 4814 | 12/14/2020 | Hacking/IT Incident | Email |
| Holy Redeemer Ambulatory Surgical Center | [illegible] | Healthcare Provider | [illegible] | [illegible] | Hacking/IT Incident | Email |
| Texas Tech University Health Sciences Center | TX | Healthcare Provider | 37000 | 12/09/2020 | Hacking/IT Incident | Network Server |
| Family Health Center of Worcester | MA | Healthcare Provider | [illegible] | [illegible] | Hacking/IT Incident | Network Server |
| Allegheny Health Network | PA | Healthcare Provider | 299507 | 12/03/2020 | Hacking/IT Incident | Network Server |
| AMITA Health | IL | Healthcare Provider | [illegible] | [illegible] | Hacking/IT Incident | Network Server |
| US Med, LLC | FL | Healthcare Provider | 685 | 11/30/2020 | Hacking/IT Incident | Network Server |
| Tufts Health Plan | MA | Health Plan | [illegible] | [illegible] | Hacking/IT Incident | Email |
| US Fertility LLC | MD | Business Associate | 5439 | 11/25/2020 | Hacking/IT Incident | Network Server |
| Peachtree Immediate Care FP, LLC | GA | Healthcare Provider | 1462 | 11/23/2020 | Hacking/IT Incident | Email |
| Indian Health Council Inc. | CA | Healthcare Provider | 5769 | 11/20/2020 | Hacking/IT Incident | Network Server |
| Louisiana State University- Health Care Services Division | LA | Healthcare Provider | 8000 | 11/20/2020 | Hacking/IT Incident | Email |

# ***Polling Questions:***

***1) Do you have any direct responsibility for cybersecurity in your organization?***

***Polling Options: Yes, No***

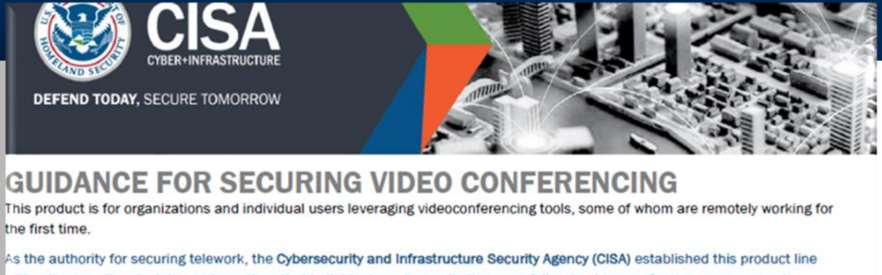
***2) Do you use an outside party to manage your cybersecurity?***

***Polling Options: Yes, No, I Don’t Know***

# COVID-19 Induced Cyber Triple Threat - Cyber Criminals Exploiting a Crisis

## Threat 1: Expanded Attack Surface

- Rapid Expansion and Deployment of network and internet connected technologies
- Connected Medical Devices and Ventilators, remote monitoring to save PPE
- Telehealth and Telemedicine
- Telework
- Cloud Services



CISA
CYBER+INFRASTRUCTURE
DEFEND TODAY, SECURE TOMORROW

GUIDANCE FOR SECURING VIDEO CONFERENCING

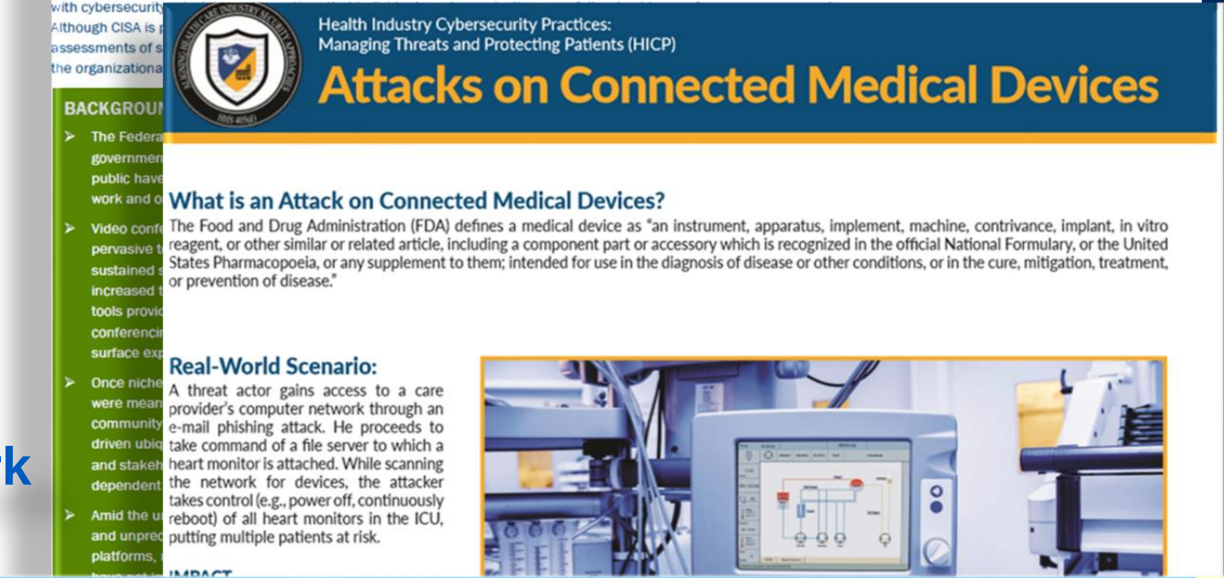
This product is for organizations and individual users leveraging videoconferencing tools, some of whom are remotely working for the first time.

As the authority for securing telework, the Cybersecurity and Infrastructure Security Agency (CISA) established this product line with cybersecurity

Although CISA is p

assessments of s

the organizationa



BACKGROUN

- The Federa governmen public have work and o
- Video confe pervasive t sustained s increased t tools provi conferencin surface exp
- Once niche were mean community driven ubiq and stakeh dependent
- Amid the u and unpred platforms,

Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients (HICP)

Attacks on Connected Medical Devices

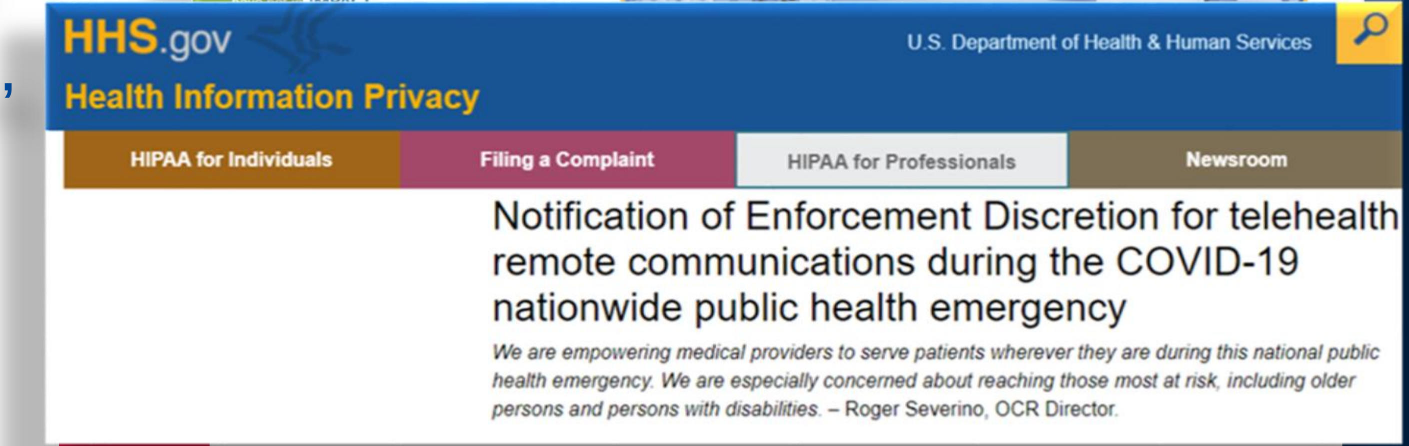
What is an Attack on Connected Medical Devices?

The Food and Drug Administration (FDA) defines a medical device as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease."

Real-World Scenario:

A threat actor gains access to a care provider's computer network through an e-mail phishing attack. He proceeds to take command of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the ICU, putting multiple patients at risk.

IMPACT



HHS.gov

U.S. Department of Health & Human Services

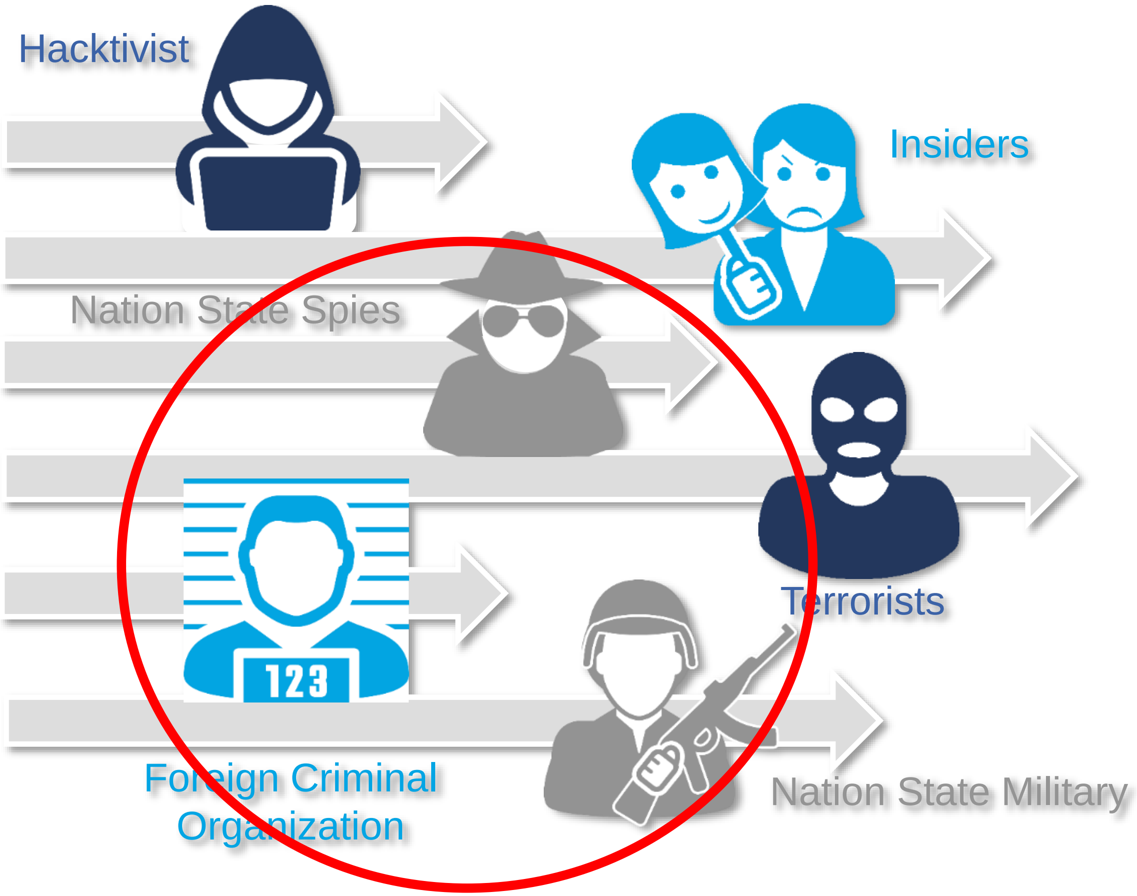
Health Information Privacy

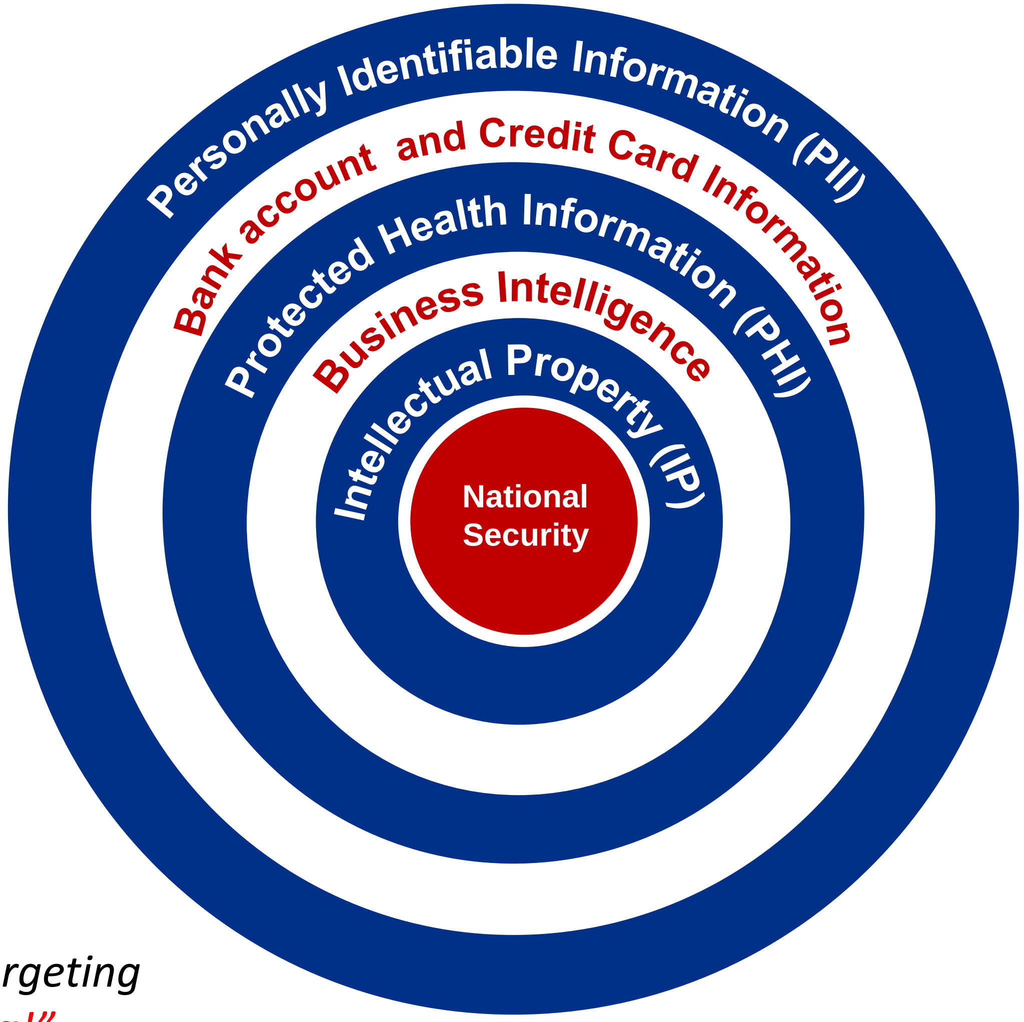
Notification of Enforcement Discretion for telehealth remote communications during the COVID-19 nationwide public health emergency

*We are empowering medical providers to serve patients wherever they are during this national public health emergency. We are especially concerned about reaching those most at risk, including older persons and persons with disabilities.* – Roger Severino, OCR Director.

