

Welcome to our SAN & WCET Webcast

May 11, 2022

The webcast will begin shortly.

There is no audio being broadcast at this time.

*An archive of this webcast will be available on
the SAN website next week.*





Cybersecurity Webinar Series

Part 1:

CISA Overview Briefing on the Cybersecurity Threat on Postsecondary Institutions

May 11, 2022

Welcome!

Use the Q&A box for questions.

Recording, Slide Deck, and Resources will be available next week on the SAN website.



Cheryl Dowd
Senior Director, Policy Innovations
State Authorization Network (SAN)
cdowd@wiche.edu

Who we are

The State Authorization Network (SAN) empowers members to successfully resolve regulatory challenges to improve student protections in digital learning across state lines.

We provide expert analysis, resources and training to prepare for emerging issues, collaborate on compliance strategies, develop solutions and evaluate their efficacy.

Our members are digital learning and compliance professionals representing 800+ institutions and organizations nationally and across all sectors.

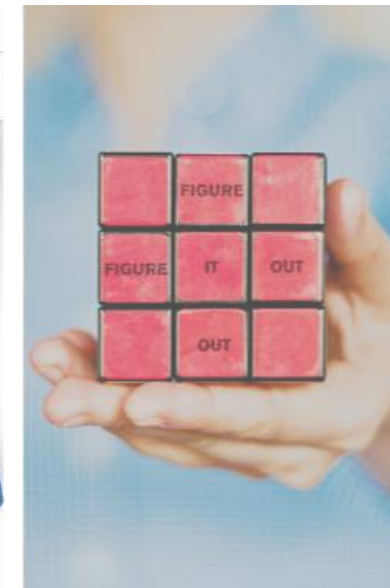


@wcet_info

#wcetSAN



wcetsan.wiche.edu



Questions from the Audience

Please use the Q & A box for questions and comments as we move through today's event.



Moderator



Kathryn Kerensky

Director,
Digital Learning Policy & Compliance

State Authorization Network (SAN)

kkerensky@wiche.edu

Agenda

01

Overview

02

Cybersecurity
Advisor Program

03

Cyber Threats

04

How They Do It

05

Questions



Presenter



David Sonheim
Chief of Cybersecurity
Region VIII; CISA
Department of Homeland Security



CYBERSECURITY THREAT LANDSCAPE: SECURING HIGHER EDUCATION

David Sonheim
Chief of Cybersecurity, Region 8
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

DEFEND TODAY → SECURE TOMORROW



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Homeland Security

We are the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Cybersecurity and Infrastructure Security Agency (CISA)



Mission

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.



Vision

A secure and resilient critical infrastructure for the American people.



OVERALL GOALS

GOAL 1

DEFEND TODAY

**Defend against urgent
threats and hazards**

seconds | days | weeks

GOAL 2

SECURE TOMORROW

**Strengthen critical
infrastructure and
address long-term risks**

months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future



PARTNERSHIP
DEVELOPMENT



INFORMATION AND
DATA SHARING



CAPACITY BUILDING



INCIDENT
MANAGEMENT
& RESPONSE



RISK ASSESSMENT
AND ANALYSIS



NETWORK DEFENSE












EMERGENCY
COMMUNICATIONS

16 Critical Infrastructure Sectors

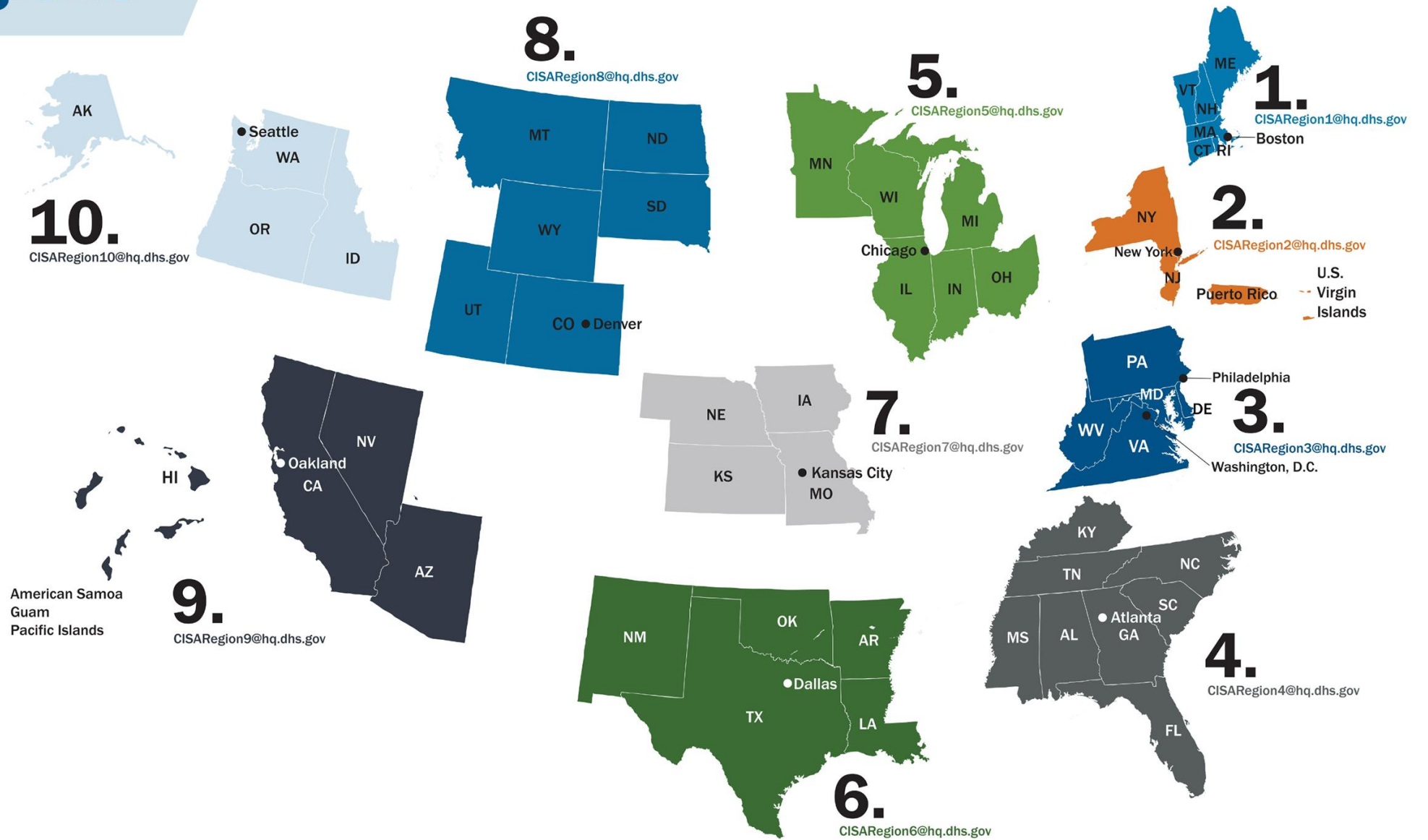
These 16 sectors underpin the essential services of our Nation's economy, security, and health. CISA serves as the lead agency for 8 of the sectors.



 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Irving, TX
- 7 Kansas City, MO
- 8 Lakewood, CO
- 9 Oakland, CA
- 10 Seattle, WA
- CS Pensacola, FL



CISA Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess:** Evaluate critical infrastructure cyber risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder requirements.
- **Coordinate:** Bring together incident support and lessons learned.



