Collaboration in the Security Community

Chip Conner-Rondot - REN-ISAC
Paul Howell – Internet2
Nick Lewis – Internet2

Agenda

- Who are we and why are we here?

- Collaborative successes

- Your feedback!

EDUCAUSE

- EDUCAUSE Cybersecurity and Privacy Professionals Conference – May 1-3, 2023 in Bellevue, WA – last week!

- Community Groups – Awareness and Education, GRC, CPO, Privacy, TOP, HECVAT, and 171 compliance

- EDUCAUSE QuickPolls, are one-day polls that rapidly gather, analyze, and share input from the EDUCAUSE community about specific emerging topics.

EDUCAUSE

| Events | Searcl |

HOME | **LEARNING EXPERIENCE** | **REGISTRATION**

Learning Lab | Creating a Campus Culture of Security and Privacy

Part 1: August 1 | 1:00–2:00 p.m.ET
Part 2: August 3 | 1:00–2:30 p.m. ET
Part 3: August 10 | 1:00–2:30 p.m. ET
Part 4: August 17 | 1:00–2:30 p.m. ET

Overview

As security and privacy have become increasingly intertwined, it's become critical to develop a campus culture that embraces both. A strategic awareness plan helps ensure that your efforts are successful. Attendees will participate in exercises to assess their audiences, develop messaging, identify needed assets (including campus partners), and build an effective plan.

Learning Outcomes:

NOTE: You will be asked to complete assignments in between the Learning Lab segments that support the learning outcomes stated below. You will receive feedback and constructive critique from course facilitators.

- Understand key elements and considerations in creating a security and privacy awareness plan

Regist
Space
now t

Particip
is enco
conten
be view

INTERNET2 2023 COMMUNITY EXCHANGE

COMM ex 23

Career paths – find your path

The Four Pathways

The four pathways serve to guide professionals supporting and transforming higher education through the innovative use of technology.

Information Security

The Information Security Pathway is for higher education professionals whose primary role is to keep the campus community safe and protect institutional data across systems and for constituents, including students, faculty, staff, and partners.

LEARN MORE

Information Technology

The Information Technology Pathway is for leaders and professionals who support information technology systems and their strategy, management, budgets, and policy. The pathway guides those who manage the technology ecosystem comprising the systems and services that institutions use to store and manage data and processes, whether on campus, in the cloud, or through shared services.

LEARN MORE

Innovation

The Innovation Pathway is for professionals dedicated to the advancement of their institution's mission and strategic goals through the innovative and creative application of strategies and solutions. This pathway supports those tasked with leveraging data and technology in support of cross-institutional transformation.

LEARN MORE

Teaching & Learning

The Teaching and Learning Pathway guides those working to enhance or transform learning experiences and student success across the institution through the effective application of learning science and relevant data to guide the selection of pedagogies and technologies.

LEARN MORE

Positions and years spent at each professional level will vary.

2021 EDUCAUSE Horizon Report Information Security Edition

2021 EDUCAUSE Horizon Report®

- Cloud Vendor Managment • Endpoint Detection and Response
- Multifactor Authentication (MFA)/Single Sign-On (SSO)
- Preserving Data Authenticity/Integrity
- Research Security • Student Data Privacy and Governance

This report profiles important trends and key technologies and practices shaping the future of information security, and envisions a number of scenarios and implications for that future. It is based on the perspectives and expertise of a global panel of leaders from across the higher education landscape

Quicktalks…

Member QuickTalk | Core Data Service (CDS) Study Group

Online
June 07, 2022

Join our study group to connect with EDUCAUSE experts and your peers about how to get the most out of your CDS experience.

Member QuickTalk | Showcase Coffee Shop: The Digital versus Brick-and-Mortar Balancing Game

Online
May 12, 2022

Grab your coffee and join us for an informal discussion on digital and physical work and learning spaces.

Member QuickTalk | Core Data Service (CDS) Study Group

Online
May 10, 2022

Join our study group to connect with EDUCAUSE experts and your peers about how to get the most out of your CDS experience.