# Healthcare = Data Rich Environment = Target Rich Environment

## Targeted Data

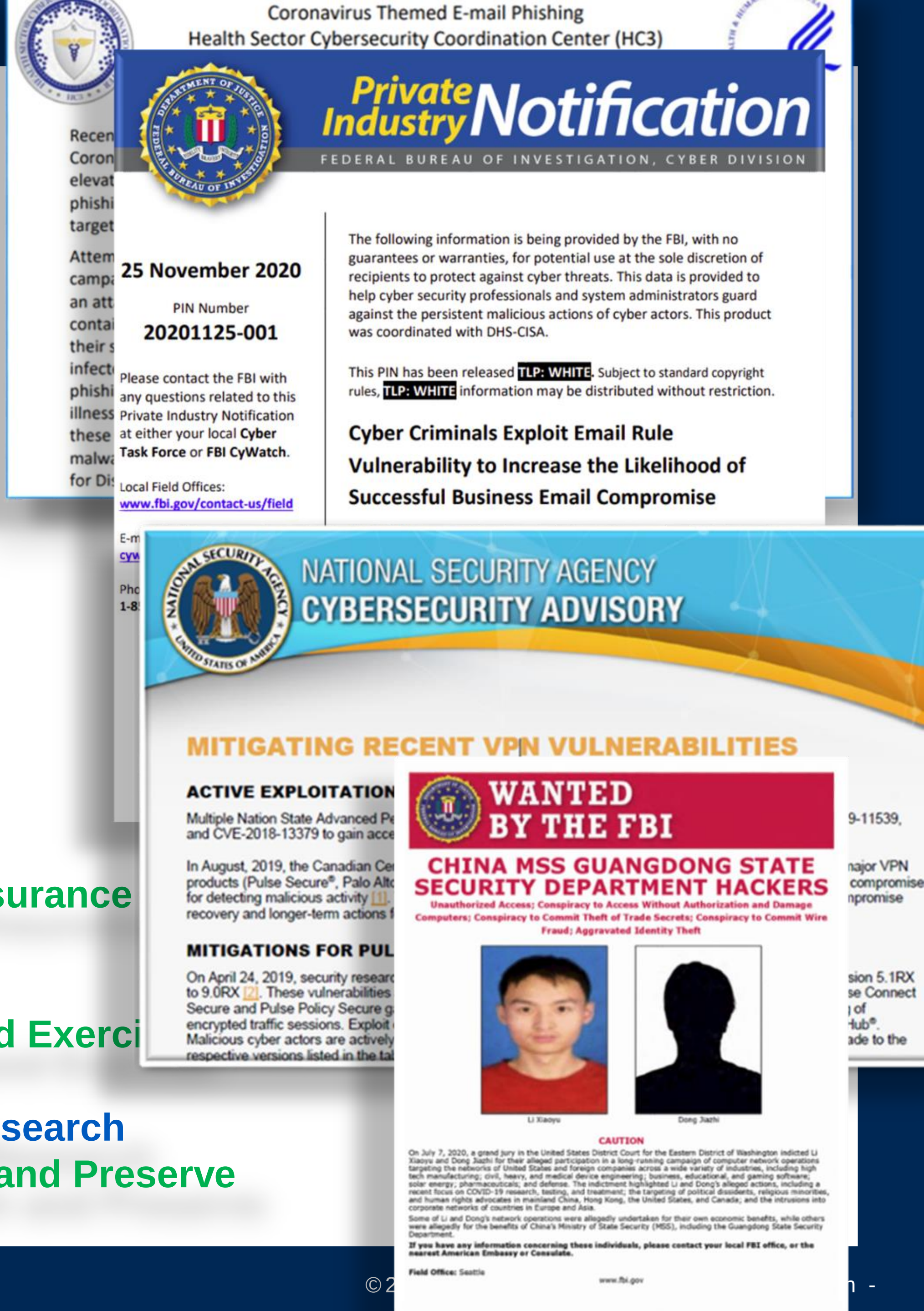



Personally Identifiable Information (PII)
Bank account and Credit Card Information
Protected Health Information (PHI)
Business Intelligence
Intellectual Property (IP)
National Security

*Nation states, criminals, insiders and hacktivists are aggressively targeting healthcare providers to steal their valuable data. **"One stop hacking!"***

# Threat 2: Increased Attacks

- Up to a 700% increase in phishing emails, including BEC
  - MFA, Email ATP, Verbal Authentication – *Education!*
- Attacks on devices and remote network vulnerabilities
  - Network/Device Mapping, Inventory, Security and Patching
- Business Associate and Cloud Attacks
  - Data Mapping, Vendor Risk Management Program, BAA, Cyber Insurance
- Ransomware Attacks – Patient Care and Safety Issue!
  - Redundant Offline Backups, Patching, Incident Response Plan and Exerci
- Theft of COVID Related Research, Treatment Protocols and Vaccine Research
  - Risk Management Program to Identify Risk and Protect Research and Preserve Government Funding



Coronavirus Themed E-mail Phishing
Health Sector Cybersecurity Coordination Center (HC3)

Recen
Coron
elevat
phishi
target
Attem
campa
an att
contai
their s
infect
phishi
illness
these
malwa
for Di

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

25 November 2020

PIN Number
20201125-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-m
cyw

Pho
1-8

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This product was coordinated with DHS-CISA.

This PIN has been released **TLP: WHITE**. Subject to standard copyright rules, **TLP: WHITE** information may be distributed without restriction.

**Cyber Criminals Exploit Email Rule Vulnerability to Increase the Likelihood of Successful Business Email Compromise**

NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

MITIGATING RECENT VPN VULNERABILITIES

ACTIVE EXPLOITATION

Multiple Nation State Advanced Pe | 9-11539,
and CVE-2018-13379 to gain acce

In August, 2019, the Canadian Ce | najor VPN
products (Pulse Secure®, Palo Alto | compromise
for detecting malicious activity [1]. | npromise
recovery and longer-term actions f

MITIGATIONS FOR PUL

On April 24, 2019, security researc | sion 5.1RX
to 9.0RX [2]. These vulnerabilities | se Connect
Secure and Pulse Policy Secure g | of
encrypted traffic sessions. Exploit | Hub®.
Malicious cyber actors are actively | ade to the
respective versions listed in the tal

WANTED
BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaoyu

Dong Jiazhi

CAUTION

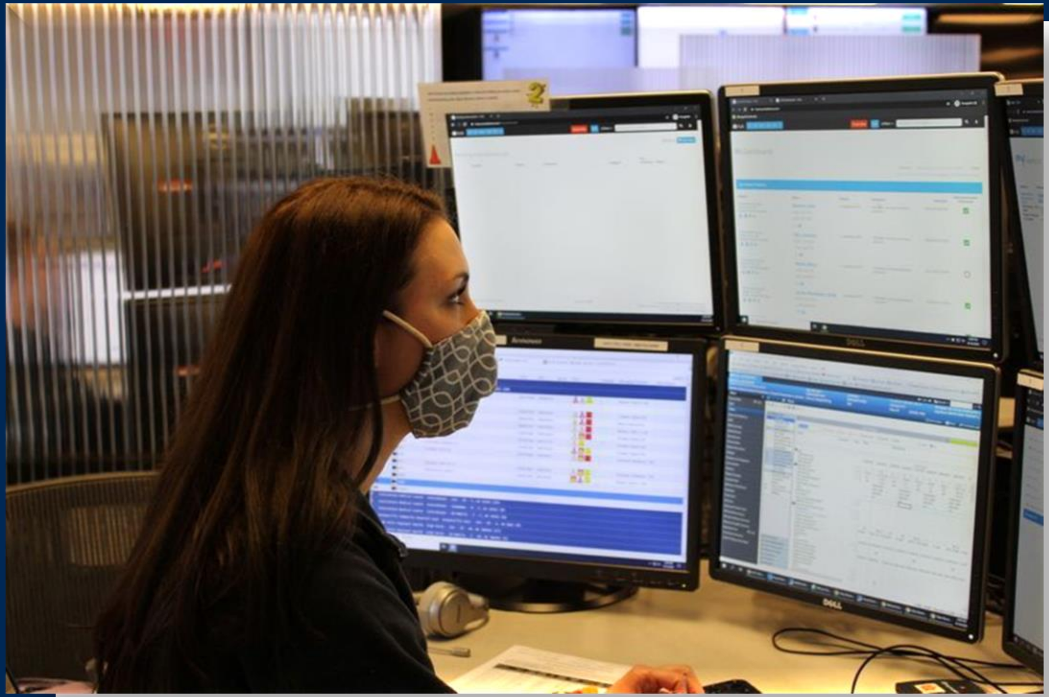
On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaoyu and Dong Jiazhi for their alleged participation in a long-running campaign of computer network operations targeting the networks of United States and foreign companies across a wide variety of industries, including high tech manufacturing; civil, heavy, and medical device engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. The indictment highlighted Li and Dong's alleged actions, including a recent focus on COVID-19 research, testing, and treatment; the targeting of political dissidents, religious minorities, and human rights advocates in mainland China, Hong Kong, the United States, and Canada; and the intrusions into corporate networks of countries in Europe and Asia.

Some of Li and Dong's network operations were allegedly undertaken for their own economic benefits, while others were allegedly for the benefits of China's Ministry of State Security (MSS), including the Guangdong State Security Department.

**If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.**

**Field Office:** Seattle

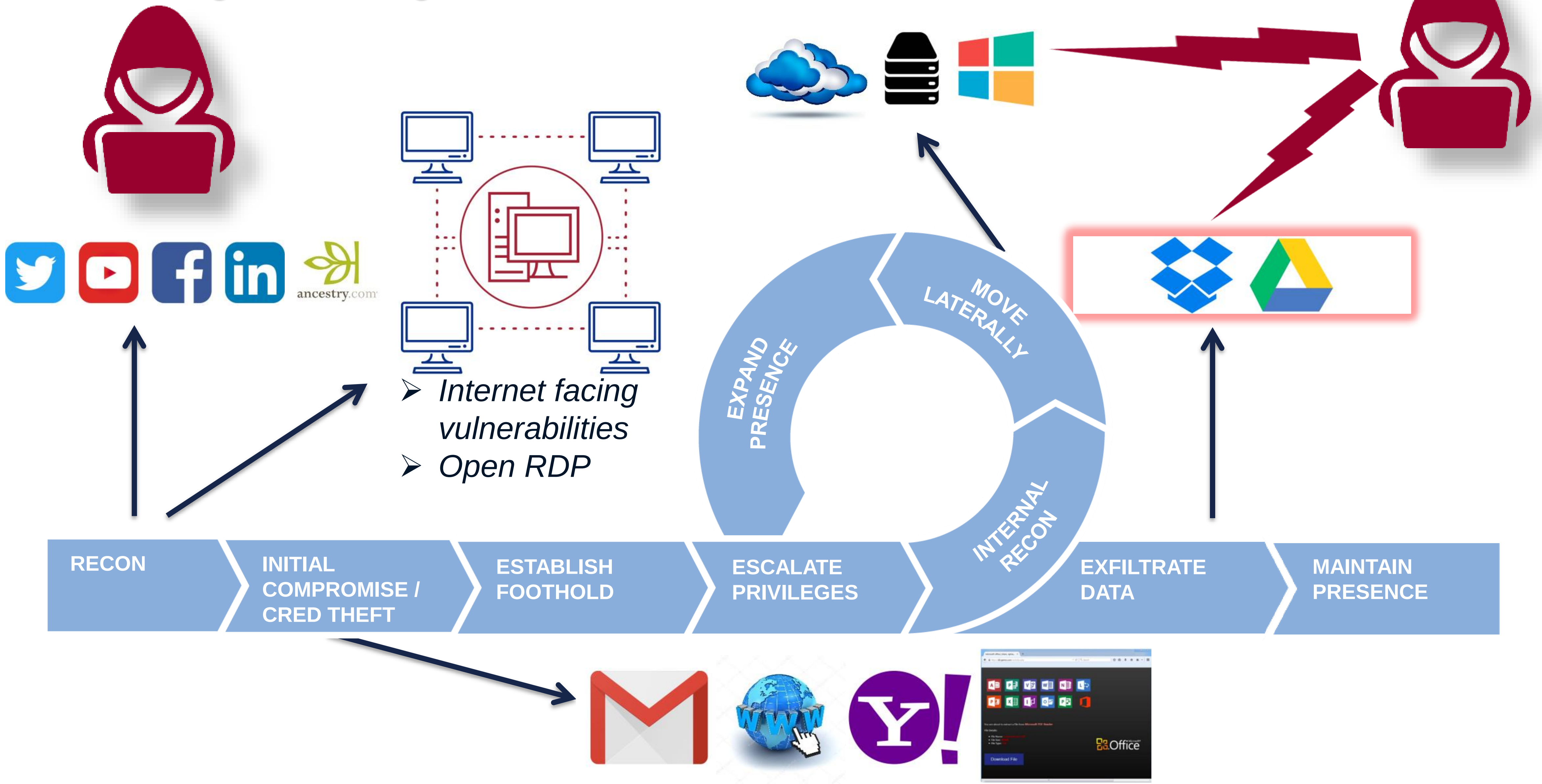
www.fbi.gov



# *Threat 3: Resource Constraints*

- **Hospitals and health systems face human, financial and technical cybersecurity resource constraints *due to reduced hospital revenue***
- ***The AHA released a report in June which estimated the total losses for hospitals and health systems to be at least $323 billion***
- ***Leaving limited funds available to bolster cybersecurity defenses, recruit and retain scarce cybersecurity professionals***

# Anatomy of a Cyber Attack



- Internet facing vulnerabilities
- Open RDP

RECON

INITIAL COMPROMISE / CRED THEFT

ESTABLISH FOOTHOLD

ESCALATE PRIVILEGES

INTERNAL RECON

MOVE LATERALLY

EXPAND PRESENCE

EXFILTRATE DATA

MAINTAIN PRESENCE

# Polling Questions:

1) Do you use multi-factor authentication on ALL your social media and personal email accounts?

Polling Options: Yes, No, I Don’t Know

2) Does your organization conduct email phishing tests?

Polling Options: Yes, No, I Don’t Know

3) Does your organization use a warning banner to identify emails originating from outside the organization?

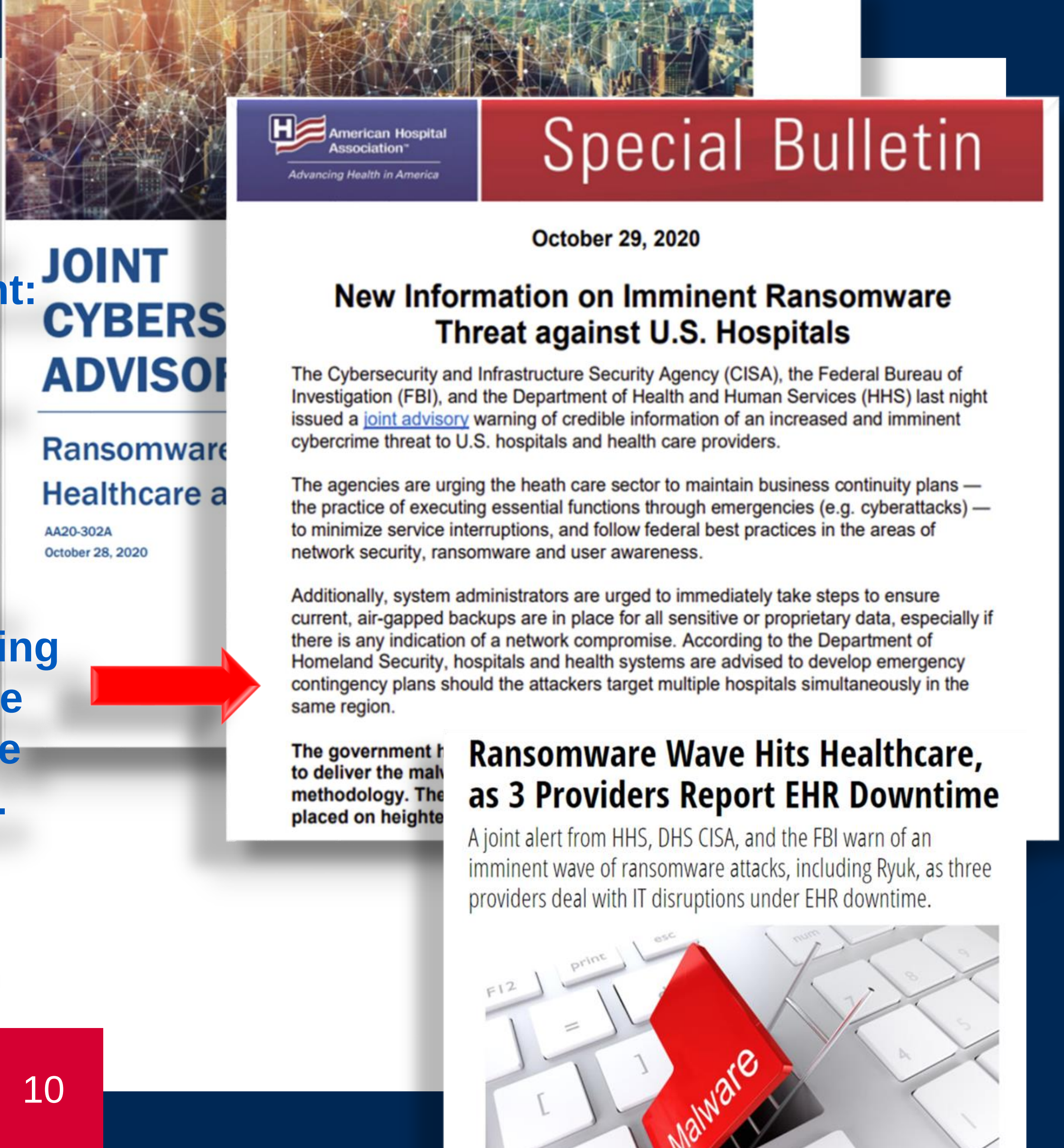
Polling Options: Yes, No, I Don’t Know

# October 28 – 30

- On 10/28 late evening, an unprecedented cyber warning is issued by the government: "CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."