CYBER THREATS



Today's Risk Landscape

America remains at risk
from a variety of threats:



ACTS OF TERRORISM



CYBER ATTACKS



EXTREME WEATHER



PANDEMICS



ACCIDENTS
OR TECHNICAL
FAILURES

Cyber Threats of Today

Ransomware

- WannaCry
- REvil/Sodinokibi (targeting MSPs)
- Ryuk (targeting medical, education, SLTT)
- Conti, Robinhood, Maze, Fobos, CovidLock, CryptoLocker, Pysa, VoidCrypt...

Malware

- Remote Access Trojans or RATs: **Trickbot**, Emotet, LokiBot, IcedID, BazarLoader
- Wiperware NotPetya
- ICS/OT specific: Triton/hatman malware targets Safety Instrumented Systems (SIS)

Advanced Persistent Threats (APTs)

- Energetic Bear/Berserk Bear (targets U.S. state, local, territorial, and tribal (SLTT) government networks, as well as aviation networks)

Threats to External Dependencies

- 3rd party vendors, service providers, infrastructure providers
- Supply chain Compromise



TLP: AMBER





Current Cybersecurity Threats

Cyber Criminal Groups (RaaS)

- **Capability:**
 - Extremely High
 - Attack at Scale
- **Motivation:**
 - Financial Gain
 - Notoriety
- **Intent:**
 - Business or delivery of critical service Interruption

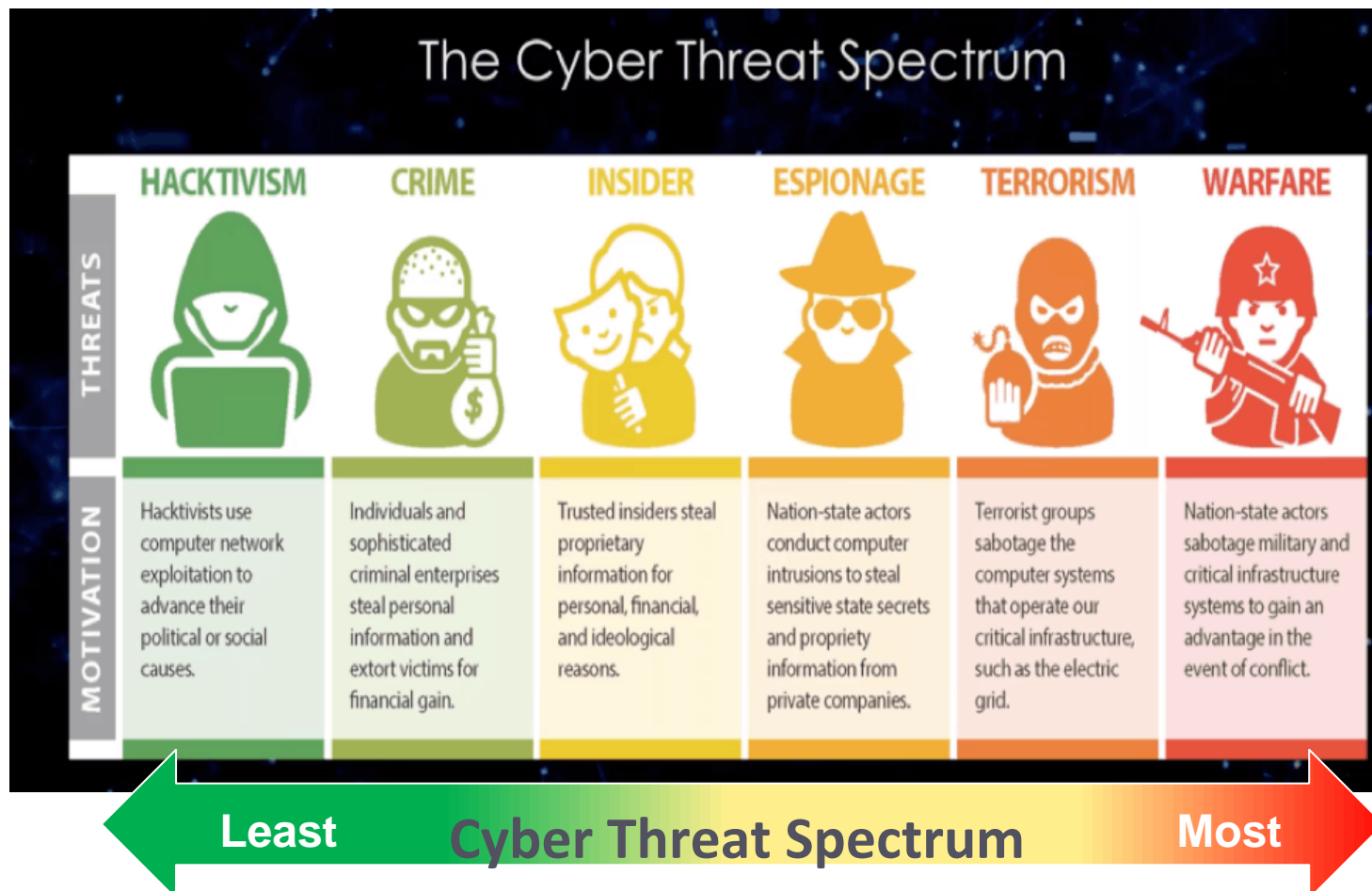


Threat =

Capability + Motivation + Intent

Advanced Persistent Threats

- **Capability:**
 - Top Tier, Multi-Stage, Deliberate
- **Motivation:**
 - Espionage & Influence Ops
 - Gov't & Think Tanks
- **Intent:**
 - Maintain presence until N. State Goals are achieved.



