

Welcome to our SAN & WCET Webcast

June 8, 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 2:

Postsecondary Cyber Risks Associated with 3rd Parties due to Ransomware

June 8, 2022

Welcome!

Use the Chat 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

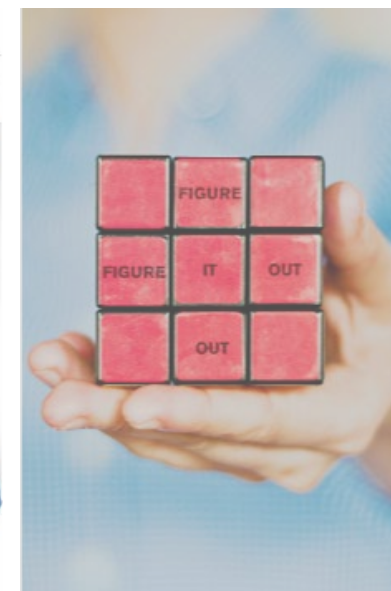
#wcetSAN



wcetsan.wiche.edu

The State Authorization Network

The leader for guidance and support for navigating state and federal regulatory compliance for out-of-state activities of postsecondary institutions.





Questions from the Audience

Please do not hesitate to use the chat 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

Today's Risk
Landscape

02

What is
Ransomware?

03

Real
Examples of
Attacks

04

Third –
Party/Vendor
Dependency
Management

05

Strategies to
Protect the
Institutions

06

Questions

Presenters



David Sonheim

Chief of Cybersecurity
Region 8 ; CISA

Department of Homeland Security



Tanya Taplin

State Cybersecurity Coordinator
(North Dakota); Region 8 CISA
Department of Homeland Security



POSTSECONDARY CYBER RISKS ASSOCIATED WITH 3RD PARTIES DUE TO RANSOMWARE

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

Tanya Taplin
State Cybersecurity Advisor, North Dakota
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

DEFEND TODAY → SECURE TOMORROW



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



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

Beyond the Headlines: What is Ransomware?

Ransomware 101

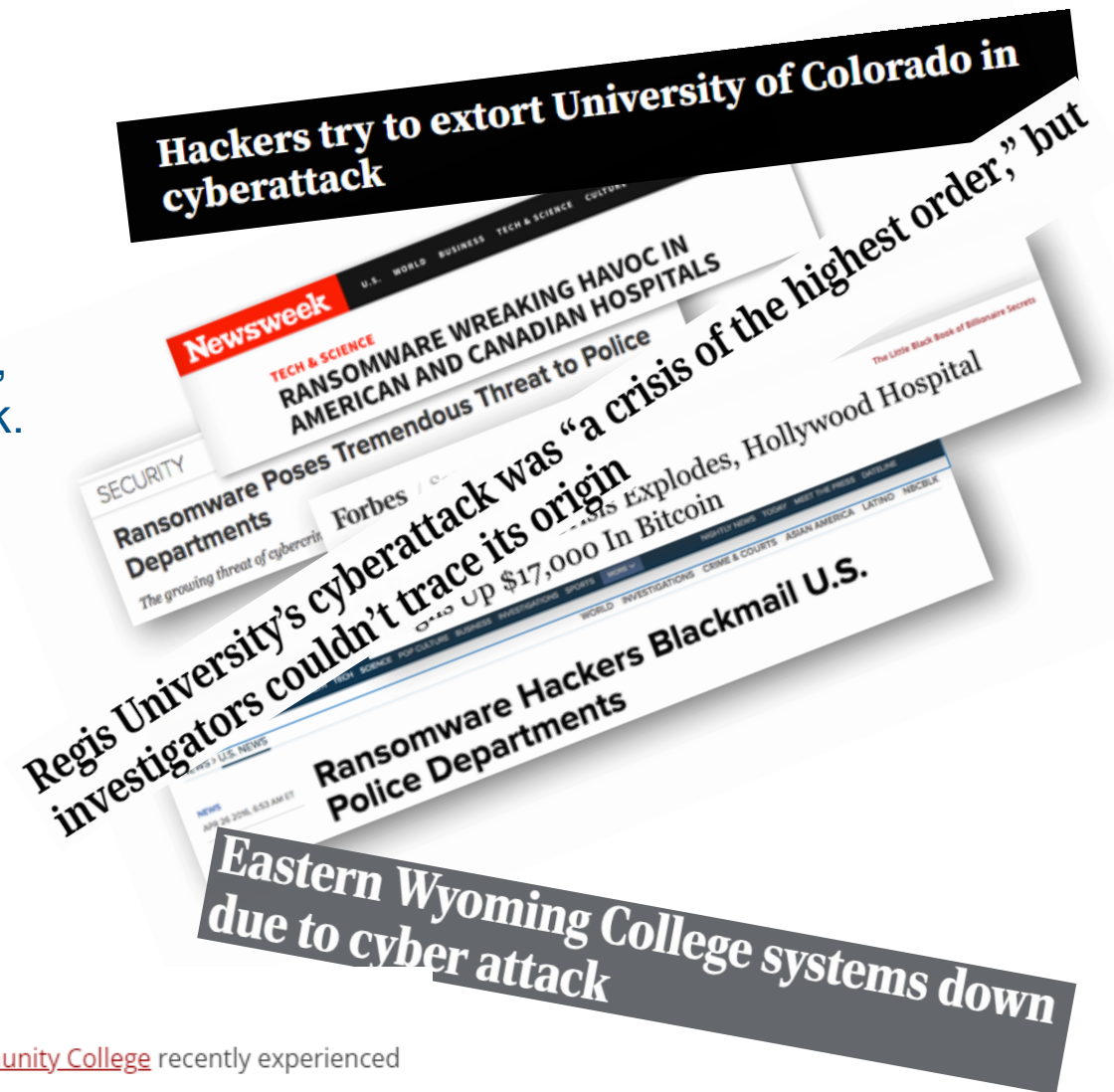
Ransomware is a type of malicious software (Malware) specifically designed to encrypt critical data, rendering systems unusable and making them inaccessible.