- On 10/29 the AHA which has been directly briefed by DHS and FBI ahead of the warning and issues a special bulletin amplifying the warning and indicating phishing emails are the primary attack "vector" / methodology.

- Potential for multiple hospitals being targeted in same region simultaneously



JOINT CYBERS
ADVISOF

Ransomware
Healthcare a

AA20-302A
October 28, 2020

American Hospital Association™
Advancing Health in America

Special Bulletin

October 29, 2020

**New Information on Imminent Ransomware Threat against U.S. Hospitals**

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) last night issued a joint advisory warning of credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers.

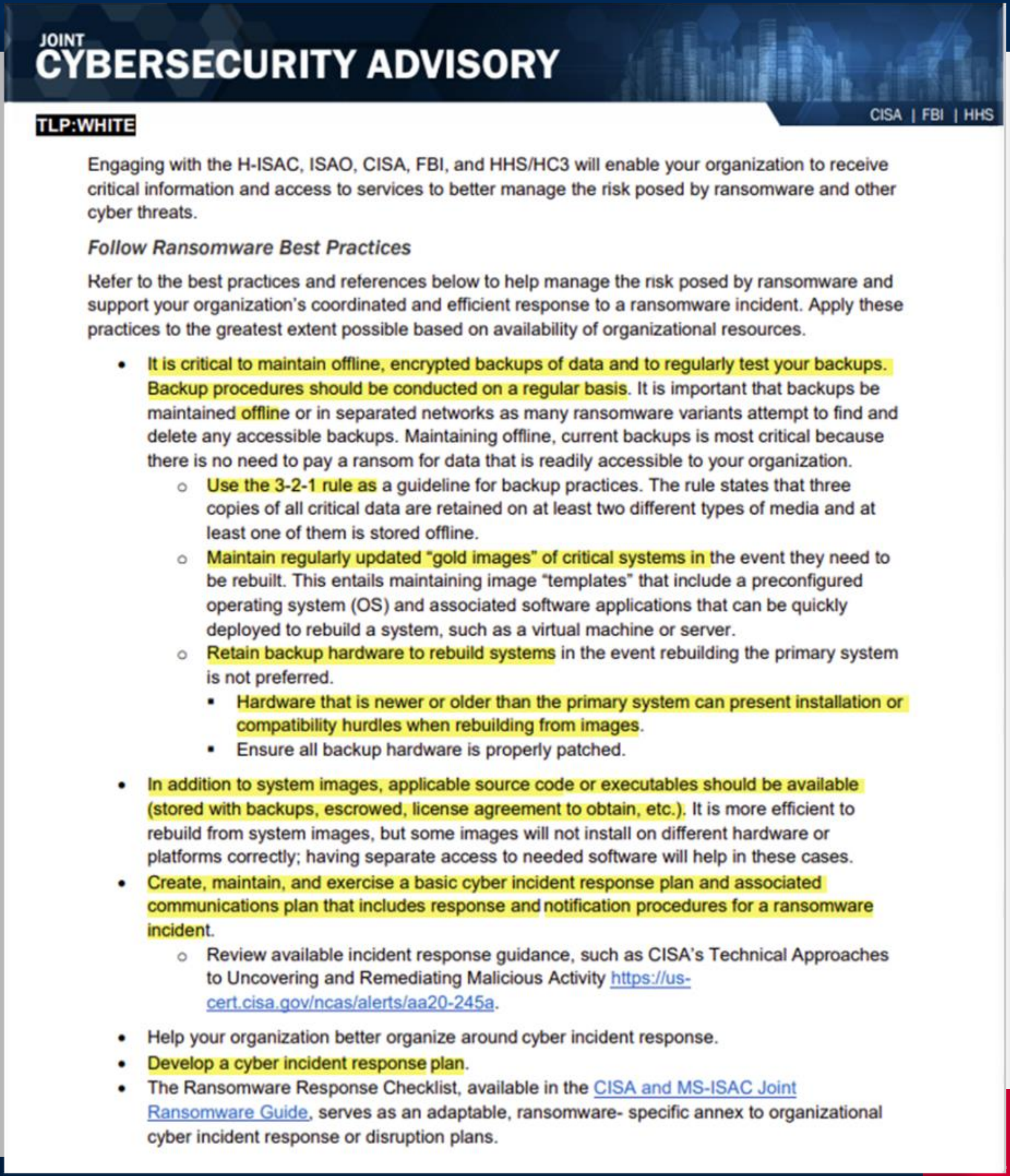
The agencies are urging the heath care sector to maintain business continuity plans — the practice of executing essential functions through emergencies (e.g. cyberattacks) — to minimize service interruptions, and follow federal best practices in the areas of network security, ransomware and user awareness.

Additionally, system administrators are urged to immediately take steps to ensure current, air-gapped backups are in place for all sensitive or proprietary data, especially if there is any indication of a network compromise. According to the Department of Homeland Security, hospitals and health systems are advised to develop emergency contingency plans should the attackers target multiple hospitals simultaneously in the same region.

**The government h**
**to deliver the malw**
**methodology. The**
**placed on heighte**

**Ransomware Wave Hits Healthcare, as 3 Providers Report EHR Downtime**

A joint alert from HHS, DHS CISA, and the FBI warn of an imminent wave of ransomware attacks, including Ryuk, as three providers deal with IT disruptions under EHR downtime.

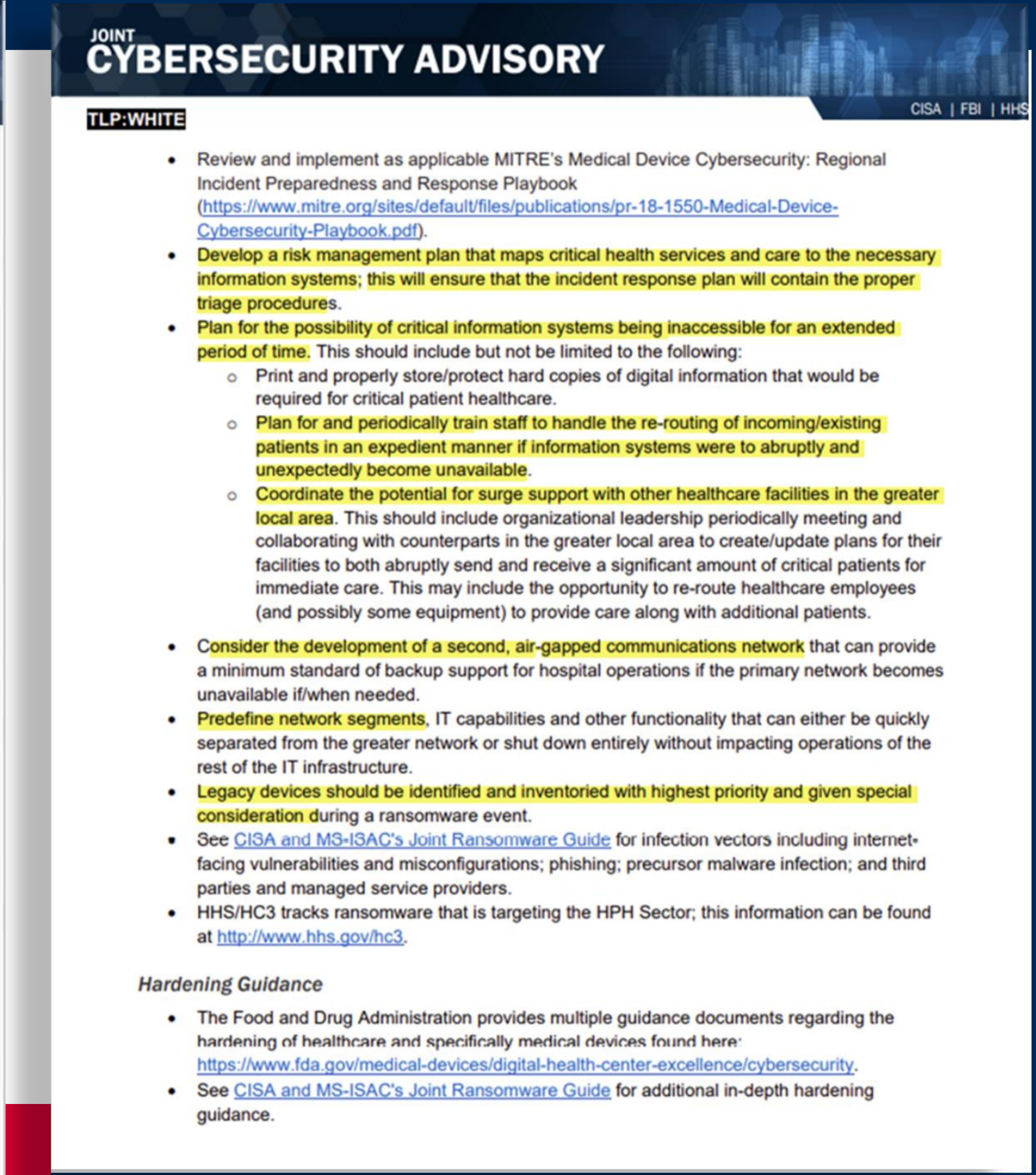


Engaging with the H-ISAC, ISAO, CISA, FBI, and HHS/HC3 will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

*Follow Ransomware Best Practices*

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.

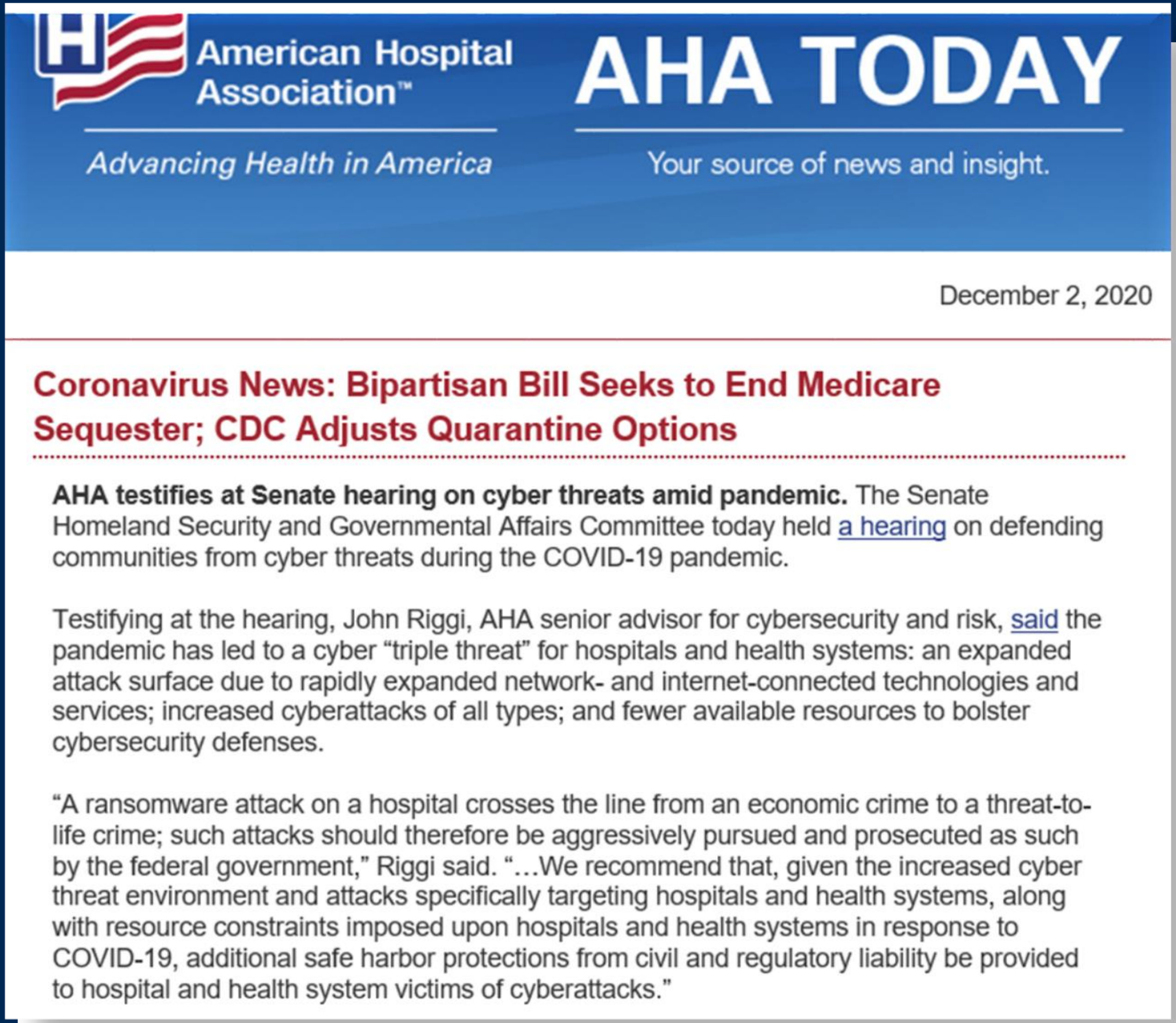
- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline or in separated networks as many ransomware variants attempt to find and delete any accessible 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.
    - Use the 3-2-1 rule as a guideline for backup practices. The rule states that three copies of all critical data are retained on at least two different types of media and at least one of them is stored offline.
    - 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.
        - Ensure all backup hardware is properly patched.
- 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 CISA's Technical Approaches to Uncovering and Remediating Malicious Activity https://us-cert.cisa.gov/ncas/alerts/aa20-245a.
- Help your organization better organize around cyber incident response.
- Develop a cyber incident response plan.
- The Ransomware Response Checklist, available in the CISA and MS-ISAC Joint Ransomware Guide, serves as an adaptable, ransomware- specific annex to organizational cyber incident response or disruption plans.



- Review and implement as applicable MITRE's Medical Device Cybersecurity: Regional Incident Preparedness and Response Playbook (https://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf).
- Develop a risk management plan that maps critical health services and care to the necessary information systems; this will ensure that the incident response plan will contain the proper triage procedures.
- Plan for the possibility of critical information systems being inaccessible for an extended period of time. This should include but not be limited to the following:
    - Print and properly store/protect hard copies of digital information that would be required for critical patient healthcare.
    - Plan for and periodically train staff to handle the re-routing of incoming/existing patients in an expedient manner if information systems were to abruptly and unexpectedly become unavailable.
    - Coordinate the potential for surge support with other healthcare facilities in the greater local area. This should include organizational leadership periodically meeting and collaborating with counterparts in the greater local area to create/update plans for their facilities to both abruptly send and receive a significant amount of critical patients for immediate care. This may include the opportunity to re-route healthcare employees (and possibly some equipment) to provide care along with additional patients.
- Consider the development of a second, air-gapped communications network that can provide a minimum standard of backup support for hospital operations if the primary network becomes unavailable if/when needed.
- Predefine network segments, IT capabilities and other functionality that can either be quickly separated from the greater network or shut down entirely without impacting operations of the rest of the IT infrastructure.
- Legacy devices should be identified and inventoried with highest priority and given special consideration during a ransomware event.
- See CISA and MS-ISAC's Joint Ransomware Guide for infection vectors including internet-facing vulnerabilities and misconfigurations; phishing; precursor malware infection; and third parties and managed service providers.
- HHS/HC3 tracks ransomware that is targeting the HPH Sector; this information can be found at http://www.hhs.gov/hc3.