TLP: AMBER



Attacker Profiles

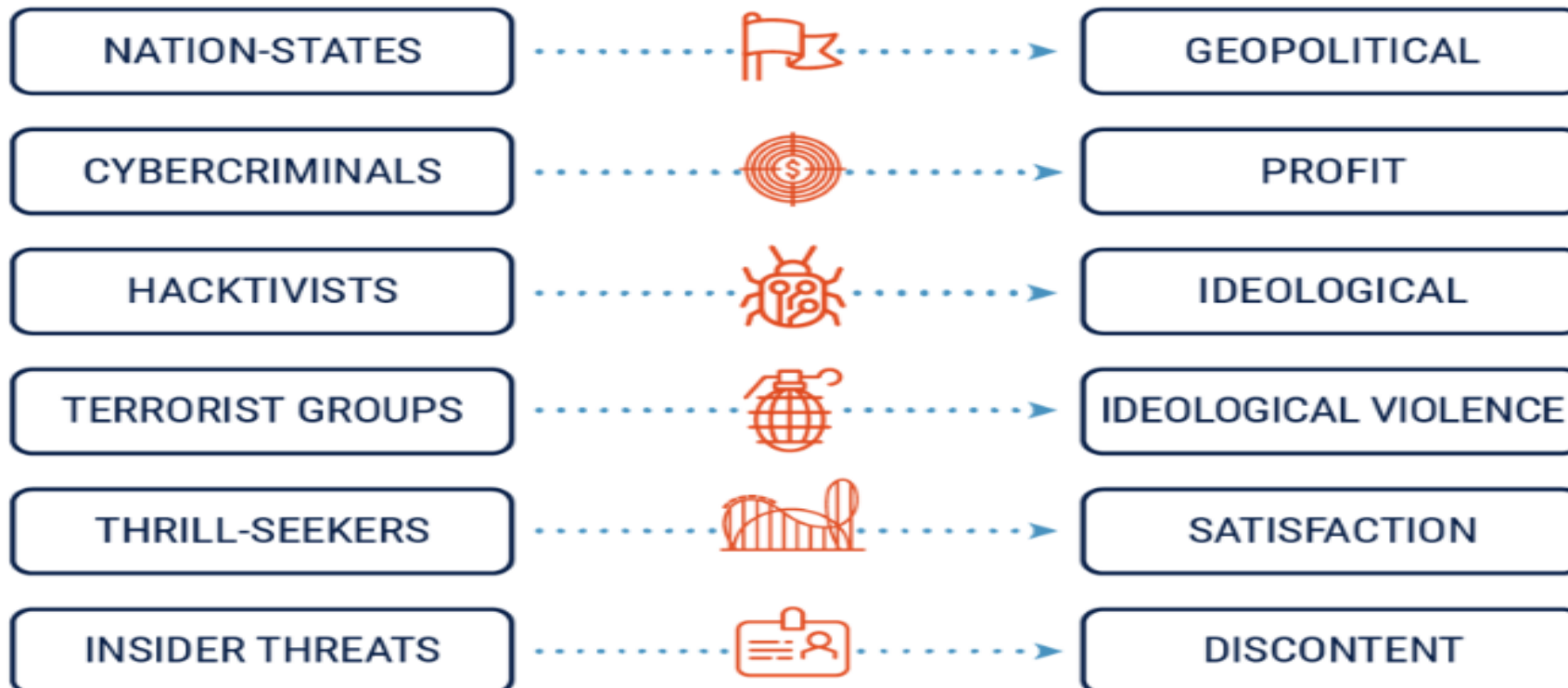
MOTIVATIONS

Cyber threat actors can be categorized by their motivations and, to a degree, by their sophistication. Threat actors value access to devices, processing power, computing resources, and information for different reasons. In general, each type of cyber threat actor has a primary motivation.

Figure 1: Cyber threat actors

CYBER THREAT ACTOR

MOTIVATION



The Threat to Critical Infrastructure



Beyond the Headlines: What is Ransomware?

Ransomware 101

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

Malicious actors typically steal the data first, then demand ransom in exchange for decryption. Then threaten to publicly release, added pressure.



BUSINESS

CNA website back up two weeks after insurance giant hit with 'sophisticated ransomware attack'

By ROBERT CHANNICK
CHICAGO TRIBUNE | APR 05, 2021 AT 11:18 AM

Newsweek

TECH & SCIENCE

RANSOMWARE WREAKING HAVOC IN AMERICAN AND CANADIAN HOSPITALS

SECURITY

Ransomware Poses Tremendous Threat to Police Departments

The growing threat of cybercrimes

Forbes / Security / #CyberSecurity

As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up \$17,000 In Bitcoin

NBC NEWS

STATE

2020 was a great year for ransomware, Palo Alto Networks says

Ransomware suspected in cyberattack that crippled major US newspapers

Source inside Tribune Publishing says printing outage caused by Ryuk ransomware infection.

Hackers Blackmail U.S.

Ransomware Statistics, Data, Trends and Facts - 2021

- Ransomware attacks against universities increased by 100% between 2019 and 2020. ([BlueVoyant](#), 2021)
- Since 2020, 1,681 higher education facilities have been affected by 84 ransomware attacks. ([Emsisoft](#), 2021)
- 66% of universities lack basic email security configurations. ([BlueVoyant](#), 2021)
- 38% of analyzed universities in the Cybersecurity in Higher Education Report had unsecured or open database ports. ([BlueVoyant](#), 2021)
- Cyberattacks against K-12 schools rose 18% in 2020. ([K-12 Cybersecurity](#), 2020)
- A school district in Massachusetts paid \$10,000 in Bitcoin after a ransomware attack in April 2018. ([Cyberscoop](#), 2018)
- On average, it costs education institutions \$2.73 million to remediate the impact of a ransomware attack, including the cost of downtime, data recovery, ransom payments, security repairs and network repairs. ([Edscoop](#), 2021)

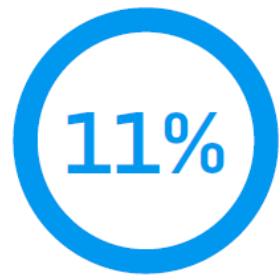


Impact of Ransomware Attacks



(credit: CBS)

- University of California – Paid \$1.14 million ransom in cryptocurrency
(<https://er.educause.edu/articles/2021/6/the-increasing-threat-of-ransomware-in-higher-education>)
- University of Colorado - Did not pay ransom, impacted for several weeks, restored from backup.
- Regis University – Down during critical start to the school year, multiple systems including phones and email. Paid ransom, declined to disclose amount of payment.
- On average education organizations recovered 68% of their data after paying ransom
(<https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf>)