Cyber actors typically steal or extract the sensitive data first, then encrypt local system data or data that is on the network. Then they demand ransom payment in exchange for decryption key. Then threaten to publicly release, added pressure.



College Cyberattacks on the Rise

In addition to Regis, New York's [Monroe College](#) and Massachusetts' [Cape Cod Community College](#) recently experienced cyberattacks.



Why Target Higher Education Sector?

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

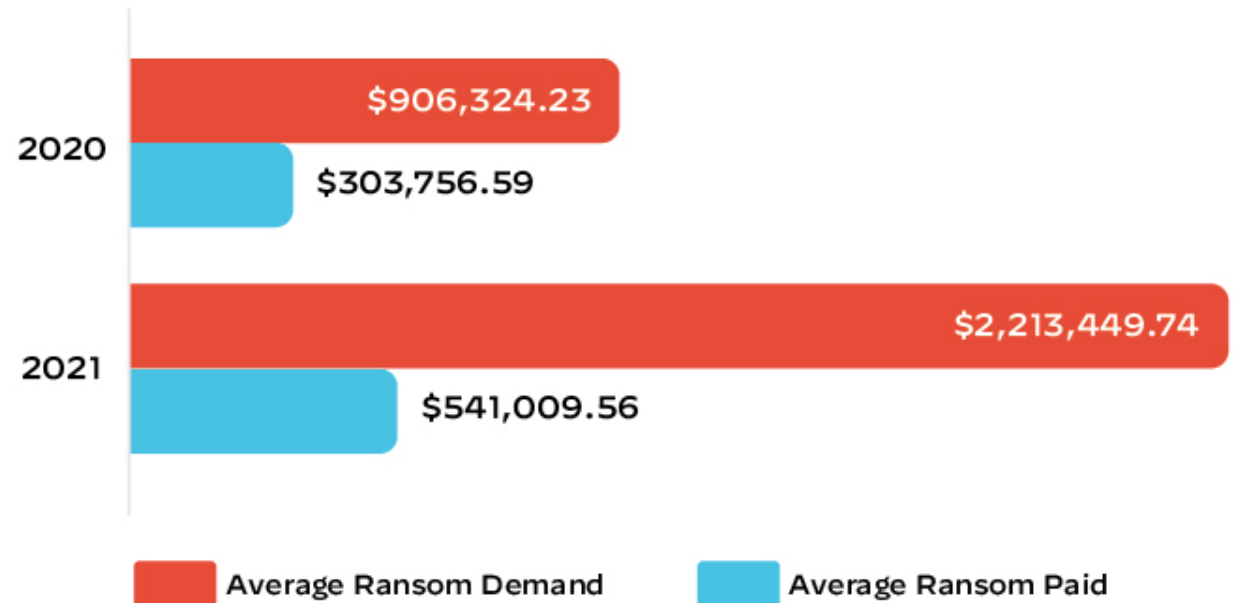
The average ransom paid for organizations increased from \$900,000 in 2020 to **\$2.2 million** in 2021 → 144% year-over-year increase.