*Hardening Guidance*

- The Food and Drug Administration provides multiple guidance documents regarding the hardening of healthcare and specifically medical devices found here: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.
- See CISA and MS-ISAC's Joint Ransomware Guide for additional in-depth hardening guidance.



American Hospital Association™

Advancing Health in America

# AHA TODAY

Your source of news and insight.

December 2, 2020

## Coronavirus News: Bipartisan Bill Seeks to End Medicare Sequester; CDC Adjusts Quarantine Options

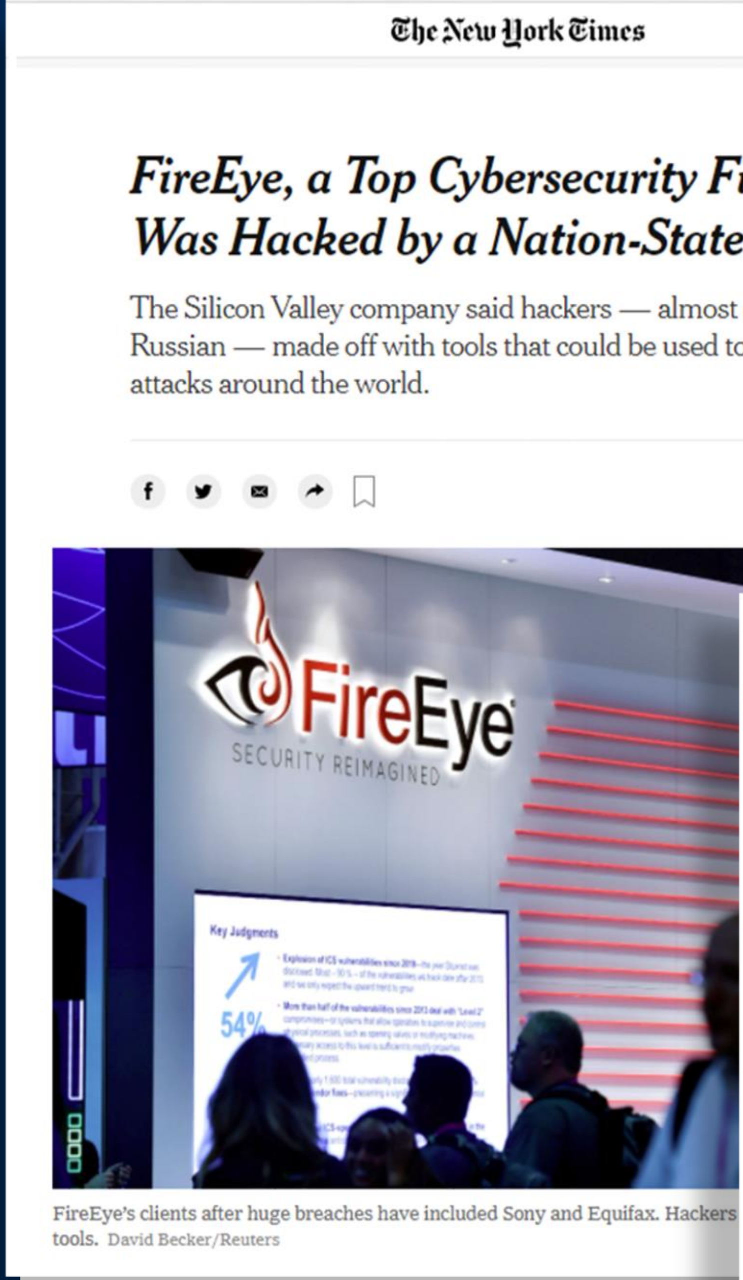
**AHA testifies at Senate hearing on cyber threats amid pandemic.** The Senate Homeland Security and Governmental Affairs Committee today held a hearing on defending communities from cyber threats during the COVID-19 pandemic.

Testifying at the hearing, John Riggi, AHA senior advisor for cybersecurity and risk, said the pandemic has led to a cyber "triple threat" for hospitals and health systems: an expanded attack surface due to rapidly expanded network- and internet-connected technologies and services; increased cyberattacks of all types; and fewer available resources to bolster cybersecurity defenses.

"A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; such attacks should therefore be aggressively pursued and prosecuted as such by the federal government," Riggi said. "…We recommend that, given the increased cyber threat environment and attacks specifically targeting hospitals and health systems, along with resource constraints imposed upon hospitals and health systems in response to COVID-19, additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks."

"A ransomware attack on a hospital crosses the line from an economic crime to a threat-to-life crime; these attacks should therefore be aggressively pursued and prosecuted as such"

"…With resource constraints imposed upon hospitals and health systems in response to COVID-19, ***additional safe harbor protections from civil and regulatory liability be provided to hospital and health system victims of cyberattacks."***

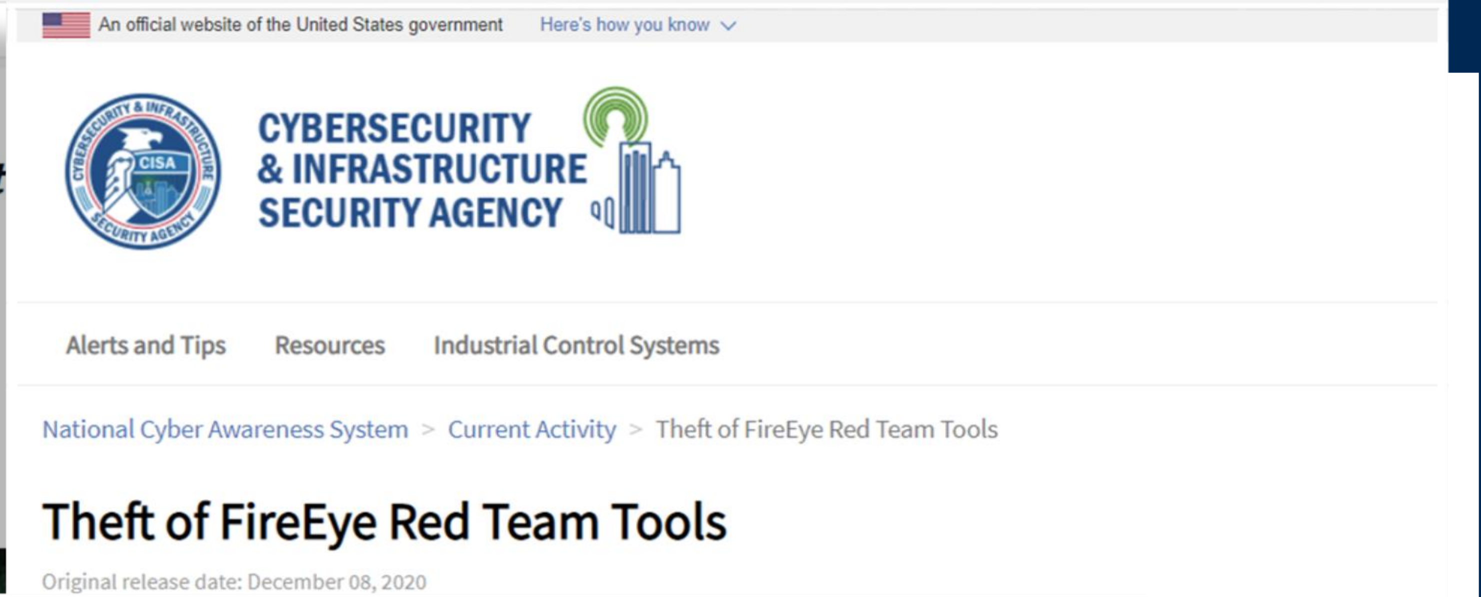


The New York Times

## FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State

The Silicon Valley company said hackers — almost certainly Russian — made off with tools that could be used to mount new attacks around the world.

FireEye's clients after huge breaches have included Sony and Equifax. Hackers tools. David Becker/Reuters



An official website of the United States government Here's how you know

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

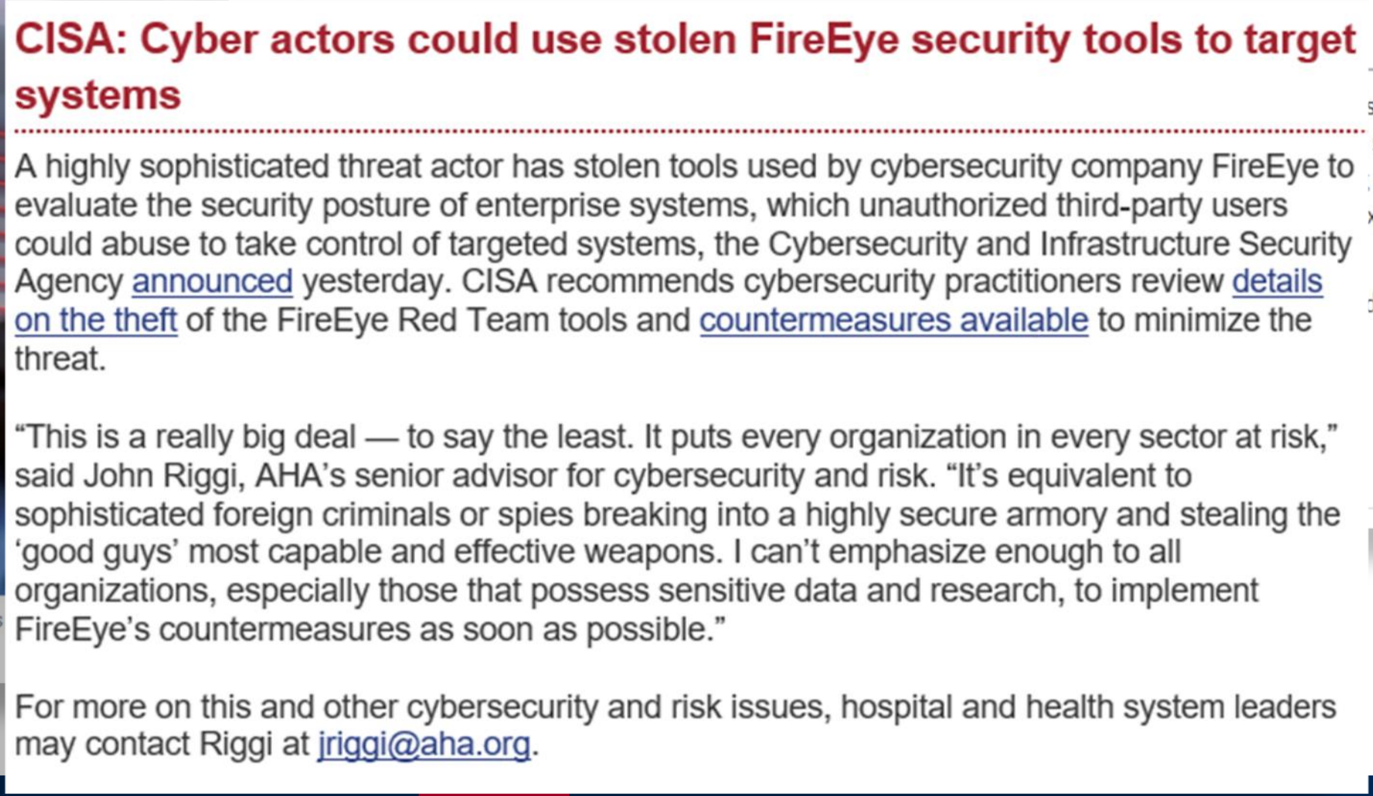
National Cyber Awareness System > Current Activity > Theft of FireEye Red Team Tools

## Theft of FireEye Red Team Tools

Original release date: December 08, 2020

sticated threat actor. Red
systems. Although the
maliciously used to
xposed tools do not

d FireEye's GitHub

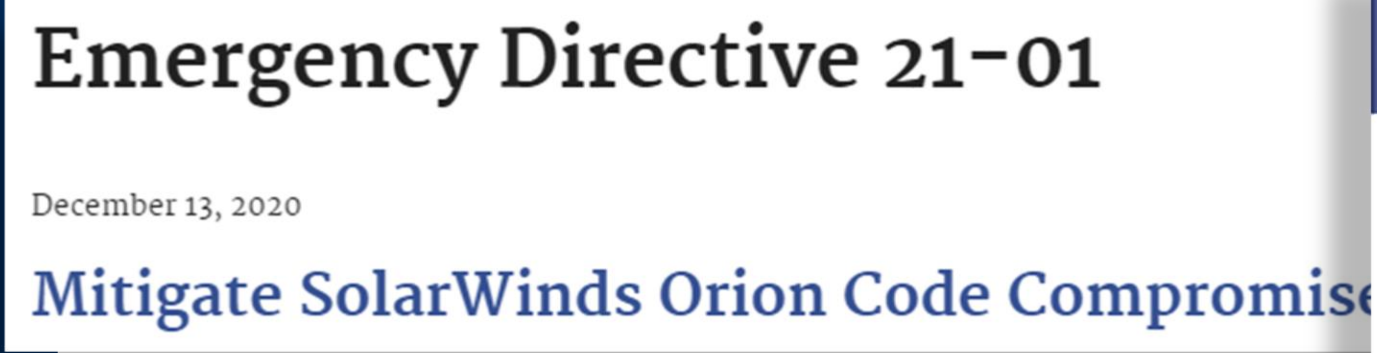


## CISA: Cyber actors could use stolen FireEye security tools to target systems

A highly sophisticated threat actor has stolen tools used by cybersecurity company FireEye to evaluate the security posture of enterprise systems, which unauthorized third-party users could abuse to take control of targeted systems, the Cybersecurity and Infrastructure Security Agency announced yesterday. CISA recommends cybersecurity practitioners review details on the theft of the FireEye Red Team tools and countermeasures available to minimize the threat.

"This is a really big deal — to say the least. It puts every organization in every sector at risk," said John Riggi, AHA's senior advisor for cybersecurity and risk. "It's equivalent to sophisticated foreign criminals or spies breaking into a highly secure armory and stealing the 'good guys' most capable and effective weapons. I can't emphasize enough to all organizations, especially those that possess sensitive data and research, to implement FireEye's countermeasures as soon as possible."

For more on this and other cybersecurity and risk issues, hospital and health system leaders may contact Riggi at jriggi@aha.org.



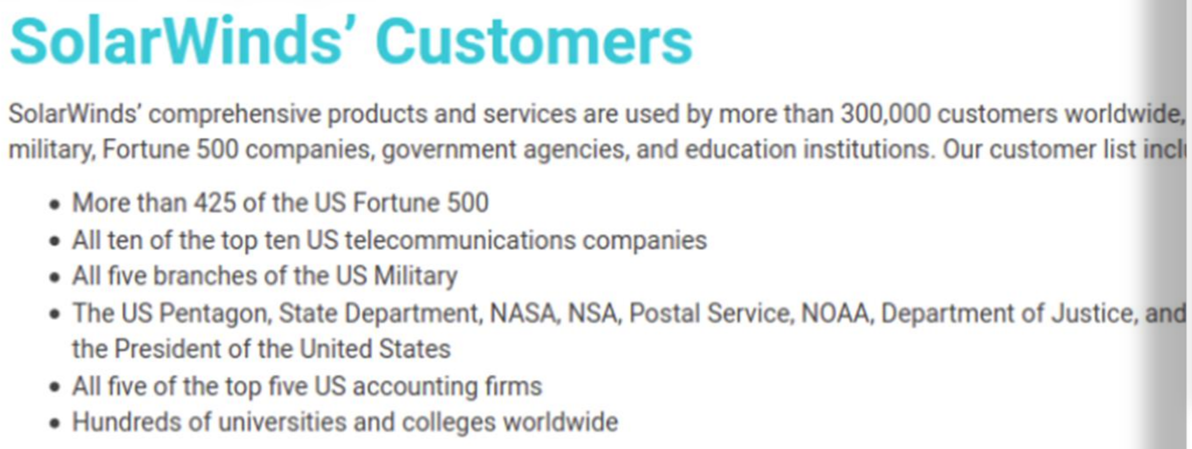
# Emergency Directive 21-01

December 13, 2020

## Mitigate SolarWinds Orion Code Compromise

"Affected agencies shall immediately disconnect or power down SolarWinds Orion products, versions 2019.4 through 2020.2.1 HF1, from their network."