Got ALL their data back



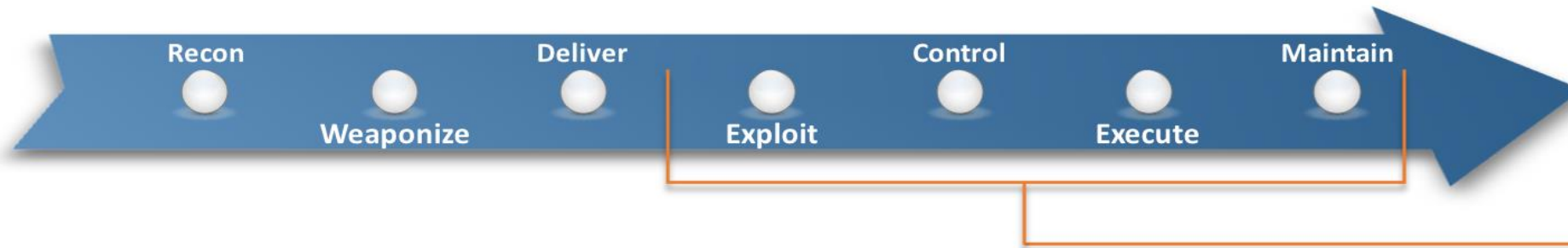
Got half or less of their data back



HOW THEY DO IT



Initial Foothold..Infect..Exploit..Escalate..Exfill



Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

MITRE

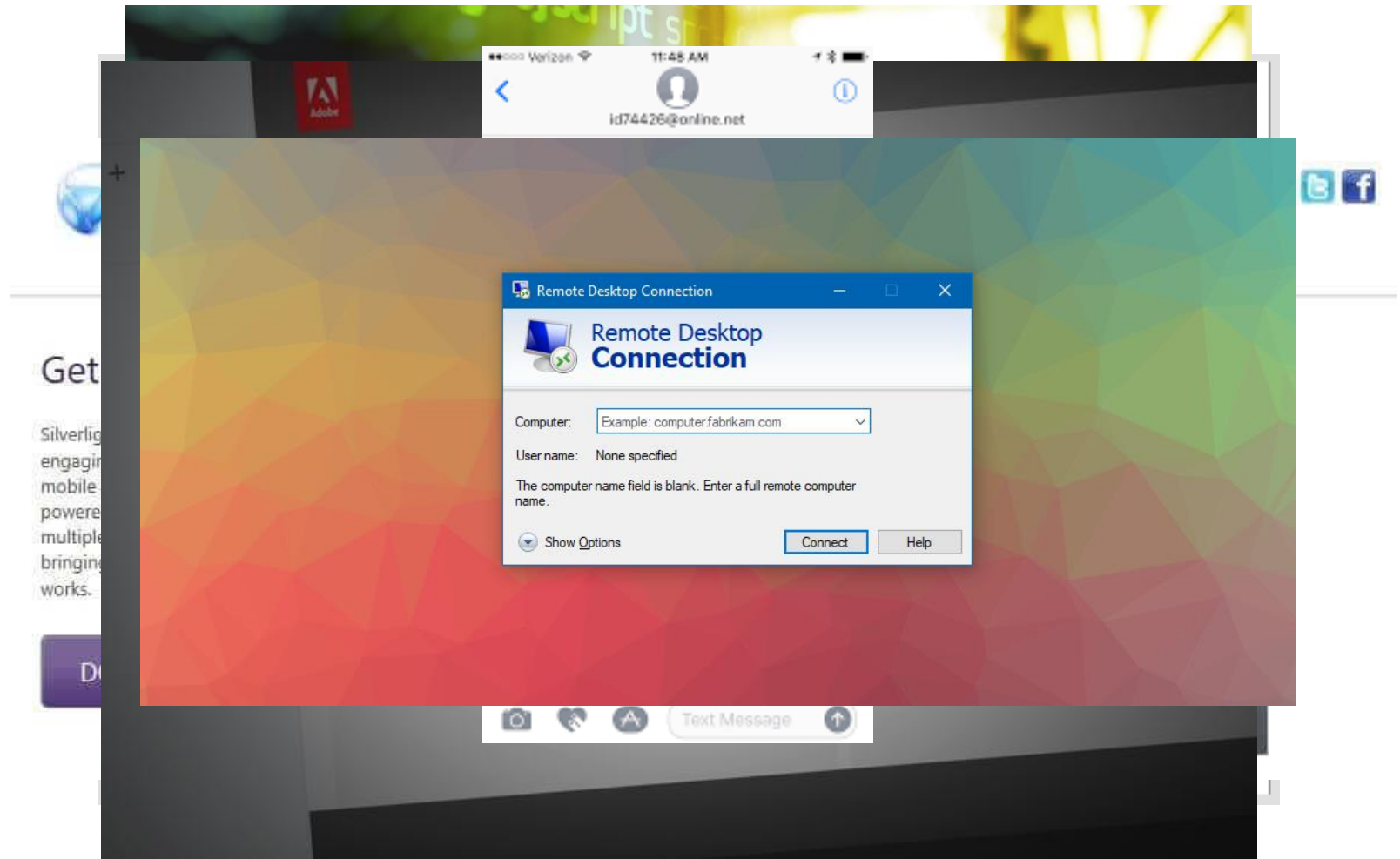
- Ransomware incidents can severely impact business processes and leave organizations without essential data they need to operate and deliver mission-critical services.
- Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.



Methods of Infection

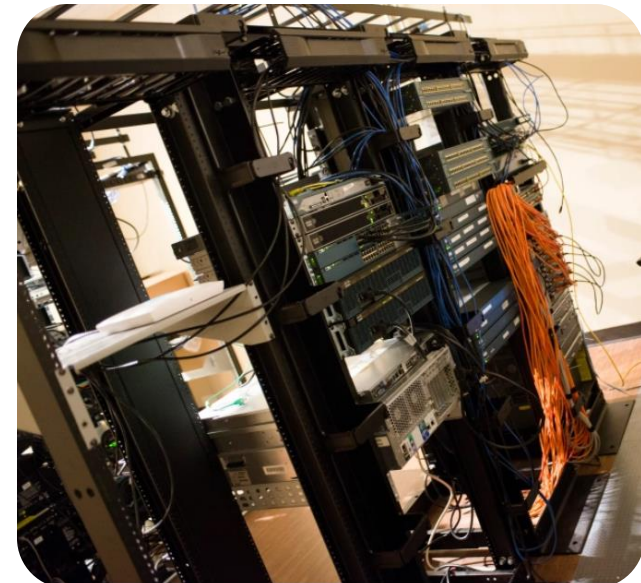
The following can all be vectors of infection for ransomware attacks:

- Phishing
- Compromised Websites
- Malvertising
- Exploit Kits
- Downloads
- Messaging Applications
- Brute Force via Remote Desktop



Challenges in Higher Education

- Sheer volume of digital assets that are collected, produced, shared, and managed. Assets have significant intellectual / research value
- Global student population / non-US Students. No control over devices brought to campus by students, faculty, and staff. (smartphones, electronic or video doorbells in dorm rooms, electronic lights). Leveraged for DDoS.
- Increasingly more difficult to hire, train and retain security professionals
- Research as core mission: many higher education institutions are researched based, providing an open environment. When we welcome everyone, the likelihood of malicious intent increases.



CISA's Cyber Hygiene Data and Population Sample

Vulnerability Scanning (VS)

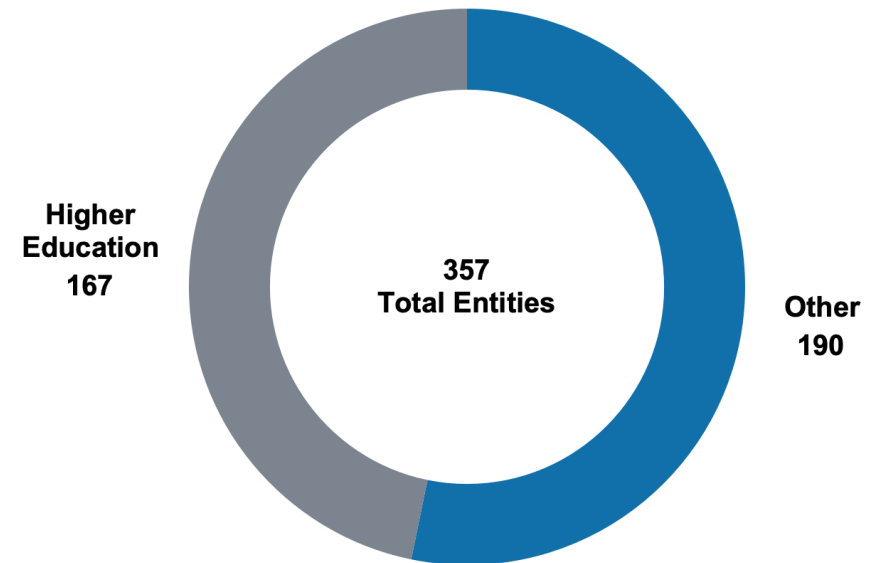
- 357 Education entities enrolled prior to FY21 and were scanned throughout FY21.
- VS provides information on internet-accessible vulnerabilities among scanned entities that can be exploited by threat actors.
- By the end of FY21, 543 Education entities enrolled in CyHy VS, a 52% increase during FY21.

Web Application Scanning (WAS)

- 18 entities and 114 web applications scanned.
- WAS provides information on design flaws or misconfigurations among scanned entities that can be exploited by threat actors.

CISA Assessments

- 5 Risk and Vulnerability Assessments (RVAs).
- Simulate scenarios that emulate threat actors' tactics and techniques using the MITRE Enterprise ATT&CK framework.



Education Entities represented in FY21 VS sample

FY21 Key Findings for Education Entities

Exposure to Known Exploited Vulnerabilities (KEVs)



Instances of 42 KEVs were active on 244 Education entity networks during FY21, likely indicating that some agencies were exposed to threat actors that leverage KEVs to compromise networks.

Unsupported Operating Systems (OS)



33 entities likely eliminated use of unsupported and vulnerable Windows OSs (Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008), by the end of FY21.

Vulnerability Reduction



By the end of FY21, **active vulnerabilities per entity decreased by 16.7%**, suggesting that entities remediated outstanding internet-accessible vulnerabilities, likely reducing their attack surface and risk.