EDUCAUSE

Jobs   .EDU Domain   EDUCAU

Hybrid Campus Showcase   Topics   Insights   Conferences & Learning   Community   Wh

Thursday, December 09 | 1:00PM–2:00PM ET | Online

Member QuickTalk | Cyber Insurance: Renewals, Rate Increases and Shared Strategies

Cyber Insurance has become an increasingly important topic for our members that is likely to continue evolving for higher education. As we look to 2022 and upcoming insurance renewals, we would like to provide members an opportunity to discuss their experiences and questions, as well as share strategies to address premium increases and new requirements imposed by underwriters and carriers.

To get the most from the QuickTalk experience, we encourage attendees to review the recently published **FAQ** on cyber insurance for higher education. This will be an interactive event and all are invited to contribute their questions and expertise.

QuickTalk Moderators

Aaron Baillio
CISO, University of Oklahoma

Brian Kelly
Director of the Cybersecurity Program, EDUCAUSE

Additional Resources

- **Frequently Asked Questions About Cyber Insurance**

Cloud Services Updates

- Cloud Scorecard – over 50 service providers with many of interest to information security

- Institutional Profiles

- Cloud Vendor Risk Management service evaluation

- NET+ Kion – management and compliance across AWS, Azure, and GCP

- CWE Webinar Series – addressing some security topics

MY PORTFOLIO UPDATES

- CrashPlan (39), Duo (204), LastPass (69), Palo Alto Networks (3), Splunk (29) updates

  - NET+ Splunk added Splunk Cloud to the program!

  - MFA Community Survey 2023 data analysis underway

  - Starting NET+ LastPass Service Advisory Group

- Current Community Calls – CrashPlan (20) and Duo (60-120). Might restart PAN and Splunk.

- Exploring new service providers

NATIONAL RESEARCH AND EDUCATION NETWORK UPDATES

Routing Integrity Initiative encourages the community's adoption of best practices that strengthen the resilience and reliability of data movement across the R&E network ecosystem to support our shared missions

- Routing Security as defined by Mutually Agreed Norms for Routing Security (see MANRS.org)
- Hardening of network devices (MFA authentication, regular review of firmware, logging, etc.)
- Detection and mitigation of DDoS attacks
- Resilient cloud connectivity
- IPv6 Deployment
- Routing Integrity Assessment service - contact manrs@internet2.edu
- Reports showing the accuracy of published routing policy for RENs
    ### https://github.internet2.edu/ssw/IRR-report
- Autonomous System Provider Authorization Working Group (ASPA-WG) is develop recommendations for its adoption by R&E networks