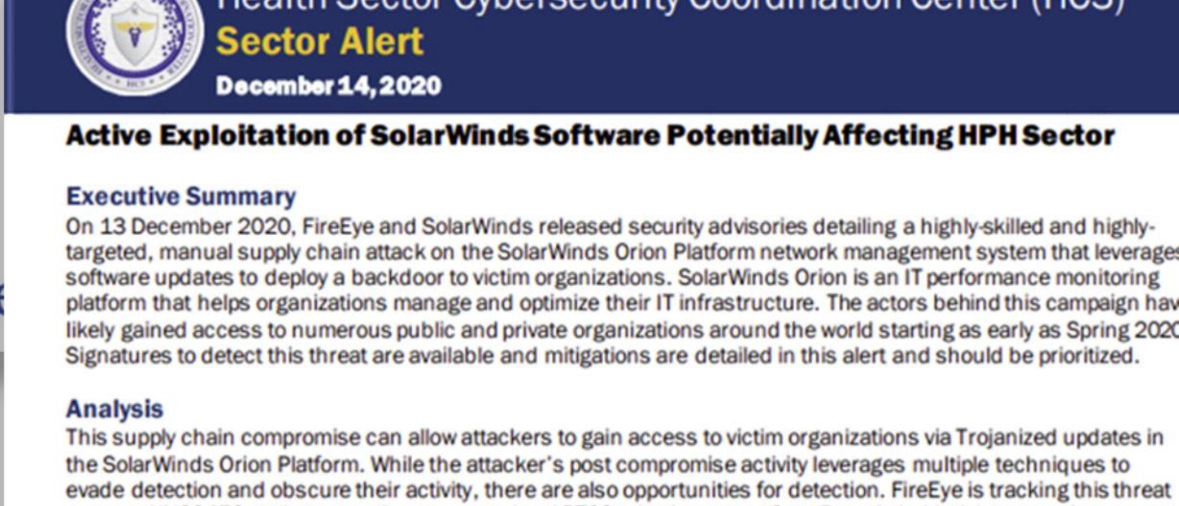
"Treat all hosts monitored by the SolarWinds Orion monitoring software as compromised by threat actors and assume that further persistence mechanisms have been deployed"



## SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, military, Fortune 500 companies, government agencies, and education institutions. Our customer list incl

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide



Health Sector Cybersecurity Coordination Center (HC3)

**Sector Alert**

**December 14, 2020**

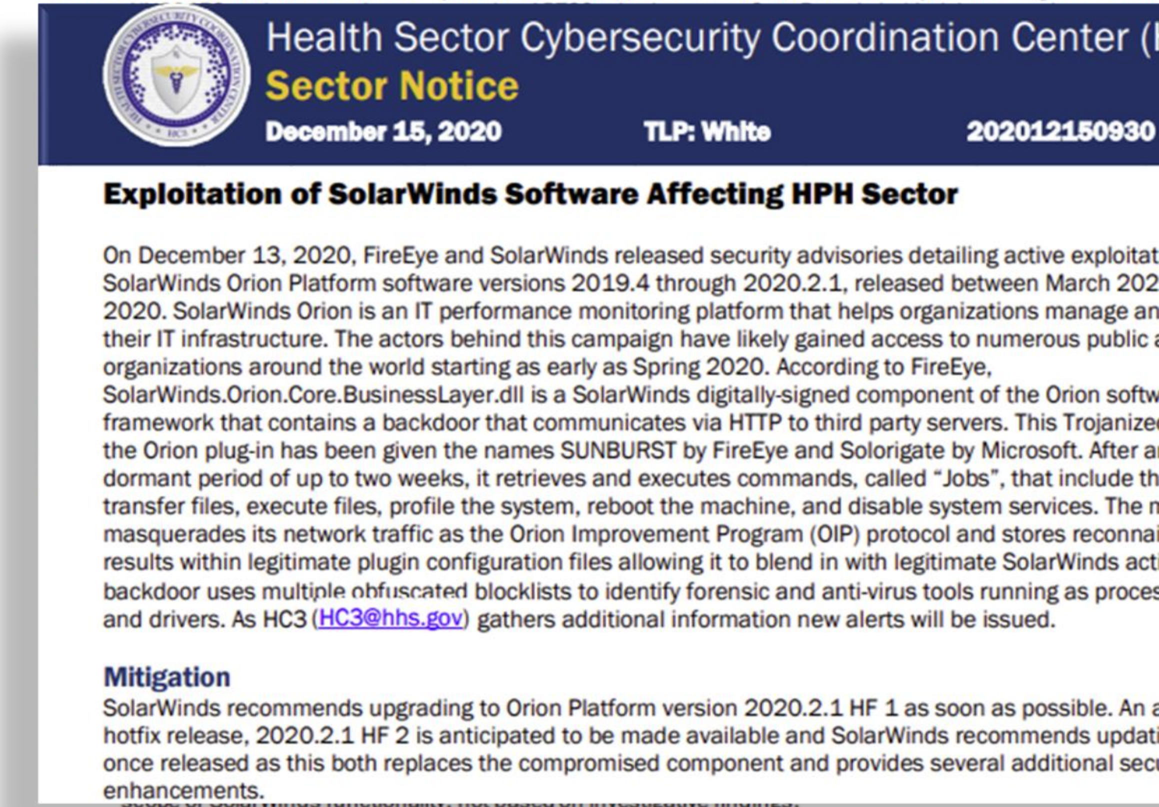
**Active Exploitation of SolarWinds Software Potentially Affecting HPH Sector**

**Executive Summary**

On 13 December 2020, FireEye and SolarWinds released security advisories detailing a highly-skilled and highly-targeted, manual supply chain attack on the SolarWinds Orion Platform network management system that leverage software updates to deploy a backdoor to victim organizations. SolarWinds Orion is an IT performance monitoring platform that helps organizations manage and optimize their IT infrastructure. The actors behind this campaign hav likely gained access to numerous public and private organizations around the world starting as early as Spring 202 Signatures to detect this threat are available and mitigations are detailed in this alert and should be prioritized.

**Analysis**

This supply chain compromise can allow attackers to gain access to victim organizations via Trojanized updates in the SolarWinds Orion Platform. While the attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, there are also opportunities for detection. FireEye is tracking this threat



Health Sector Cybersecurity Coordination Center (

**Sector Notice**

**December 15, 2020** **TLP: White** **202012150930**

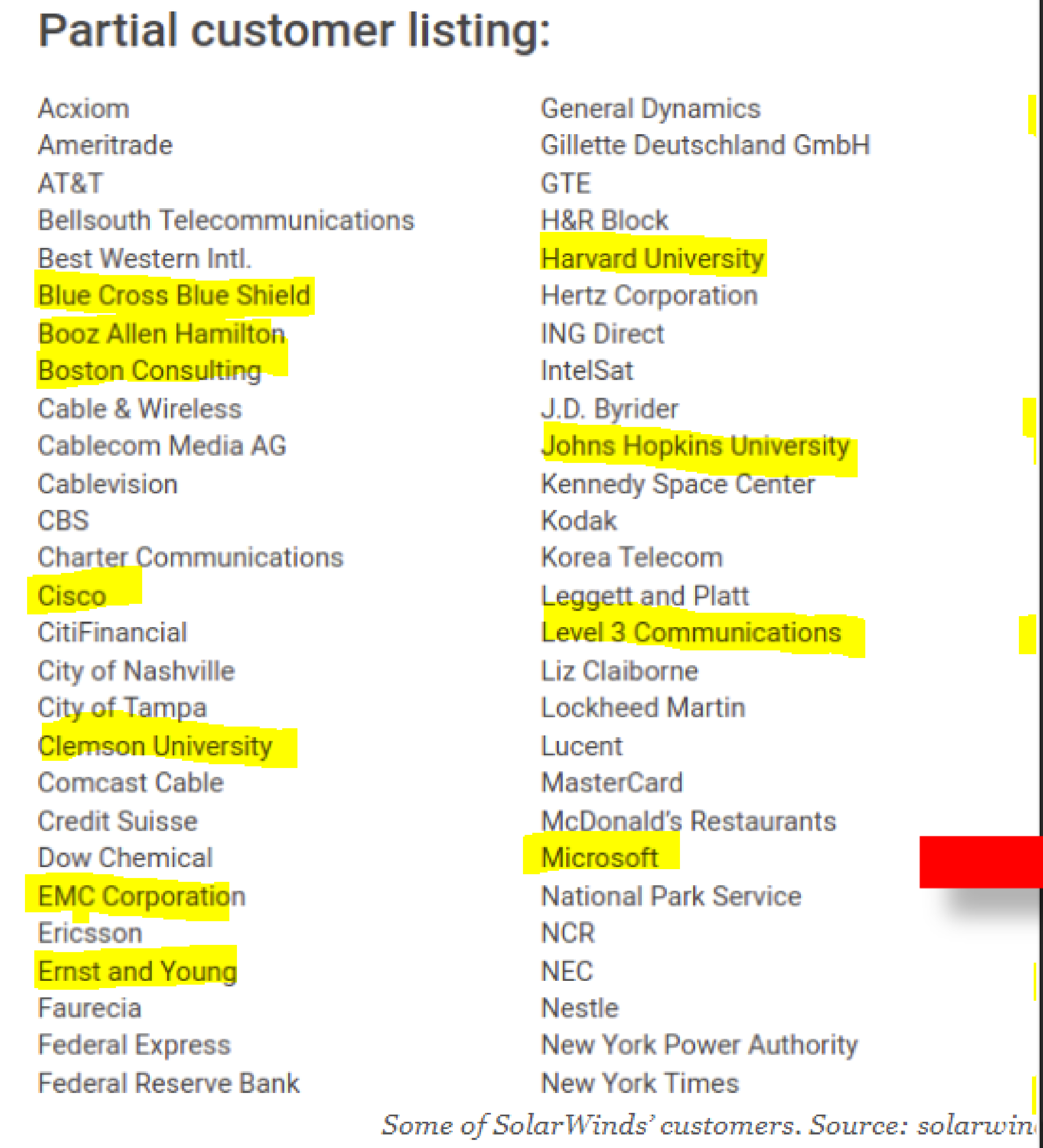
**Exploitation of SolarWinds Software Affecting HPH Sector**

On December 13, 2020, FireEye and SolarWinds released security advisories detailing active exploitat SolarWinds Orion Platform software versions 2019.4 through 2020.2.1, released between March 202 2020. SolarWinds Orion is an IT performance monitoring platform that helps organizations manage an their IT infrastructure. The actors behind this campaign have likely gained access to numerous public a organizations around the world starting as early as Spring 2020. According to FireEye, SolarWinds.Orion.Core.BusinessLayer.dll is a SolarWinds digitally-signed component of the Orion softw framework that contains a backdoor that communicates via HTTP to third party servers. This Trojanize the Orion plug-in has been given the names SUNBURST by FireEye and Solorigate by Microsoft. After a dormant period of up to two weeks, it retrieves and executes commands, called "Jobs", that include th transfer files, execute files, profile the system, reboot the machine, and disable system services. The m masquerades its network traffic as the Orion Improvement Program (OIP) protocol and stores reconnai results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds act backdoor uses multiple obfuscated blocklists to identify forensic and anti-virus tools running as proce and drivers. As HC3 (HC3@hhs.gov) gathers additional information new alerts will be issued.

**Mitigation**

SolarWinds recommends upgrading to Orion Platform version 2020.2.1 HF 1 as soon as possible. An a hotfix release, 2020.2.1 HF 2 is anticipated to be made available and SolarWinds recommends updati once released as this both replaces the compromised component and provides several additional secu enhancements.

SolarWinds recommends upgrading to Orion Platform version 2020.2.1 HF 1 as soon as possible. An additional hotfix release, 2020.2.1 HF 2 is anticipated to be made available Tuesday, December 15, 2020 and SolarWinds recommends updating to HF 2 once released as this both replaces the compromised component and provides several additional security enhancements.

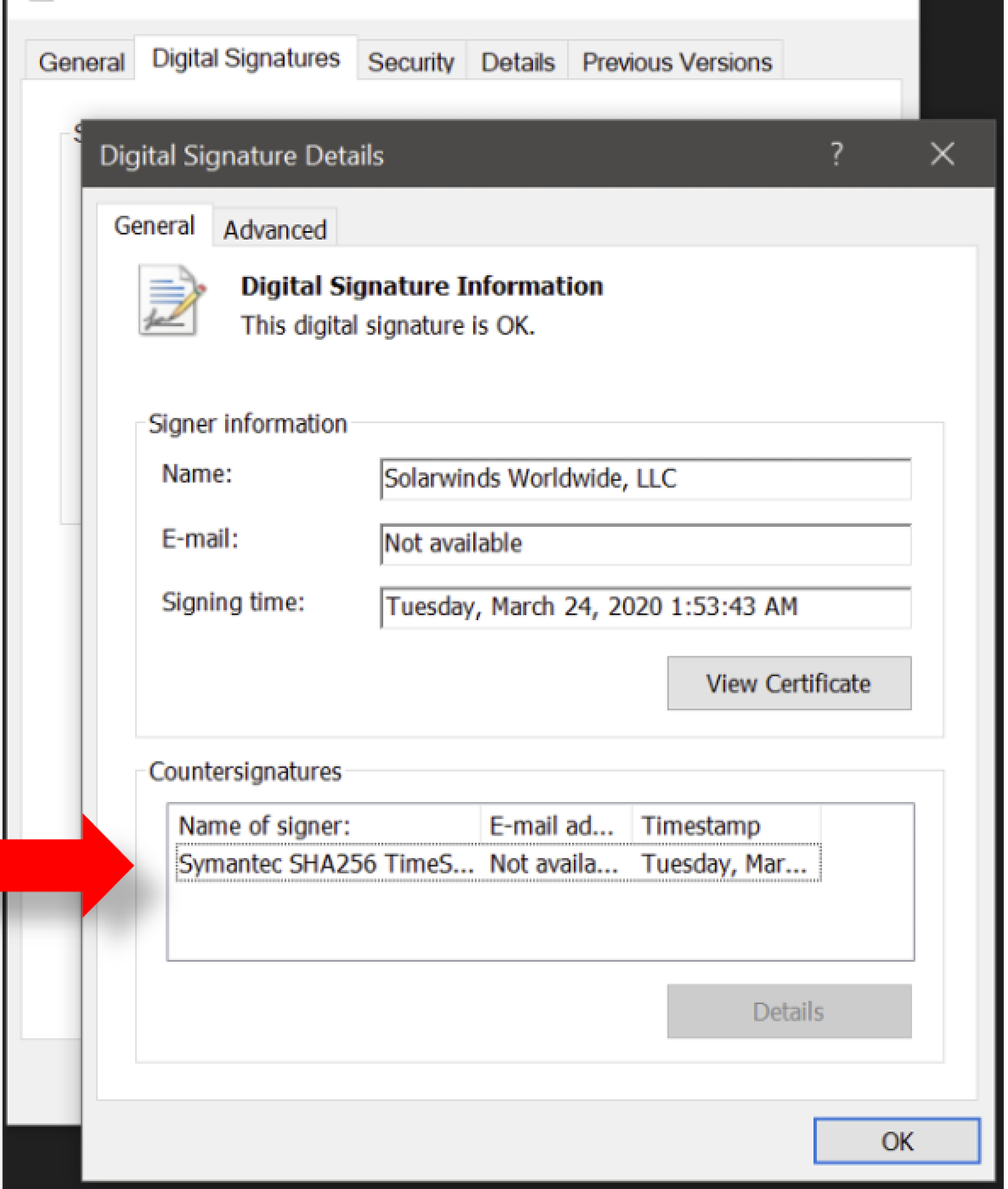


# Partial customer listing:

Acxiom
Ameritrade
AT&T
Bellsouth Telecommunications
Best Western Intl.
Blue Cross Blue Shield
Booz Allen Hamilton
Boston Consulting
Cable & Wireless
Cablecom Media AG
Cablevision
CBS
Charter Communications
Cisco
CitiFinancial
City of Nashville
City of Tampa
Clemson University
Comcast Cable
Credit Suisse
Dow Chemical
EMC Corporation
Ericsson
Ernst and Young
Faurecia
Federal Express
Federal Reserve Bank