Exposed Risky Services



47.0% of scanned Education entities exposed risky services, e.g., Remote Desktop Protocol (RDP), on internet-accessible hosts that can provide threat actors avenues for initial access, command and control (C2), and data exfiltration.



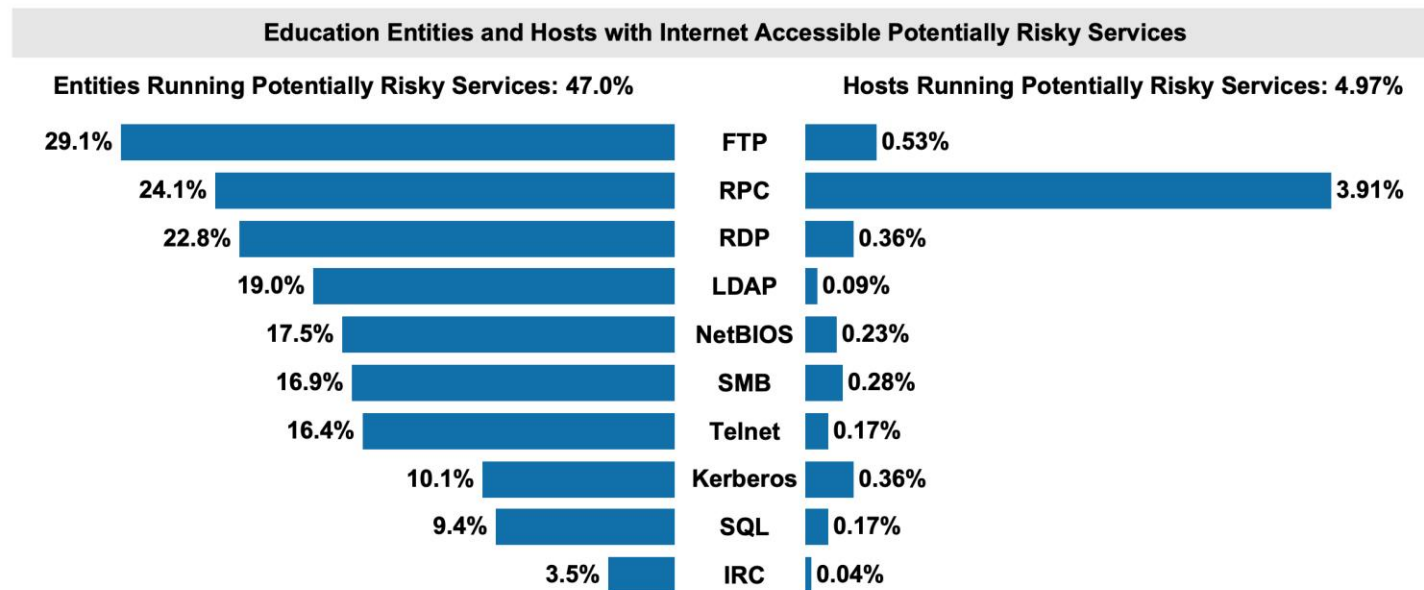
TLP: AMBER

David Sonheim
May 12, 2022

Exposed Risky Services

47.0% of scanned entities used a potentially risky service that can increase exposure and risk of compromise.

- **29.1%** of scanned entities used File Transfer Protocol (FTP), which leverages cleartext communications susceptible to password sniffing and eavesdropping attacks.
- **24.1%** of scanned entities used Remote Procedure Call (RPC), which allows an application to execute procedures and interact with services on a network, exposing critical server component to exploit and damage.
- **22.8%** of scanned entities used Remote Desktop Protocol (RDP), which is known to be a prime vector for Ransomware infections, gaining initial access, providing avenues for command and control, and data exfiltration, according to government and industry reporting.



*Population actively scanned in FY21 includes 543 entities and 447,674 hosts.

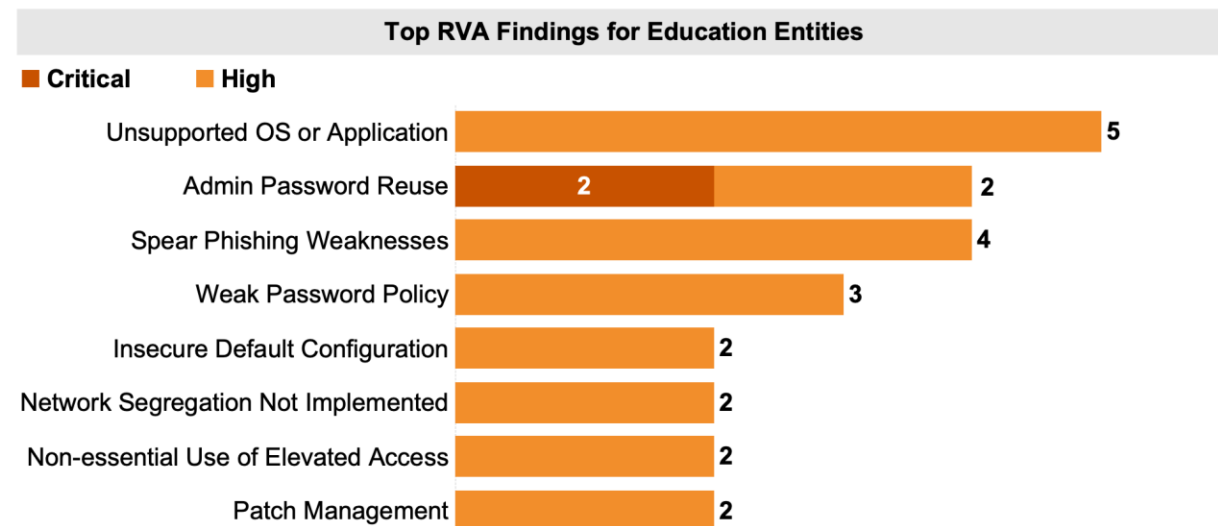
TLP: AMBER

David Sonheim
May 12, 2022

Phishing and Password Weaknesses

CISA conducted assessments for 5 Education entities during FY21 and frequently observed unsupported OS or applications, and admin password reuse weaknesses within internet-accessible and internal systems and hosts.

- High severity unsupported OS or application weaknesses were frequently observed, likely indicating that some Education entities are operating with unsupported systems that do not have patches for newer vulnerabilities, increasing risk of compromise. This finding is also supported by earlier analysis of Windows OS.
- Critical and high severity admin password re-use weaknesses suggest that Education entities likely re-use the same administrative password on multiple systems that likely increase ease and risk of compromise if threat actors compromise one or more shared passwords.