The Education Sector traditionally has been a vulnerable and a trusting community whose mission is to promote knowledge and information sharing

– This unfortunately results in Higher Education being labeled a Soft Cyber Target for cyber criminals who are primarily financially motivated.



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



FY21 Key Findings for Higher Education Sector

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.



Impact from 3rd Party Vendor & Ransomware Attack



University of Colorado

Boulder | Colorado Springs | Denver | Anschutz Medical Campus

Lessons learned from notable third-party data breaches of 2021

About the Accellion Cyberattack

The University of Colorado experienced a cyberattack on a vulnerability in software provided by third-party vendor Accellion, which alerted the university in late January. CU is one of many Accellion customers that were affected by the attack. We believe personally identifiable information from students, employees and others may have been compromised.

- Bleeping Computer. The CLOP Ransomware group hacked approximately 300K unique PII related records demanding \$10 million in bitcoin threatening the publishing of the sensitive data if payment is not received. CU was one of at least 10 higher education institutions were impacted shutting down the large file transfer service which the University depended on.



Same 3rd Party Vendor – Zero Day

Actively Exploited Atlassian Zero-Day Bug Allows Full System Takeover

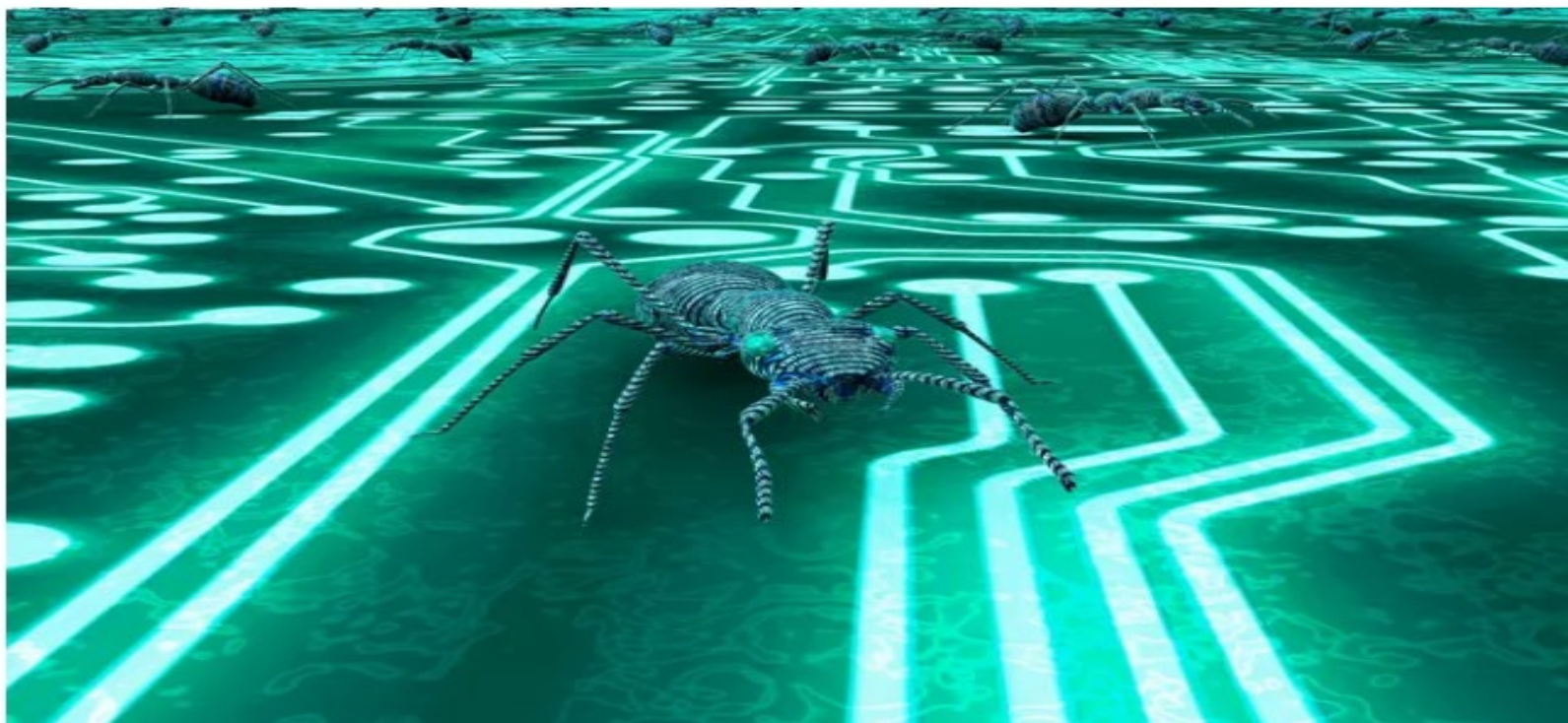
An remote code execution (RCE) vulnerability in all versions of the popular Confluence collaboration platform can be abused in credential harvesting, cyber espionage, and network backdoor attacks.