General Dynamics
Gillette Deutschland GmbH
GTE
H&R Block
Harvard University
Hertz Corporation
ING Direct
IntelSat
J.D. Byrider
Johns Hopkins University
Kennedy Space Center
Kodak
Korea Telecom
Leggett and Platt
Level 3 Communications
Liz Claiborne
Lockheed Martin
Lucent
MasterCard
McDonald's Restaurants
Microsoft
National Park Service
NCR
NEC
Nestle
New York Power Authority
New York Times

*Some of SolarWinds' customers. Source: solarwin*



Digital Signature Details

**Digital Signature Information**
This digital signature is OK.

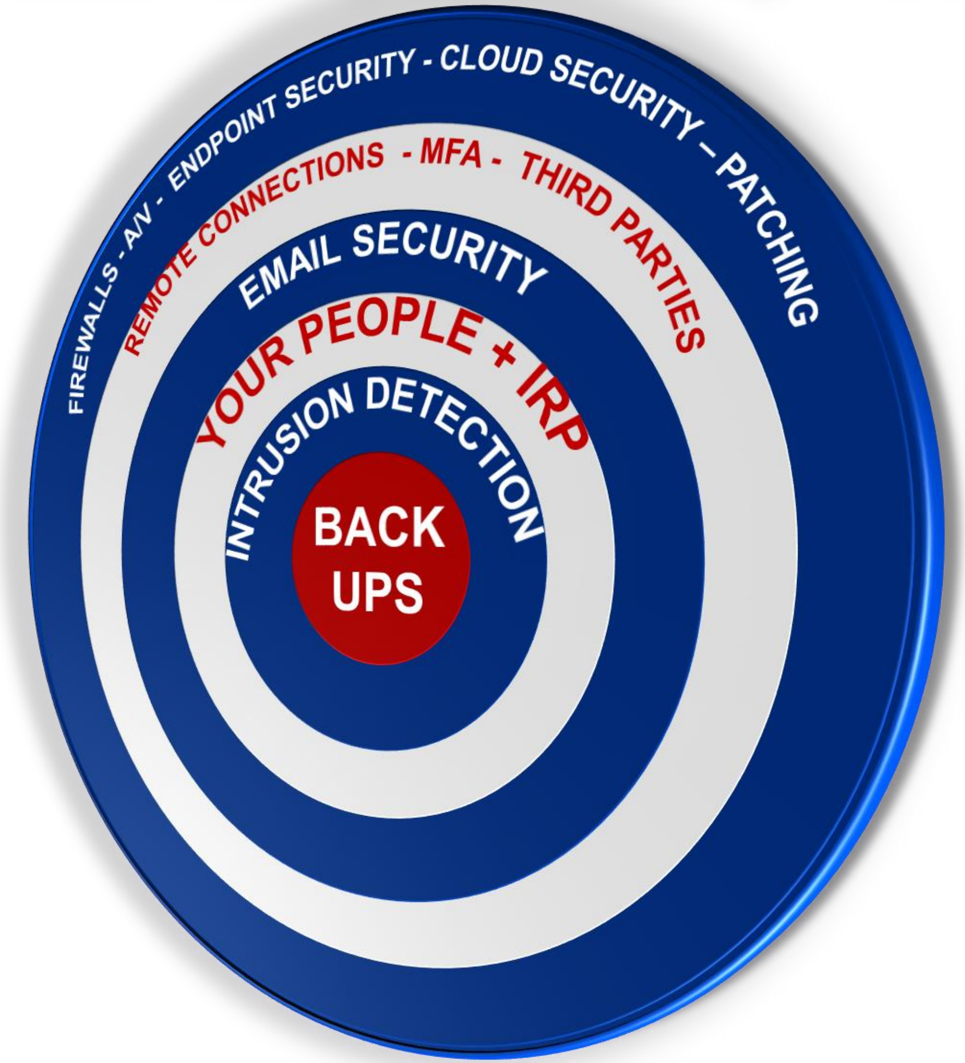
Signer information

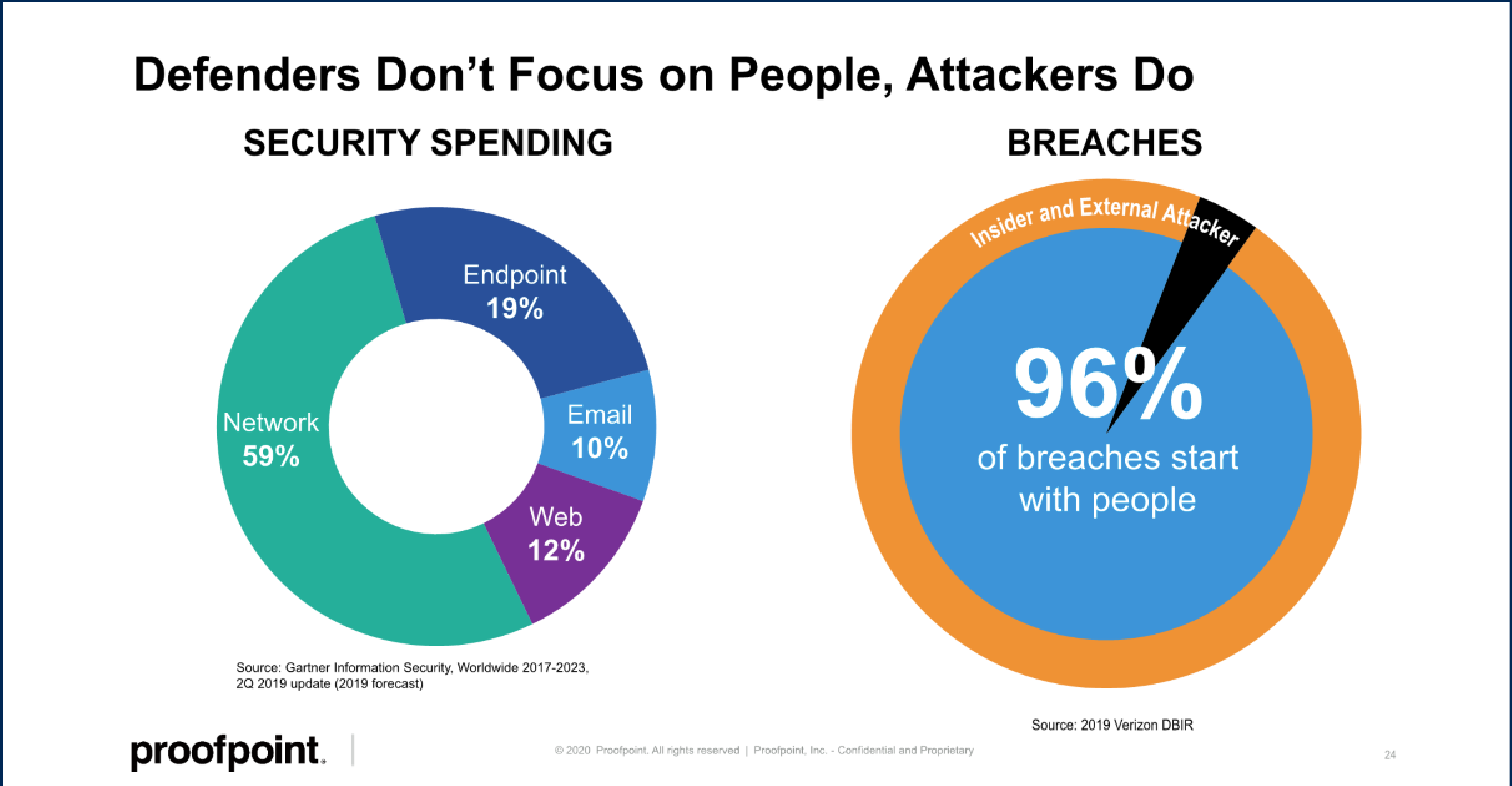
Name: Solarwinds Worldwide, LLC
E-mail: Not available
Signing time: Tuesday, March 24, 2020 1:53:43 AM

Countersignatures

| Name of signer: | E-mail ad... | Timestamp |
|---|---|---|
| Symantec SHA256 TimeS... | Not availa... | Tuesday, Mar... |

# A Layered Approach to Cybersecurity = Defense in Depth


FIREWALLS - A/V - ENDPOINT SECURITY - CLOUD SECURITY – PATCHING
REMOTE CONNECTIONS - MFA - THIRD PARTIES
EMAIL SECURITY
YOUR PEOPLE + IRP
INTRUSION DETECTION
BACK UPS



# Defenders Don’t Focus on People, Attackers Do

## SECURITY SPENDING

Source: Gartner Information Security, Worldwide 2017-2023, 2Q 2019 update (2019 forecast)

## BREACHES

96%

of breaches start with people

Source: 2019 Verizon DBIR

# Strategic Vendor Risk Management Program Considerations

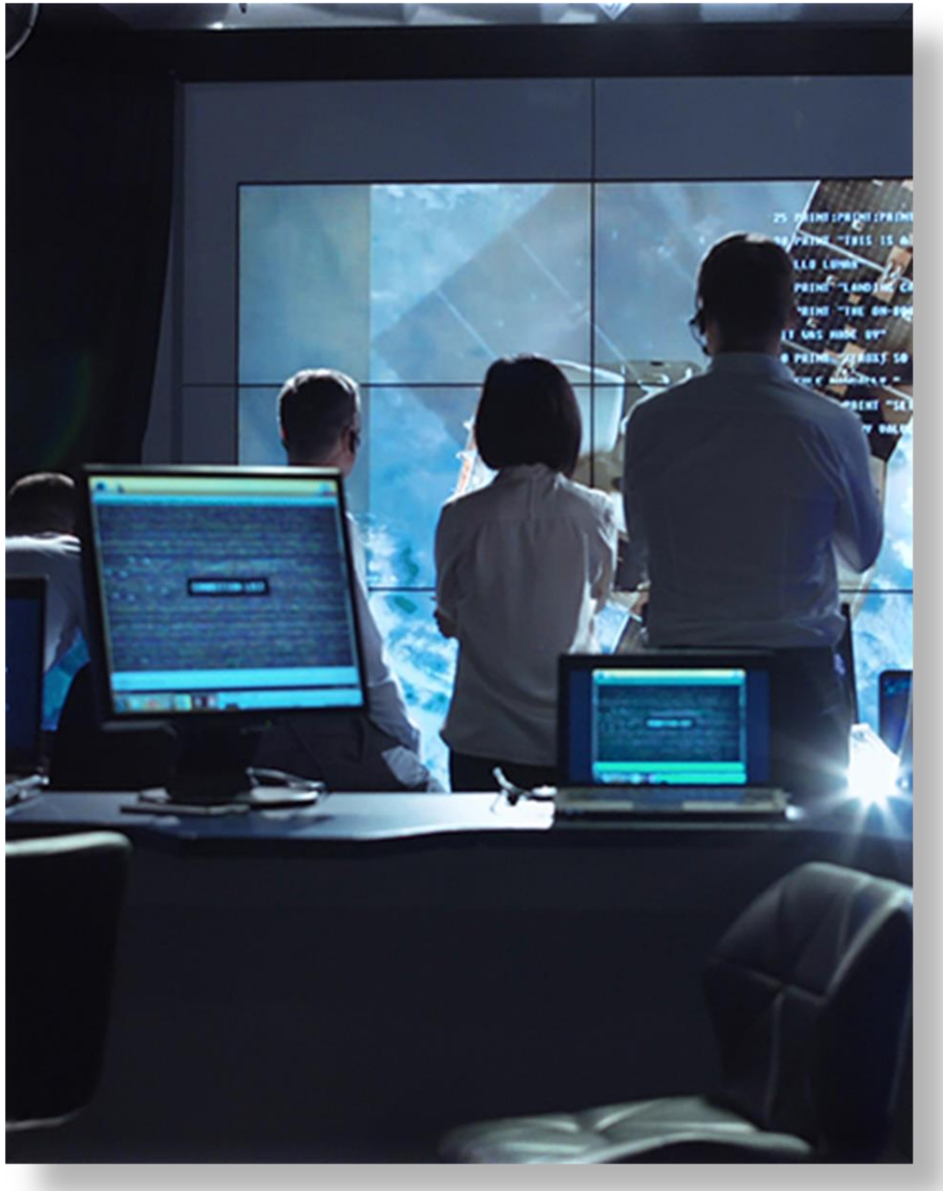
American Hospital Association™

*Advancing Health in America*

https://healthsectorcouncil.org/wp-content/uploads/2020/09/Health-Industry-Cybersecurity-Supply-Chain-Risk-Management-Guide-v2.pdf

- Does your organization have a vendor risk management program (VRM)? What is the governance structure and does that structure still make sense?
- Is there a formal process to incorporate cybersecurity in the VRM program?
- Is there process to conduct periodic in-depth technical, legal, policy and procedural review of the VRM program and the BAA?
- Does the BAA include cybersecurity and cyber insurance requirements for the vendor and any subs of the vendor? Are the coverages and limits sufficient?
- Annual cyber risk assessments for vendors?
- Compliance requirements with applicable regulatory standards - HIPAA, PCI, PII, taxpayer funded medical research and IP?
- **Identify, risk classify and risk prioritize** vendors *and their subcontractors* based upon:
- **Aggregation** of data – regulated data and unregulated data such as pop health genetic studies, clinical trials, COVID-19 research
- **Access** to sensitive data, networks, systems and physical locations
- **Criticality/Impact** to continuity of operations - Clinical, facilities, utilities, business (e.g. telecom, medical transcription, billing and coding, PPE supplies, etc)
- **Foreign** operations and foreign subcontractors
- **Implement risk based controls and cyber insurance requirements**
- Need to balance financial opportunities and greater supply-chain flexibility with potentially higher cyber risks associated with certain vendors

# Cyber Incident Response Plan



- *Backup status and security, 3-2-1, restoration point and time, offline?*
- Do we have a **unified** cyber-incident response plan & is it up to date?
- Multi-day impact and multi-incident plan?
- Does it include specific individuals from all clinical, business, admin and facilities functions - with defined roles, responsibilities and ***off hours contact information and plan access?***
- Activation and decision escalation protocol and matrices?
- Leadership role – ***designation and delegation of critical authorities***?
- Is the plan regularly tested, gaps and best practices identified and updated to include current threat scenarios such as ransomware?
- Legal, regulatory, financial and reputational risks?
- Internal and external communications strategy?
- Out of band communications ?
- Paper copies and downtime procedures?
- Continuity of operations – emergency management?
- Cyber insurance requirements – forensics firm ?
- FBI, government and forensics firm integration?

# Polling Questions:

1) Do you have an updated cross function cyber incident response plan?

Polling Options: Yes, No, I Don’t Know

2) Do you have cyber insurance?