TLP: AMBER

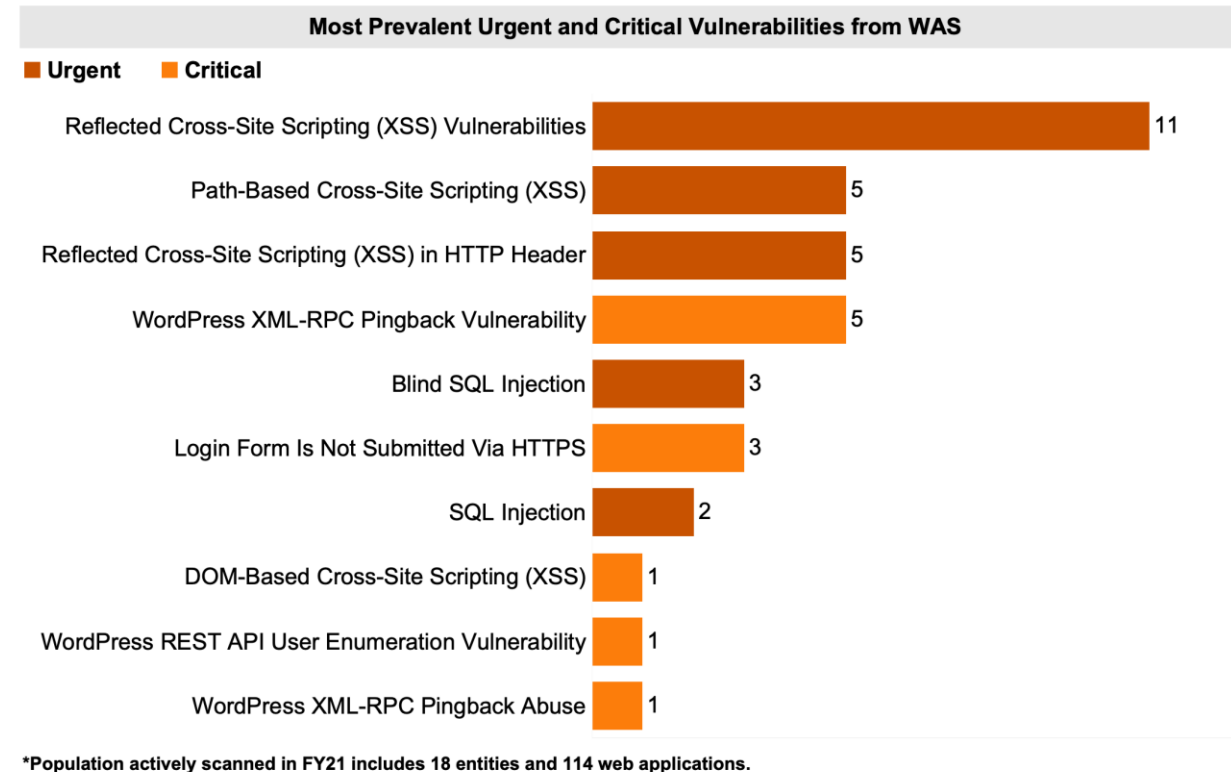
David Sonheim
May 12, 2022

Web Application Vulnerabilities

WAS probes publicly accessible web-based assets and provides insight into how systems and infrastructure appear to potential attackers to help reduce risk of compromise.

- The top three most frequently observed WAS weaknesses were due to Cross-Site Scripting (XSS), which likely enable an attacker to inject malicious code into web pages to perform follow-on actions, such as stealing credentials or sensitive information from end users. It is likely that XSS can have varied impacts that include hijacking users' sessions, installing malware, and even modifying content on Education entity websites, which increase the risk of compromise.

Education entities with urgent and critical WAS vulnerabilities likely have increased risk of compromise.

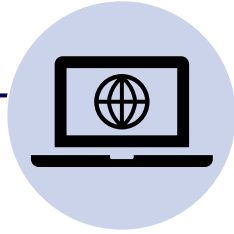


Recommendations



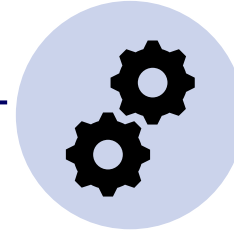
Defend Against Ransomware

- Practice network segmentation. Keep offline, encrypted backups.
- Develop, maintain and practice cyber incident response plans.
- Refrain from paying a ransom and report incidents to [CISA](#) and your [local FBI field office](#).



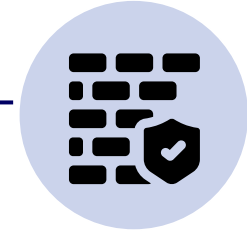
Improve Vulnerability Management

- Prioritize remediation of vulnerabilities considering likelihood of attack, ease of exploitation, and magnitude of impact.
- Modify patch management to prioritize patching KEVs and vulnerabilities with exploits available.



Secure Potentially Risky Services

- Evaluate the business need for exposing risky services on internet-accessible hosts.
- Disable or block all unnecessary services.
- If certain services are required, then operate the services with proper configurations and security features enabled, such as multifactor authentication (MFA).



Update OSs and Software

- Identify and plan to replace software, firmware, OSs, and hardware that is unsupported or scheduled to reach end-of-support.
- Maintain a thorough software asset inventory with end of support dates.
- Document exceptions and implement mitigating controls to isolate unsupported and vulnerable systems.



TLP: AMBER

David Sonheim
May 12, 2022

Why Target Education Facilities?

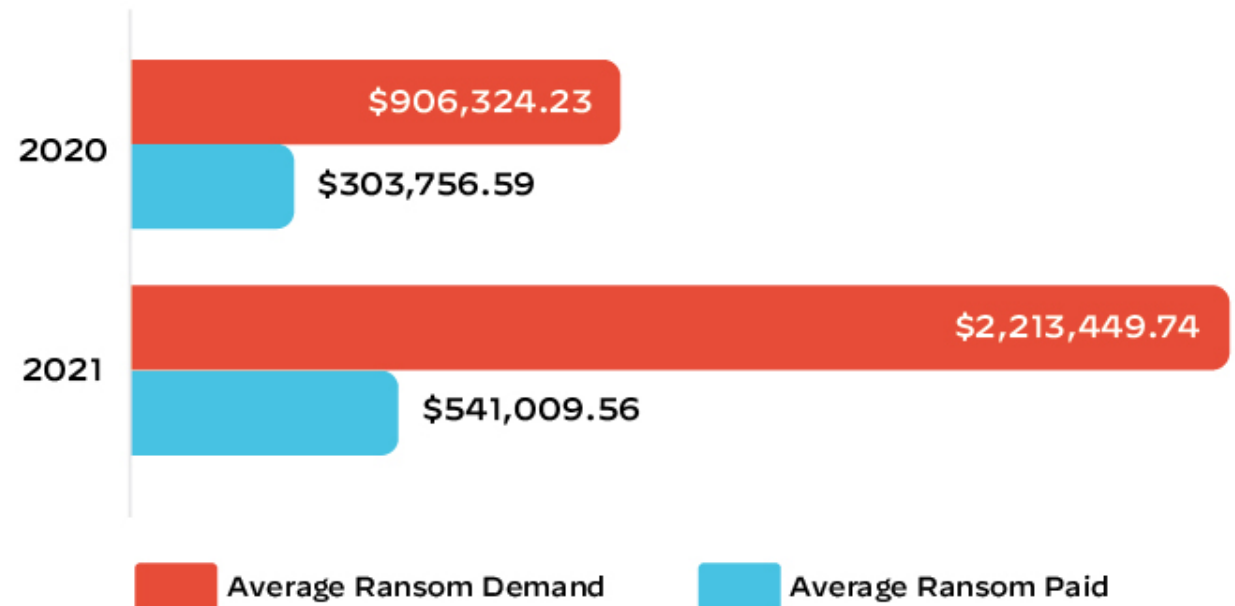
Follow the Money

“We saw ransomware attacks on businesses large and small, on cities, on schools. It’s really been a scourge”
– Jen Easterly, CISA Director