INTERNET2 ROUTING INTEGRITY MILESTONES
MAY 2023
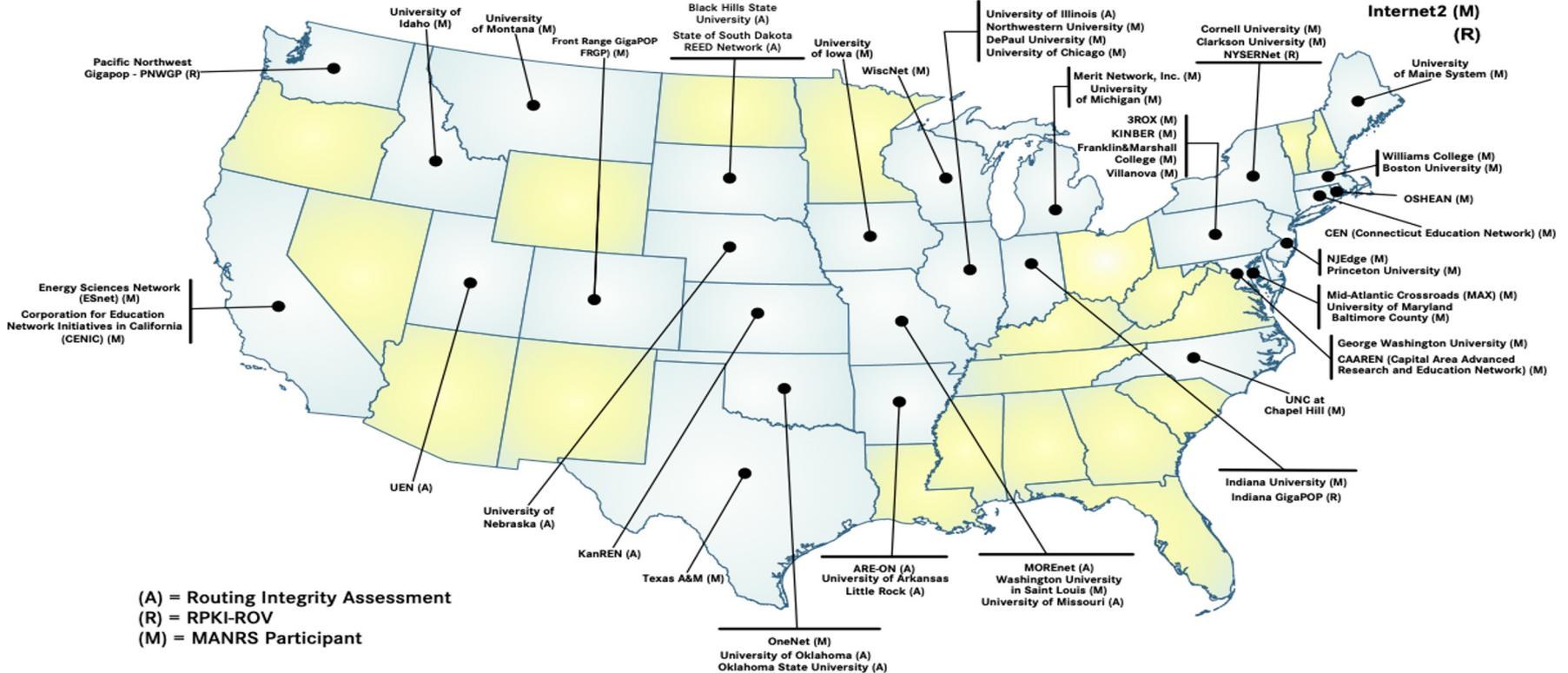
(A) = Routing Integrity Assessment
(R) = RPKI-ROV
(M) = MANRS Participant