Polling Options: Yes, No, I Don’t Know

# Risk Tolerance and Cyber Insurance

- **How much cyber risk are we willing to accept?**
- **How much risk are we willing to transfer?**
- Do we have cyber insurance?
- What are the limitations and requirements?
- Vendor and subcontractor requirements?
- **Scales with VRM risk prioritization**
- Is our cyber insurance coverage adequate and current to cover all costs associated with a:
  - Multi-day network outage
  - Breach mitigation and recovery
  - Lost revenue
  - Reputational harm
  - Legal and regulatory exposure
  - Victim and patient services – credit monitoring
- Forensics firms panel – integration with IRP
- Interaction and integration with other insurance policies
- Ransomware coverage – bitcoin
- “Act of war” exemption for cyber?

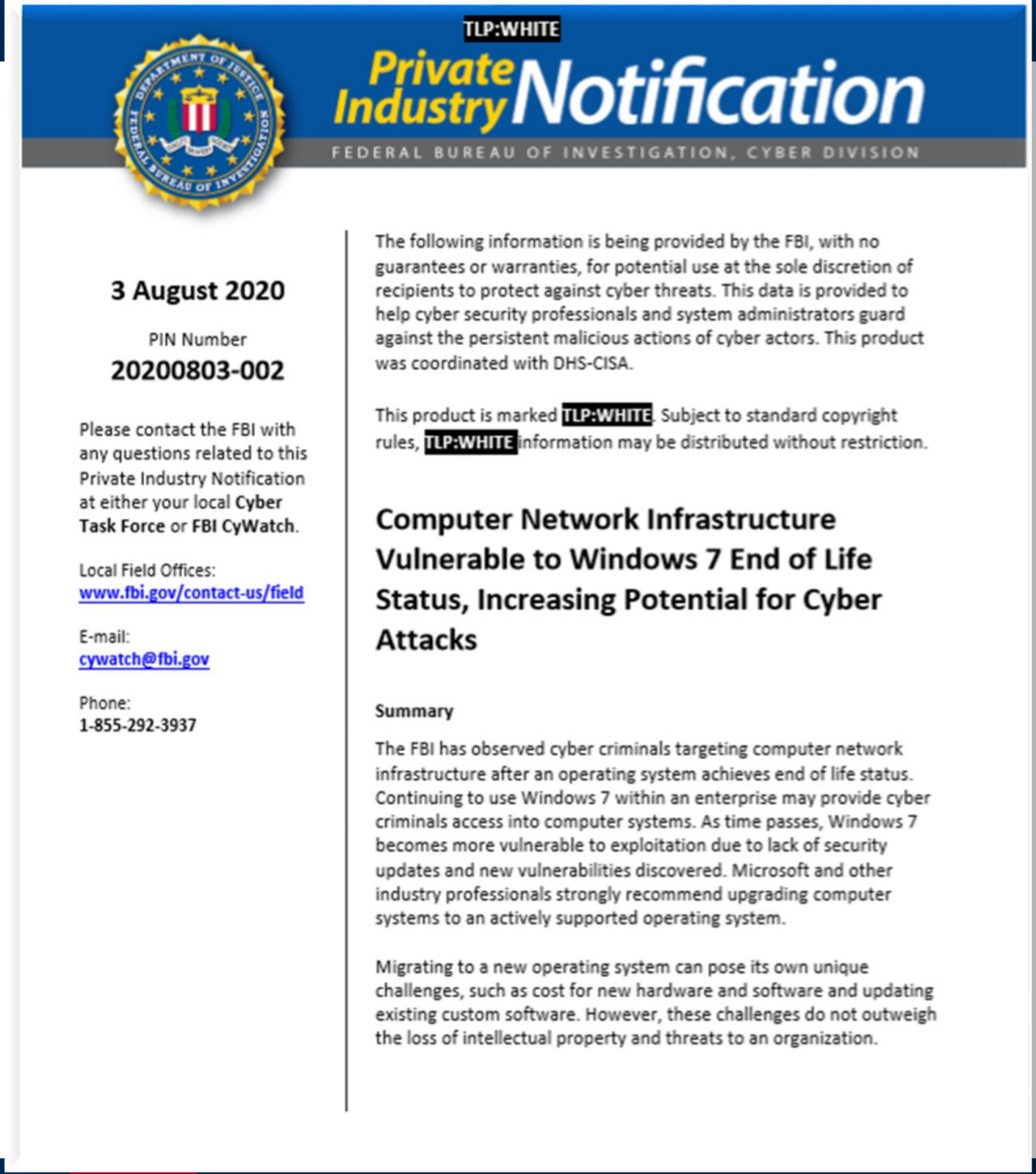
# Polling Questions:

1) Do you have multiple backup copies of your data?

Polling Options: Yes, No, I Don’t Know

1) If yes, are the backup copies offline and network and segmented?

Polling Options: Yes, No, I Don’t Know



TLP:WHITE

# Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

**3 August 2020**

PIN Number
**20200803-002**

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
**1-855-292-3937**

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This product was coordinated with DHS-CISA.

This product is marked TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

## Computer Network Infrastructure Vulnerable to Windows 7 End of Life Status, Increasing Potential for Cyber Attacks

**Summary**

The FBI has observed cyber criminals targeting computer network infrastructure after an operating system achieves end of life status. Continuing to use Windows 7 within an enterprise may provide cyber criminals access into computer systems. As time passes, Windows 7 becomes more vulnerable to exploitation due to lack of security updates and new vulnerabilities discovered. Microsoft and other industry professionals strongly recommend upgrading computer systems to an actively supported operating system.

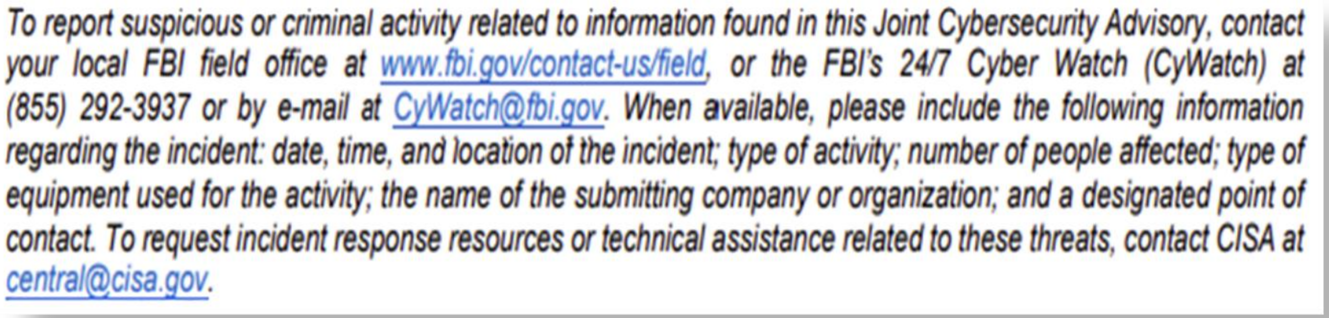
Migrating to a new operating system can pose its own unique challenges, such as cost for new hardware and software and updating existing custom software. However, these challenges do not outweigh the loss of intellectual property and threats to an organization.

American Hospital Association.

jriggi@aha.org

(O) +1 202-626-2272
(M) +1 202-640-9159

# Questions, Thoughts?



*To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at central@cisa.gov.*

## JOHN RIGGI
## Senior Advisor for Cybersecurity and Risk

### Experience Summary

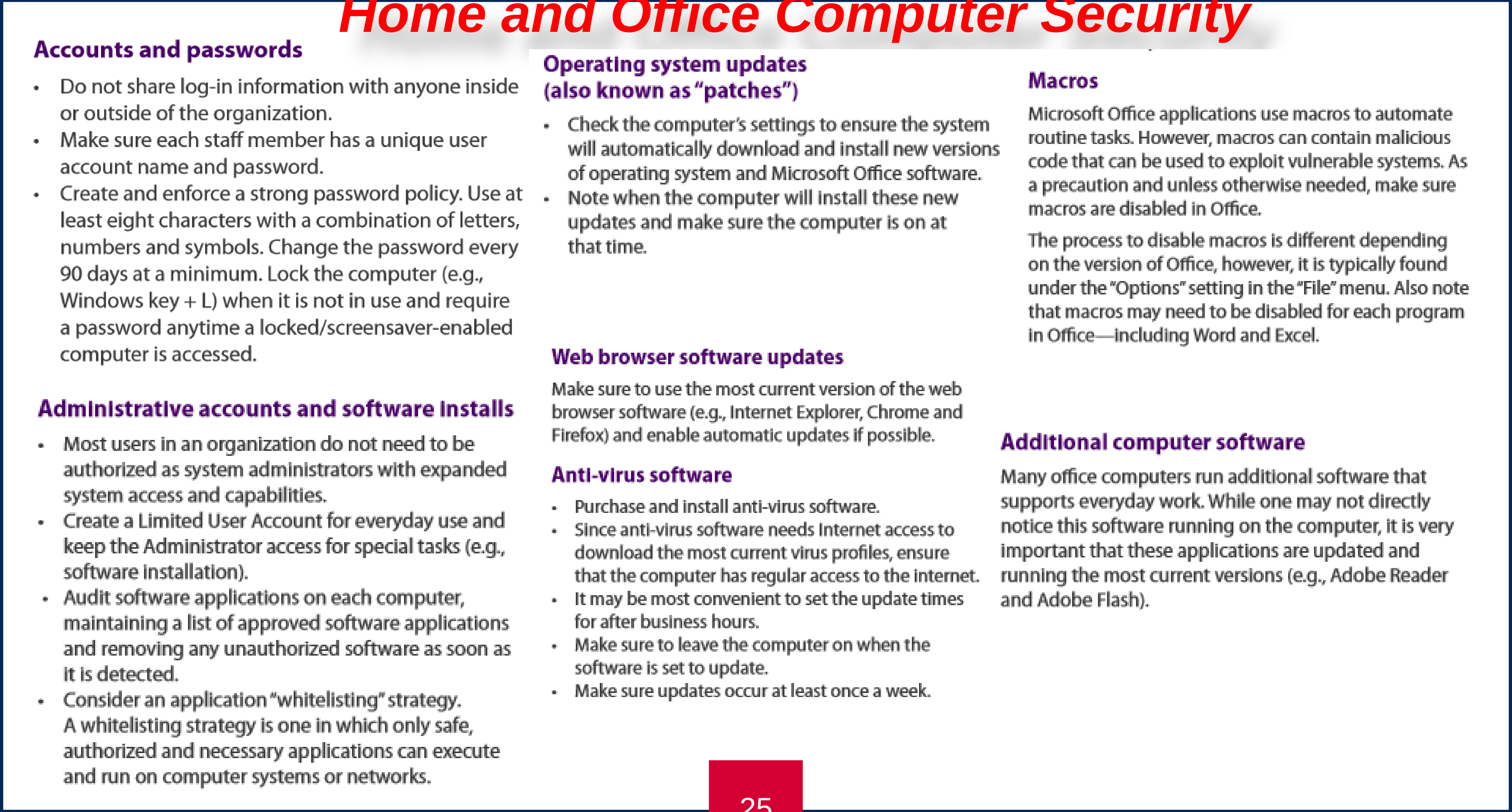
John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first senior advisor for cybersecurity and risk for the American Hospital Association and their 5000+ member hospitals. John leverages his distinctive experience at the FBI and CIA in the investigation and disruption of cyber threats, international organized crime and terrorist organizations to assist on policy and advocacy issues and provide trusted advisory services for the nations' hospitals and health systems. His trusted access to hospital leadership and government agencies enhances John's national perspective and ability to provide uniquely informed risk advisory services.

In various leadership roles at the FBI, John served as a representative to the White House Cyber Response Group and a senior representative to the CIA. He was also the FBI national operations manager for terrorist financing investigations. John also led counterintelligence field surveillance programs in Washington DC. John led the FBI Cyber Division national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors. John held a national strategic role in the investigation of the largest cyber attacks targeting healthcare and other sectors.

John currently co-leads a national HHS/healthcare sector task group to develop resources to assist the field in managing cyber risk as an enterprise risk issue. John launched a national campaign with the AHA and government agencies to help members protect medical research against foreign threats. John was recently selected to serve on the FCC hospital robocall protection group which will make recommendations on reducing unlawful robocalls to hospitals.

He also served on the NY FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the CIA's George H.W. Bush Award for Excellence in Counterterrorism, the CIAs highest award in this category.  John presents extensively on cybersecurity and risk topics and is frequently interviewed by the media.

# Home and Office Computer Security



## Accounts and passwords

- Do not share log-in information with anyone inside or outside of the organization.
- Make sure each staff member has a unique user account name and password.
- Create and enforce a strong password policy. Use at least eight characters with a combination of letters, numbers and symbols. Change the password every 90 days at a minimum. Lock the computer (e.g., Windows key + L) when it is not in use and require a password anytime a locked/screensaver-enabled computer is accessed.

## Administrative accounts and software installs

- Most users in an organization do not need to be authorized as system administrators with expanded system access and capabilities.
- Create a Limited User Account for everyday use and keep the Administrator access for special tasks (e.g., software installation).
- Audit software applications on each computer, maintaining a list of approved software applications and removing any unauthorized software as soon as it is detected.
- Consider an application "whitelisting" strategy. A whitelisting strategy is one in which only safe, authorized and necessary applications can execute and run on computer systems or networks.

## Operating system updates (also known as "patches")

- Check the computer's settings to ensure the system will automatically download and install new versions of operating system and Microsoft Office software.
- Note when the computer will install these new updates and make sure the computer is on at that time.

## Web browser software updates

Make sure to use the most current version of the web browser software (e.g., Internet Explorer, Chrome and Firefox) and enable automatic updates if possible.

## Anti-virus software

- Purchase and install anti-virus software.
- Since anti-virus software needs Internet access to download the most current virus profiles, ensure that the computer has regular access to the internet.
- It may be most convenient to set the update times for after business hours.
- Make sure to leave the computer on when the software is set to update.
- Make sure updates occur at least once a week.

## Macros

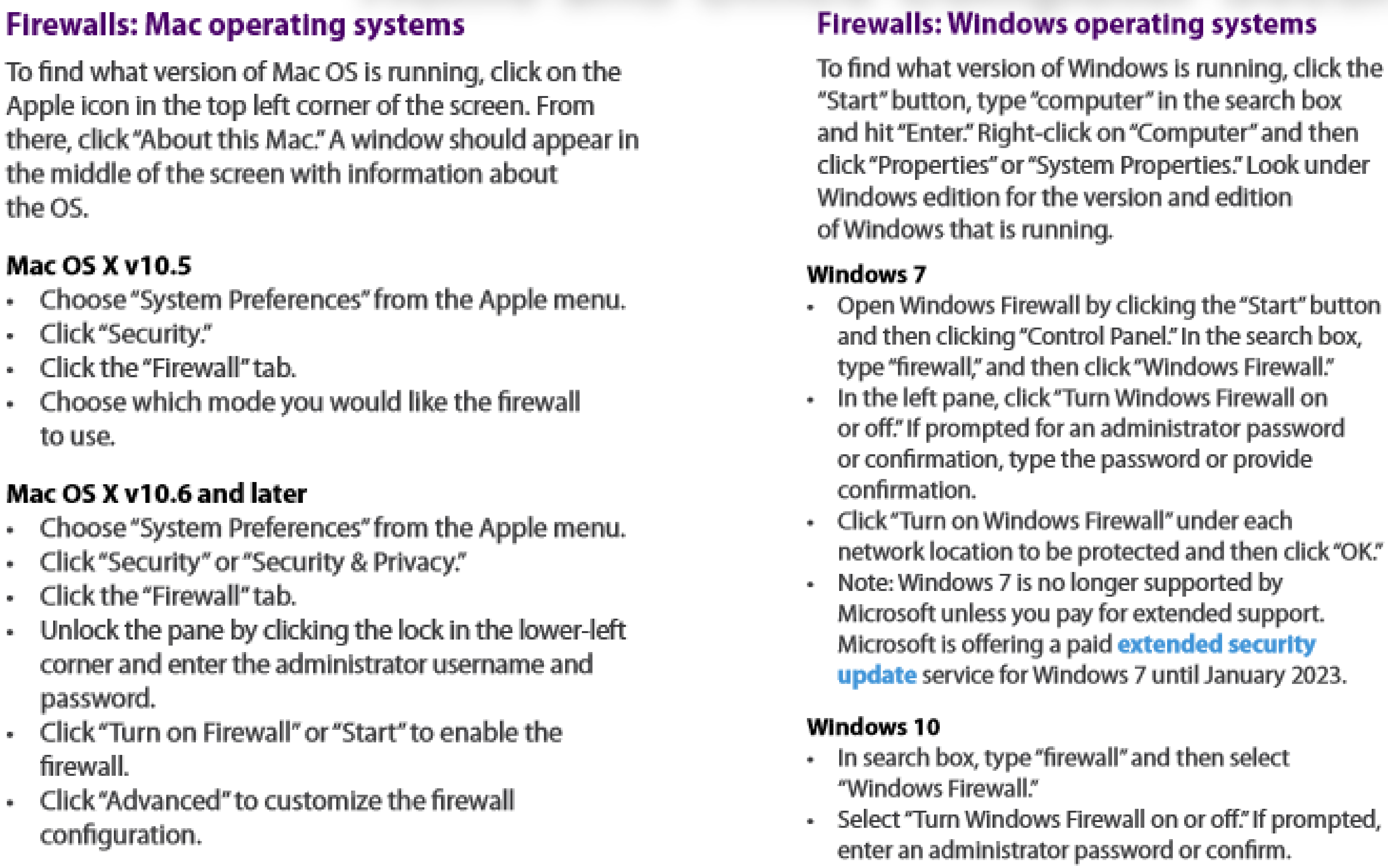
Microsoft Office applications use macros to automate routine tasks. However, macros can contain malicious code that can be used to exploit vulnerable systems. As a precaution and unless otherwise needed, make sure macros are disabled in Office.