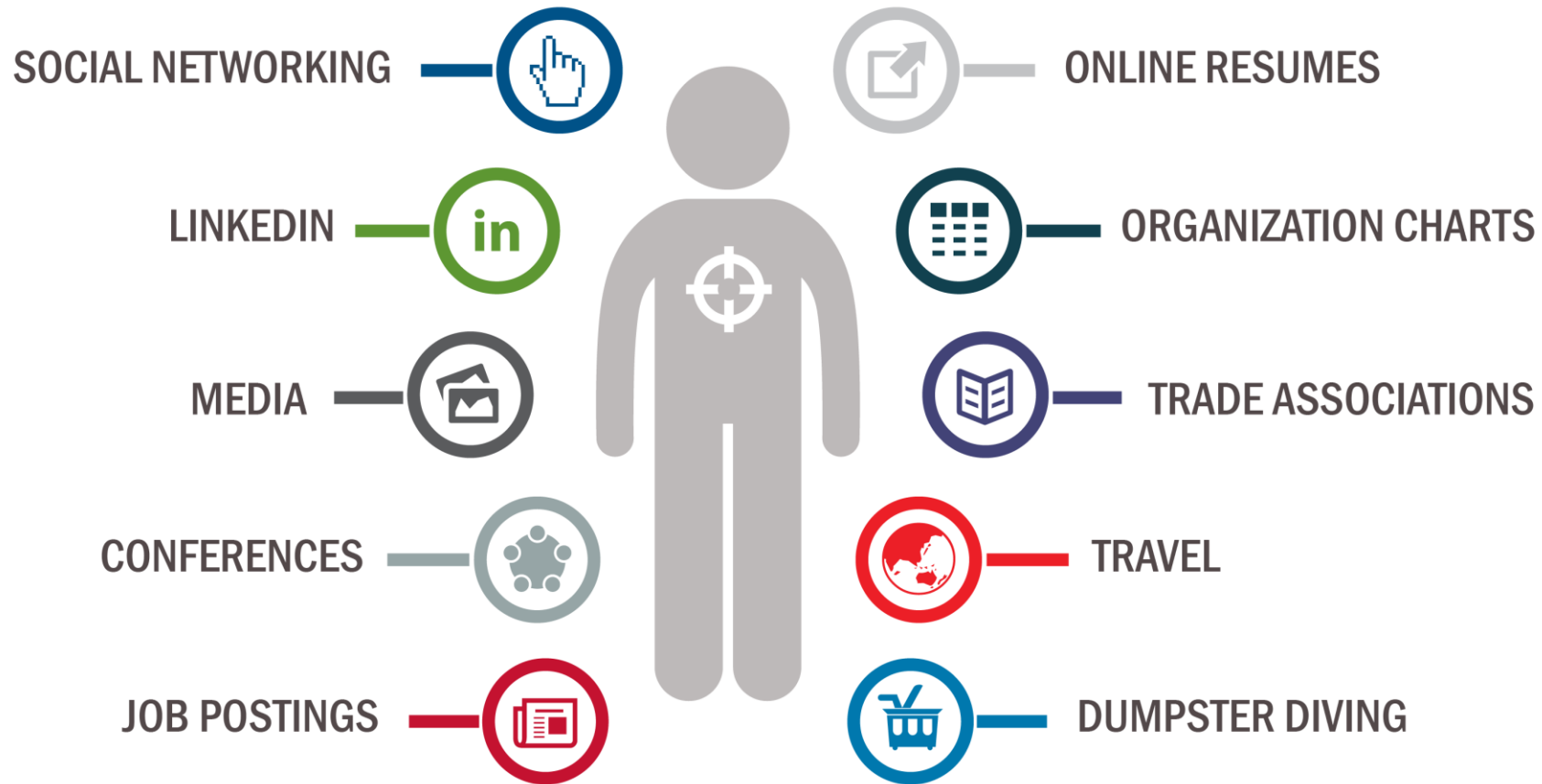
According to 2022 Unit 42 Ransomware Threat Report

The average ransom paid for organizations increased from \$900,000 in 2020 to **\$2.2 million** in 2021 → a 144% year-over-year increase.

Average ransom demands compared to average ransom payments in 2020 and 2021, according to Unit 42 incident response data



HOW ARE **YOU** TARGETED?



Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone I **ordinarily** communicate with.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- I **don't know the sender personally** and they were **not vouched for** by someone I trust.
- I **don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



TO

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.



HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?



SUBJECT

- Did I get an email with a subject line that is **irrelevant or does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?



ATTACHMENTS

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on** is a .txt file.



CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar or spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd or illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Epecially under the prevailing conditions – Always Pause and Ask:

Is this message expected?

Do I recognize the sender of this email?

Is there something odd about the email address?

Verify the email address/domain by hovering the cursor over an email address or embedded link, without clicking; the actual destination appears in a text box or bubble.

Is there a needlessly urgent call to action in the email?

Is the action sought odd or unfamiliar?

Are my network access credentials requested after clicking to open a link?

NEVER enter user name and password in these circumstances!

Be Attentive – and Protect Yourself and the Network



PHISHING EXAMPLE #1

To: <Stakeholder List>

From: Apples Customer Relations <freeapplesforyou@apple.org>

Subject: Free iPad – Just Complete a Survey!

Want the new iPad or iPad Mini? I got mine free from this site: <https://apple.com/giveaway> !!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are mitigated before the release.

If you are accept to participate in this programall we ask is that you submit a survey at the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office

Apples Campus, Cupertino, California 95114



Hover your mouse over the link text without clicking to see the actual website that you will be sent to!!



PHISHING EXAMPLE #2

To: <Stakeholder List>
From: OBRM <OBRM@organization.org>
Subject: Future Budget Plans

In the coming weeks, our state's leadership will be working to draft a plan to prevent long term financial issues and ways to avoid human resource reductions. All departments within the State Government are being directed to draft a plan to help meet projected budget shortages and find ways to reduce spending within the State Government.

We have been asked to work more efficiently with less. As a result, many budgets and programs are also facing significant reduction. The Office of Budget and Resource Management has developed a draft plan that will address any potential budget shortcomings.

To learn more about the budget and how your program maybe affected, please visit <https://www.organization.org/budget>

If you have any questions or concerns, we'd love to hear them. Please emails us here budget@organization.org

**Hover your mouse over the link text
without clicking to see the actual
website that you will be sent to!!**

Office of Budget and Resource Management



David Sonheim
May 12, 2022

Do Your Part. #BeCyberSmart.

Cybersecurity starts with
YOU and is **everyone's**
responsibility.


- National Cybersecurity Awareness Month
- STOP. THINK. CONNECT.TM (STC) Campaign
- Mandatory Initial and Continued Cybersecurity Training



There are currently an estimated
4.8 billion internet users or
62% of the world's population.

How to Protect Against Spam and Phishing

- **Be suspicious** of emails from unknown senders.
- **Do not** provide personal or corporate sensitive information requested via email.
- **Do not** use the contact information provided by the email or phone request. Contact the organization directly to verify.
- **Do not** send personal sensitive information on the internet without checking the security of the websites first.



NATIONAL CYBERSECURITY AWARENESS MONTH

DO YOUR PART. #BECYBERSMART

PHISHING

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts.

HOW CRIMINALS LURE YOU IN

The following messages from the Federal Trade Commission's OnGuardOnline are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

Phishing email, please

Criminals compromise your... not respond, and do not... as "Hello Bank... legitimacy of an email, call

any phishing emails... tion is in jeopardy. If you... person directly on a... reach out to them via

—your job title, multiple... ey can attempt a direct

PHISHING

Phishing attacks use email or malicious websites to infect your machine with malware and viruses in order to collect personal and financial information. Cybercriminals attempt to lure users to click on a link or open an attachment that infects their computers, creating vulnerability to attacks. Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts.