INTERNET2 ROUTING INTEGRITY MILESTONES
MAY 2023

(A) = Routing Integrity Assessment
(R) = RPKI-ROV
(M) = MANRS Participant
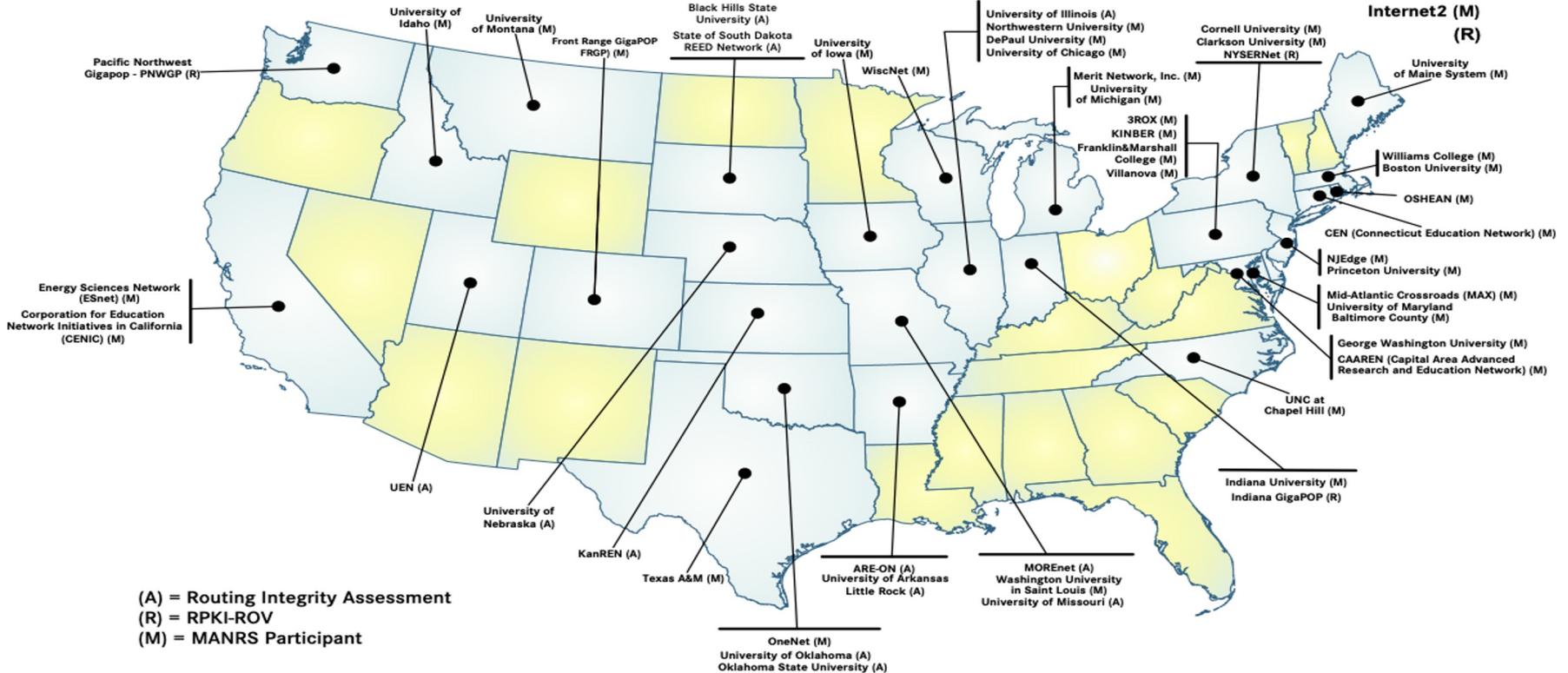
REN-ISAC

Research & Education Networks
Information Sharing & Analysis Center

REN-ISAC - What Are We Seeing?

- Ransomware Tracker
- CSIRT Metrics
- Security Event System (SES)
- Insurance
- Compliance

2022 Stats by Ransomware Group

RW Group	Count of RW Group	% of overall
Vice Society	9	21%
AvosLocker	7	16%
AlphVM (BlackCat)	4	9%
LockBit 3.0	3	7%
Unknown	3	7%
Hive	3	7%
LockBit 2.0	3	7%
Suncrypt	2	5%
BianLian	2	5%
Snatch	1	2%
Quantum	1	2%
BlackByte	1	2%
Conti	1	2%
54bb47h (Sabbath)	1	2%
REvil	1	2%
Royal	1	2%
Grand Total	43	100%

Mean Enrollment	8310.34	
Median Enrollment	3231	
RI Members Affected	19.00%	

2022 Ransomware stats

2023 Stats by Ransomware Group

RW Group	Count of RW Group	% of overall
Vice Society	11	47.83%
LockBit 3.0	2	8.70%
BianLian	2	8.70%
AvosLocker	1	4.35%
Snatch	1	4.35%
MONTI	1	4.35%
Nokoyawa	1	4.35%
Royal	1	4.35%
Medusa	1	4.35%
Play	1	4.35%
AlphVM	1	4.35%
Grand Total	23	100.00%