Tara Seals

Managing Editor, News, Dark Reading

June 03, 2022



Impact of Ransomware Attacks



Regis University Cyberattack: What You Need to Know

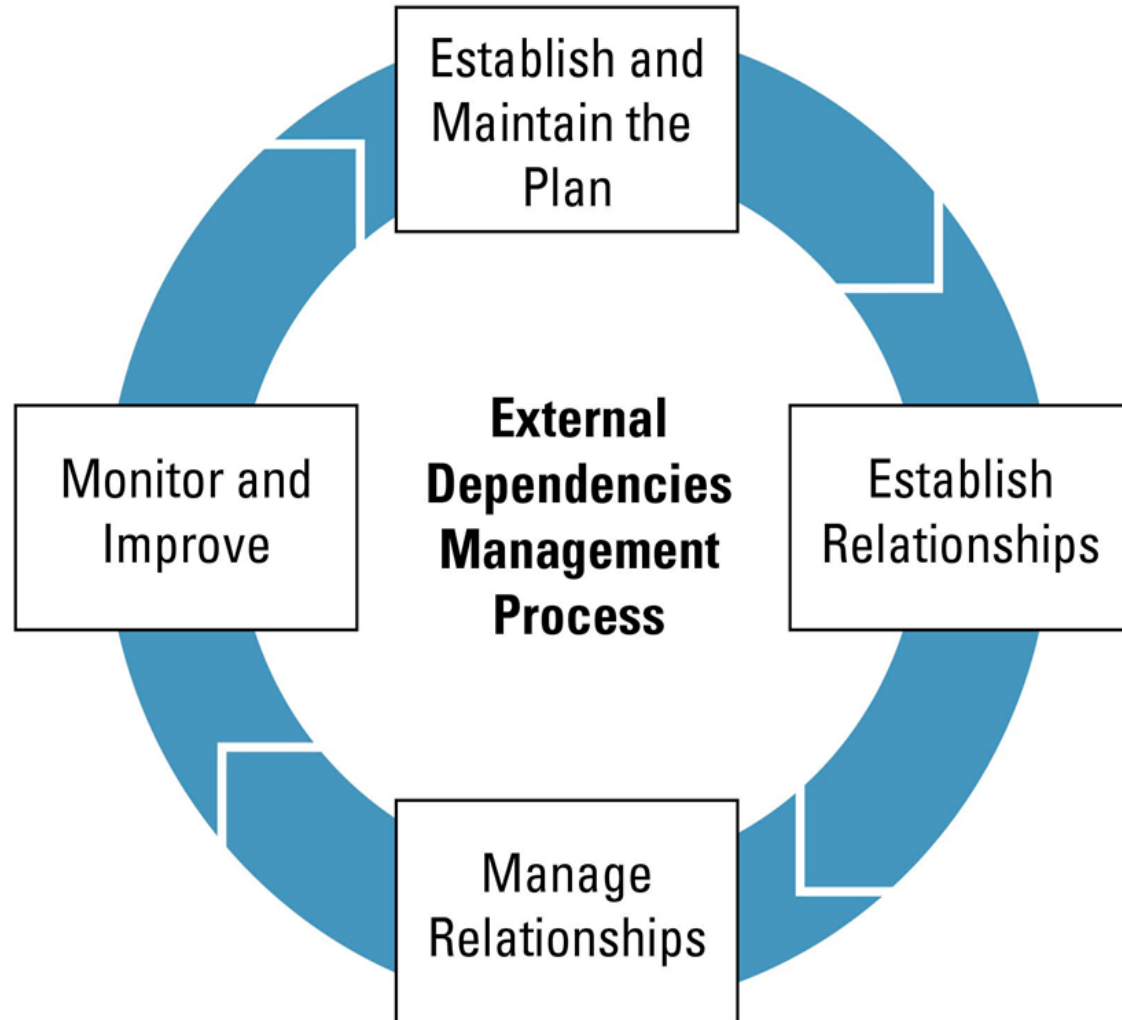
Cyberattack cripples Regis University information technology network in Denver, Colorado. "Malicious threat" likely from outside the United States, report says.