The process to disable macros is different depending on the version of Office, however, it is typically found under the "Options" setting in the "File" menu. Also note that macros may need to be disabled for each program in Office—including Word and Excel.

## Additional computer software

Many office computers run additional software that supports everyday work. While one may not directly notice this software running on the computer, it is very important that these applications are updated and running the most current versions (e.g., Adobe Reader and Adobe Flash).

# Home and Office Computer Security



## Firewalls: Mac operating systems

To find what version of Mac OS is running, click on the Apple icon in the top left corner of the screen. From there, click "About this Mac." A window should appear in the middle of the screen with information about the OS.

**Mac OS X v10.5**

- Choose "System Preferences" from the Apple menu.
- Click "Security."
- Click the "Firewall" tab.
- Choose which mode you would like the firewall to use.

**Mac OS X v10.6 and later**

- Choose "System Preferences" from the Apple menu.
- Click "Security" or "Security & Privacy."
- Click the "Firewall" tab.
- Unlock the pane by clicking the lock in the lower-left corner and enter the administrator username and password.
- Click "Turn on Firewall" or "Start" to enable the firewall.
- Click "Advanced" to customize the firewall configuration.

## Firewalls: Windows operating systems

To find what version of Windows is running, click the "Start" button, type "computer" in the search box and hit "Enter." Right-click on "Computer" and then click "Properties" or "System Properties." Look under Windows edition for the version and edition of Windows that is running.

**Windows 7**

- Open Windows Firewall by clicking the "Start" button and then clicking "Control Panel." In the search box, type "firewall," and then click "Windows Firewall."
- In the left pane, click "Turn Windows Firewall on or off." If prompted for an administrator password or confirmation, type the password or provide confirmation.
- Click "Turn on Windows Firewall" under each network location to be protected and then click "OK."
- Note: Windows 7 is no longer supported by Microsoft unless you pay for extended support. Microsoft is offering a paid **extended security update** service for Windows 7 until January 2023.

**Windows 10**

- In search box, type "firewall" and then select "Windows Firewall."
- Select "Turn Windows Firewall on or off." If prompted, enter an administrator password or confirm.

# Home Network - Router  Security

## Turn On Automatic Updates

Look in the device’s settings. You can do that by opening a web browser and typing in the device's IP address. Very often, the address is 192.168.0.1 or 192.168.1.1

## Turn Off Features You Don't Use

Remote Administration (also known as Remote Management or web access from WAN),

Disable Universal Plug-and-Play, UPnP, which many home routers have enabled by default.

## Use Strong Passwords

The ***settings and connection passwords*** can both be changed via the router’s mobile app or the settings page (aka 192.168.1.1)

Make sure the passwords you create are strong and unique—that is, different from one another and from any other password you use.

## Change the Default SSID

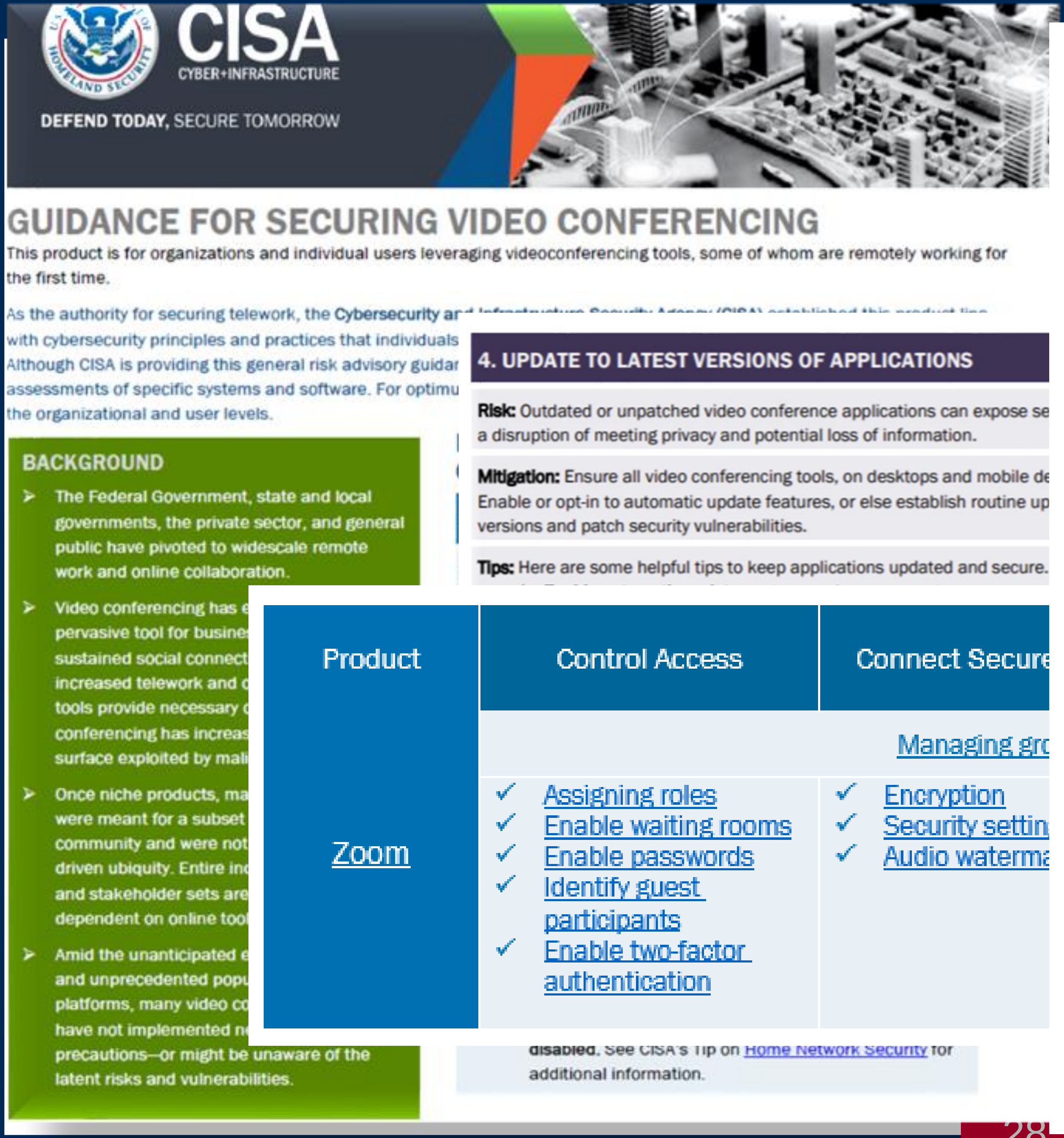
Change the default name of your WiFi network, also known as the SSID  - No need to tell the hackers the make and model of your router!

Better - Do not to broadcast the SSID at all. Once you do that, any device that's never been connected to your WiFi won’t be able to “see” your network.
Must manually input “new” network name

## Use WPA3

The latest standard, known as WPA3, encrypts your WiFi connection, making it harder for cyber criminals to guess.

If your router and other devices don’t support WPA3, you can use the previous standard called WPA2-AES.



CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY, SECURE TOMORROW

# GUIDANCE FOR SECURING VIDEO CONFERENCING

This product is for organizations and individual users leveraging videoconferencing tools, some of whom are remotely working for the first time.

As the authority for securing telework, the **Cybersecurity ar**
with cybersecurity principles and practices that individuals
Although CISA is providing this general risk advisory guidar
assessments of specific systems and software. For optimu
the organizational and user levels.

## BACKGROUND

- The Federal Government, state and local governments, the private sector, and general public have pivoted to widescale remote work and online collaboration.
- Video conferencing has e
pervasive tool for busine
sustained social connect
increased telework and c
tools provide necessary c
conferencing has increas
surface exploited by mali
- Once niche products, ma
were meant for a subset
community and were not
driven ubiquity. Entire inc
and stakeholder sets are
dependent on online tool
- Amid the unanticipated e
and unprecedented popu
platforms, many video co
have not implemented ne
precautions—or might be unaware of the latent risks and vulnerabilities.

## 4. UPDATE TO LATEST VERSIONS OF APPLICATIONS

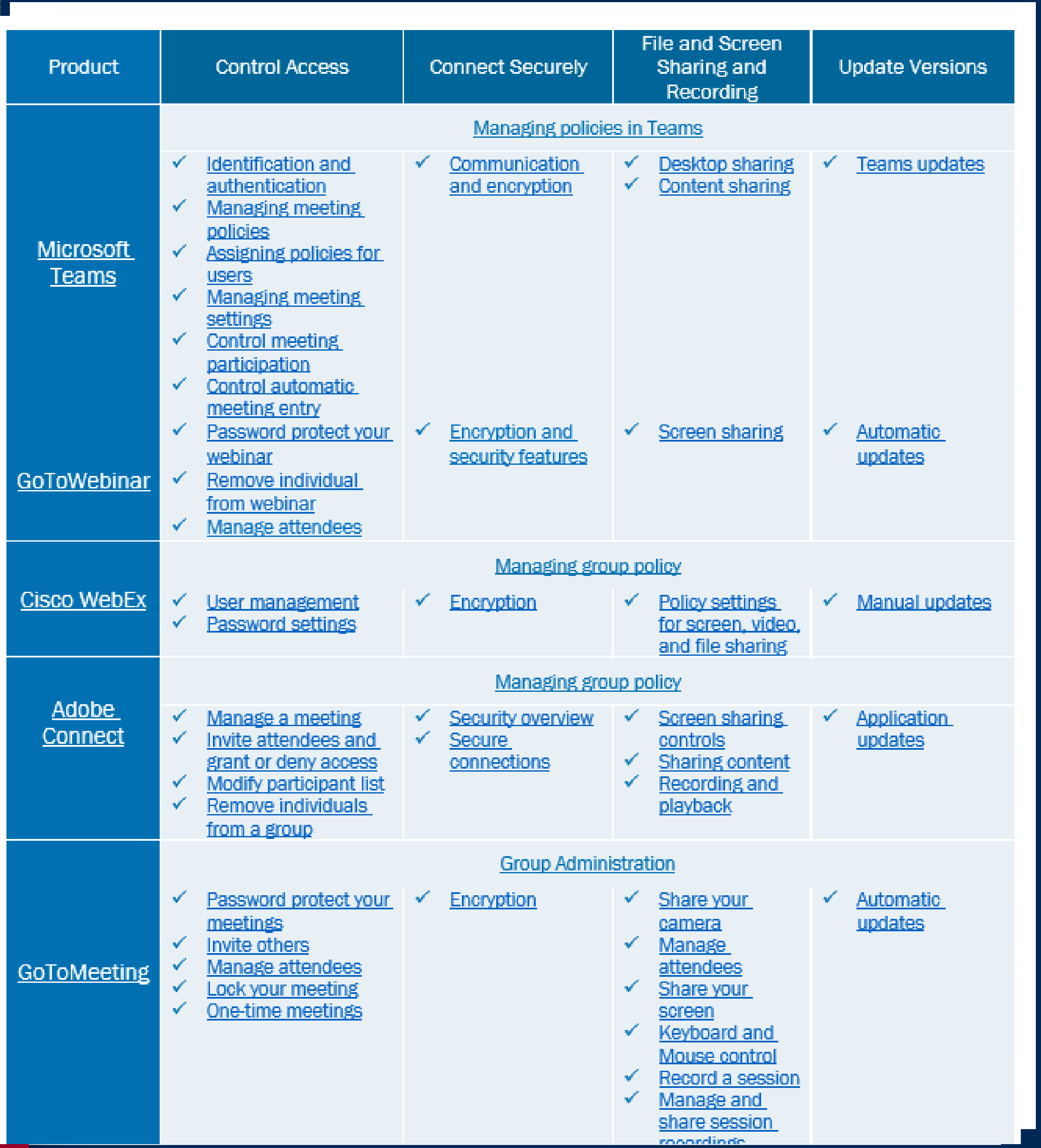
**Risk:** Outdated or unpatched video conference applications can expose se
a disruption of meeting privacy and potential loss of information.

**Mitigation:** Ensure all video conferencing tools, on desktops and mobile de
Enable or opt-in to automatic update features, or else establish routine up
versions and patch security vulnerabilities.

**Tips:** Here are some helpful tips to keep applications updated and secure.

disabled. See CISA's Tip on Home Network Security for additional information.

| Product | Control Access | Connect Secure |
|---|---|---|
| Zoom | Managing gro | |
| | ✓ Assigning roles<br>✓ Enable waiting rooms<br>✓ Enable passwords<br>✓ Identify guest participants<br>✓ Enable two-factor authentication | ✓ Encryption<br>✓ Security settin<br>✓ Audio waterma |



| Product | Control Access | Connect Securely | File and Screen Sharing and Recording | Update Versions |
|---|---|---|---|---|
| Microsoft Teams | Managing policies in Teams | | | |
| | ✓ Identification and authentication<br>✓ Managing meeting policies<br>✓ Assigning policies for users<br>✓ Managing meeting settings<br>✓ Control meeting participation<br>✓ Control automatic meeting entry | ✓ Communication and encryption | ✓ Desktop sharing<br>✓ Content sharing | ✓ Teams updates |
| GoToWebinar | ✓ Password protect your webinar<br>✓ Remove individual from webinar<br>✓ Manage attendees | ✓ Encryption and security features | ✓ Screen sharing | ✓ Automatic updates |
| Cisco WebEx | Managing group policy | | | |
| | ✓ User management<br>✓ Password settings | ✓ Encryption | ✓ Policy settings for screen, video, and file sharing | ✓ Manual updates |
| Adobe Connect | Managing group policy | | | |
| | ✓ Manage a meeting<br>✓ Invite attendees and grant or deny access<br>✓ Modify participant list<br>✓ Remove individuals from a group | ✓ Security overview<br>✓ Secure connections | ✓ Screen sharing controls<br>✓ Sharing content<br>✓ Recording and playback | ✓ Application updates |
| GoToMeeting | Group Administration | | | |
| | ✓ Password protect your meetings<br>✓ Invite others<br>✓ Manage attendees<br>✓ Lock your meeting<br>✓ One-time meetings | ✓ Encryption | ✓ Share your camera<br>✓ Manage attendees<br>✓ Share your screen<br>✓ Keyboard and Mouse control<br>✓ Record a session<br>✓ Manage and share session recordings | ✓ Automatic updates |