HOW CRIMINALS LURE YOU IN

The following messages from the Federal Trade Commission's OnGuardOnline are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."
- To see examples of actual phishing emails, and steps to take if you believe you received a phishing email, please visit "

NATIONAL CYBERSECURITY AWARENESS MONTH

How to Protect Against Ransomware

- Keep all hardware, software and operating systems up to date.
- **Always** backup your data regularly and test/run drills to restore data from backups regularly.
- Educate your family and co-workers on safe internet browsing practices.
- For organizations specifically:
 - Practice good cyber hygiene, backup and update apps, and use multifactor authentication.
 - Implement “the concept of least privilege.”
 - Educate employees on cyber awareness best practices.





How to Protect Your Company From Cyber Attacks

- Identify the most pressing targets
- Build a comprehensive, focused plan
- A good defense is the best offense
- Detect. Respond. Recover. Repeat

Observations, Mitigations, and Best Practices

Patch Management

Observation: Threat actors scan for and target vulnerable internet-accessible hosts to launch attacks. The median days to remediate vulnerabilities with known exploits for Education entities was 242.7 days for critical severity vulnerabilities and 215.3 days for high severity vulnerabilities.

Mitigation:

- Regularly scan internet-accessible hosts and remediate critical and high severity vulnerabilities within 15 and 30 days, respectively.
- Continue to reduce the backlog of vulnerabilities, especially those with known exploits that could be used to breach the defensive perimeter.
- Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of probable impact.



Observations, Mitigations, and Best Practices

Potentially Risky Services

Observation: Throughout 2020, 60 percent of Education entities scanned were running at least one potentially risky service (NetBIOS, Telnet, SMB, RDP) on an internet-accessible host.

Mitigation:

- Entities should identify all internet-accessible services and secure or disable risky services.
- Use additional security measures such as virtual private networks (VPNs), virtual network segmentation, secure credentials and MFA, host-based and network-based firewalls, Transmission Control Protocol (TCP) wrappers or port access control list (ACL) measures and prioritizing secure encryption.



How to Respond If You've Been Affected

- **Report it** immediately
 - If you're a part of an organization, be sure to report the issue to the proper Points of Contact.
- Prevent the spread of the infection by isolating the infected computers and systems.
- Try to identify the type of ransomware to help understand what you are working with.
- Work with cybersecurity professionals who are trained in resolving these issues.
- Recover your data from your backups **after** you test the backups to ensure the data on the backups is safe to restore.



Report Incidents



Report Phishing



Report Malware








Report Vulnerabilities



Share Indicators

David Sonheim
May 12, 2022

How to Stay Safe Online

- **Use** strong passwords and multi-factor authentication, if available. 
- **Keep** the software on your devices up to date. 
 - Enable automatic updates
- **Check** privacy policies and security setting to see how your information is stored and shared. 
- Shop online with **trusted and reputable** companies. 
- **Don't** download attachments or click links that you are unsure of. 



How to Stay Safe Online

- **Avoid** connecting to public Wi-Fi
 - Public Wi-Fi is typically not secure.
 - If connected, do not conduct activities involving sensitive information. Always use a VPN if you must.
- **Credit cards** > Debit cards are connected directly to your checking account balance. Bank may eventually reimburse for fraud, but it is not guaranteed.
 - Credit cards provide more protections when it comes to fraudulent activity and will almost always remove fraud charges.
- **Be wary** of emails requesting personal information
 - Organizations typically do not request this information via email.



Keeping Your Kids Safe Online

Take an active role in protecting your children

1. Be involved, be present when your kids use connected devices.
2. Supervision is very important for children of all ages.
3. Set rules and create parental controls with strong passwords that enforce the rules when not able to supervise kids closely.
4. Monitor computer and smart phone activity.
5. Children should have separate accounts on shared computers and mobile devices when possible.



Questions & Contact Info



Contact Information

David Sonheim

Region 8 Chief of Cybersecurity – (CO, WY, UT, MT, ND, SD)

David.Sonheim@cisa.dhs.gov


(720) 661-1643 (Cell)



Your Questions!



Resources for those new to the topic of state authorization



State Authorization 101

Compliance management for out-of-state activities

First time here? Try these quick links.

- [How it works >](#)
- [Why comply? >](#)
- [Resources >](#)

Scroll to learn more

[wcetsan.wiche.edu](#)

How it Works - Resources

Are you relatively new to compliance requirements for out-of-state activities? Start Here!

- [Foundational Principles for State & Federal Out-of-State Activity Compliance](#) - One page overview
- [State Authorization and Crossing State Borders, Part 1: Institutional Approvals for Out-of-State Activities](#)
- [State Authorization and Crossing State Borders, Part 2: Additional Approvals and Professional Licensure](#)
- [10 Steps You Can Take to Begin the State Authorization Process](#)
- [State Institutional Approval Quick Chart](#) - Chart to start research of state requirements.
- [Professional Licensure Disclosures - Implementation Handbook & Flowchart](#)
- [WCET & SAN Webcast: Professional Licensure Notifications Now Required!](#) See the recording, transcript, and Webcast Summary Document
- [Out-of-State Student Complaint Options White Paper & Chart](#)
- [SAN Virtual Seminar 2020 HEA & Federal Rulemaking: The Impact on Institutional Compliance](#)
- [SAN Virtual Seminar 2018](#)

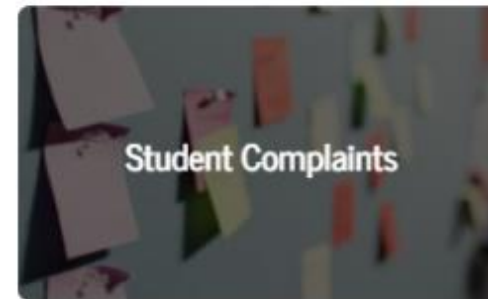
Resources by topic

- Research
- Regulation summaries
- Handbooks
- Talking points
- Sample tools
- More



wcetsan.wiche.edu

Topic Areas



Upcoming Events

Cybersecurity Webinar Series Part 2: Postsecondary Cyber Risks Associated with 3rd Parties Due to a Ransomware Incident

- *June 8, 2022. Time: 9AM Alaska, 10AM Pacific, 11AM Mountain, 12 PM Central, 1 PM Eastern*
- *Open to all SAN & WCET Members!*
- [*More information and Registration Here!*](#)

SAN Advanced Topics Workshop (Virtual) – Succession Planning for Compliance Continuity

- *September 7-9, 2022. Time: 12pm-4pm ET each day*
- [*More information can be found here!*](#)

WCET 34th Annual Meeting; Hilton Denver City Center; Denver , CO

- *October 19, 2022 – October 21, 2022 (SAN Coordinator Meeting October 18, 2022)*
- [*More information can be found here!*](#)



@wcet_info

#wcetSAN



wcetsan.wiche.edu



Thank you

to our speaker, Dave Sonheim,
and to all our attendees today!





wcetsan.wiche.edu

3035 Center Green Drive
Suite 200
Boulder, CO 80301

(303) 541-0210

Cheryl Dowd, Senior Director, Policy Innovations
(303) 541-0210 | cdowd@wiche.edu

Leigha Fletcher, Administrative Assistant
(303) 541-0211 | lfletcher@wiche.edu

Kathryn Kerensky, Director, Digital Learning Policy & Compliance
(303) 541-0290 | kkerensky@wiche.edu

Rachael Stachowiak, Director, Interstate Policy & Compliance
(303) 541-0289 | rstachowiak@wiche.edu



Note: The information and resources presented are for consideration when an institution wishes to develop a process to manage compliance. The information should not be considered legal advice. Legal questions should be directed to general counsel.