The cyberattack shut down Regis' website, phone lines, email services and online programs that students use to submit work, the university stated. It also led the university to create a supplementary web page, regisupdates.com, to communicate with students and faculty.

- Regis University – Down during critical start to the school year, multiple critical systems became unavailable. Paid ransom, amount of payment not disclosed but event after paying the ransom full access to systems was not fully restored resulting in months of disruption.



Third-Party Vendor Dependency Management Model



Relationship Formation

Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.

Relationship Management and Governance

Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.

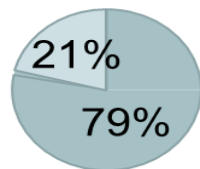
Service Protection and Sustainment

Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.

Third-Party/Vendor Dependency Management

Key practices based on recent field work

Does your organization have a plan for managing external dependencies?

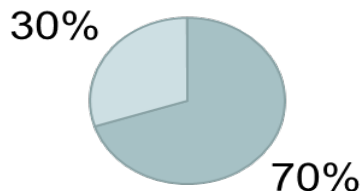


☒ No
☐ Yes

Relating to implementation of external dependency management practices, three activities seem to drive behavior*:

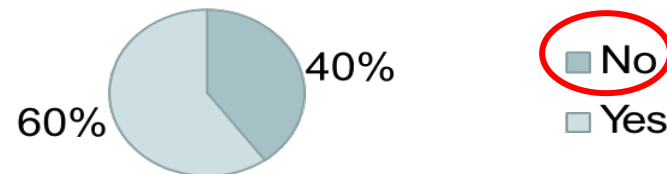
Planning
Measuring
Reporting

Does your organization periodically measure external dependency activities to ensure they are effective?



☒ No
☐ Yes

Is there management oversight of the performance of external dependency management activities?



☒ No
☐ Yes



THIRD-PARTY VENDORS & PROGRAM MANAGEMENT COMPANIES

education
data
university
college
protection
privacy
responsibility
cybersecurity



Common Third-Party Vendors

Learning Management System

- Blackboard Learn
- Canvas
- Moodle
- D2L Brightspace
- Mindflash
- Google Classroom
- Edmodo
- Quizlet
- Schoology
- NEO LMS



Online Program Management Companies

- Wiley Education Services
- Online Education Services
- 2U
- Pearson
- Academic Partnerships
- HotChalk
- iDesign
- Noodle
- Orbis Education
- Learning House
- Zovio
- Kaplan
- Grand Canyon Education
- Bisk Education



Known Vulnerabilities

- Remote Access
- Ability to elevate privileges to those belonging to a teacher.
 - Retrieve test answers
 - Modify access to gradebook
- SQL Injection
 - Ability to create secret admin accounts
 - Allowed for ability to execute malicious code

Security researchers discovered that students could abuse vulnerabilities in certain learning management system (LMS) plugins to access records and edit data.

Critical Moodle Vulnerability Could Lead to Server Compromise

they observed one security flaw through which registered users could have elevated their

This Teen Hacker Found Bugs in School Software That Exposed Millions of Records

Some kids play in a band after school. Bill Demirkapi hacked two education software giants.

Vulnerabilities in Other LMS Plugins and Software

The three WordPress LMS plugins discussed above aren't the only educational software programs

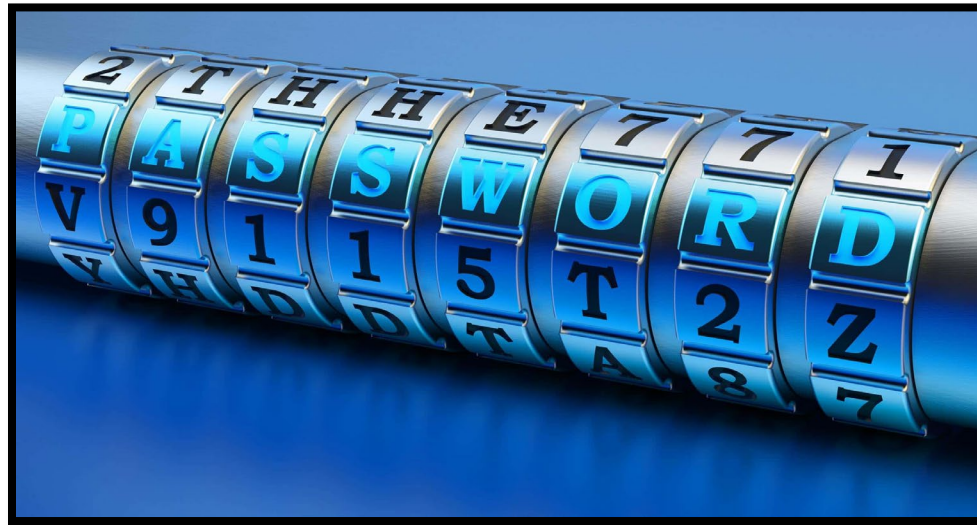
17 Serious New Security Threats Found In Google Chrome

Vulnerabilities in LMS Plugins Allow Students to Access Records, Edit Data



Security Features To Keep Data Safe

- IP Address Blocking
- SSL Certification – encrypts the data that is transmitted
- Advance Password Authentication– Implement a strong password policy.
- Mobile Security
- Account Registration
 - Allow only specific domains
 - Enable captcha



Top Questions To Your Vendor

1. How does your organization protect and defend against cyber-attacks to ensure student information is protected? What information is a priority for your organization?
2. Has the vendor ever become victim to a cyber-attack or data breach? If so, how? Has the vulnerability been resolved?
3. Do you have data security/cyber liability insurance? Consider asking for a copy of the insurance certificate.
4. Does your infrastructure/solution allow MFA?
5. Are vulnerability tests run regularly? Are you willing to share those reports?
6. Is data encrypted?
7. Where are you storing my data geographically? Where is data stored in your infrastructure? How do you transfer data?



Discussion Topics for Schools to Consider

1. Do you have your own in-house security team or is it out-sourced to a 3rd party vendor?
2. How often are 3rd party applications updated?
3. Is principle of least privilege implemented?
4. Have you identified your cybersecurity gaps?



** In a K-12 Cybersecurity [2020 Year in Review Report](#) found that at least **75%** of all data breaches impacting K-12 schools in the U.S. resulted from security incidents involving their vendors and other partners.**

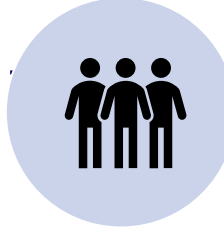


Strategy and Actions to Protect Ourselves



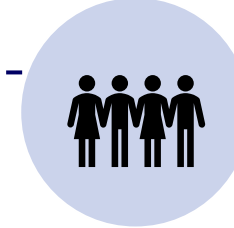
Individual Responsibility

- We ALL are responsible for protecting our institutions.
- We ALL need to do our due diligence.
- We must educate ourselves on what to do and not to do.



Organizational Team

- Teams who design and carry out projects must protect our critical data.
- It's not just the responsibility of IT staff.



Organizational Leadership

- Leadership must provide the necessary resources, policy framework and financial backing required to be successful.



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)

Tanya Taplin

Region 8 State Cybersecurity Coordinator – (North Dakota)


Tanya.Taplin@cisa.dhs.gov
(701) 515-8924 (Cell)



Your Questions!



Resources for those new to the topic



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](#)

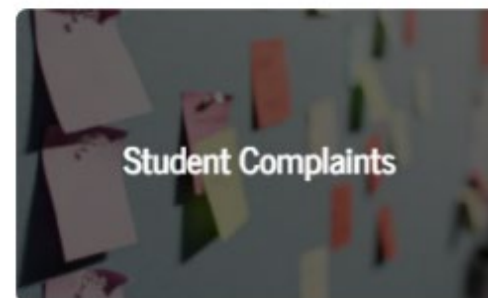
Resources by topic

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



wcetsan.wiche.edu

Topic Areas



Upcoming Events

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 and the home page of the SAN Website!*

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 and from the home page of the WCET Website!*



@wcet_info #wcetSAN



wcetsan.wiche.edu



Thank you

to our speakers, Dave Sonheim and Tanya Taplin,
and to all our attendees today!





Contact Us



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.