Mean Enrollment	13258.48
Median Enrollment	8735
RI Members Affected	8.70%

2023 Ransomware stats
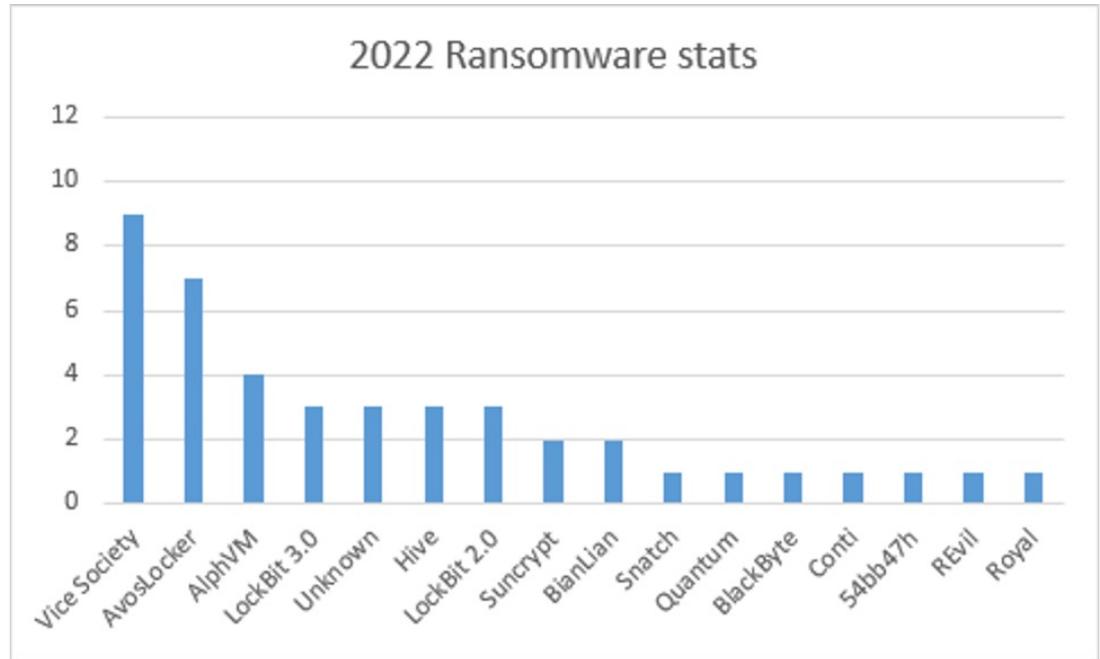
CSIRT ACTIVITY THROUGH 2023

	Jan	Feb	Mar	Q1
Notifications				
compromised machines	3570	5137	4643	**13350**
compromised credentials	6791	9977	5995	**22763**
spam or phish	15	12	10	**37**
vulnerable machines	0	67	445	**512**
open recursive DNS resolvers	75	68	99	**242**
open mail relays	0	0	0	**0**
ssh scanning	0	0	0	**0**
other	7	3	8	**18**
Total Notifications	**10,458**	**15,264**	**11,200**	**36,922**
SOC Interactions				
notification questions	10	31	9	**50**
password resets	90	7	2	**99**
notifications	23	26	31	**80**
other	7	261	198	**466**
SOC non-interactive tickets	1,026	498	278	**1802**
Total SOC Tickets	**130**	**325**	**240**	**2,497**
Unique institutions contacted per period	**2,060**	**2,189**	**1,953**	

CSIRT ACTIVITY THROUGH 2022

Vulnerabilities	Total
compromised machines	145291
compromised credentials	14226
spam or phish	561
vulnerable machines	217
open recursive DNS resolvers	1155
open mail relays	0
ssh scanning	0
other	682

Security Event System Stats

Top SES Data Providers by Unique Indicators Submitted in the Past Seven Days (Updated Hourly)

Top Threat Indicator Types Reported in the Past Seven Days (Updated Hourly)

Top Threat Types as Reported by SES Partners in the Past Seven Days (Updated Hourly)
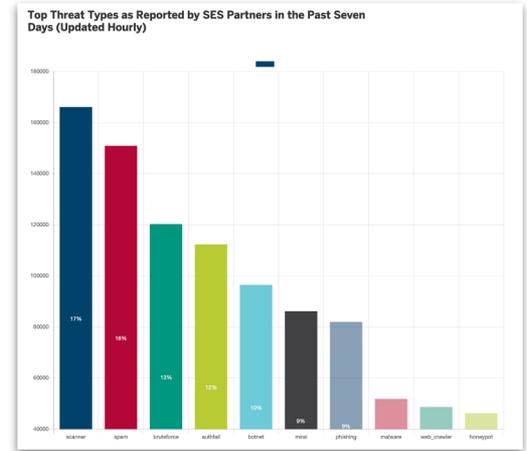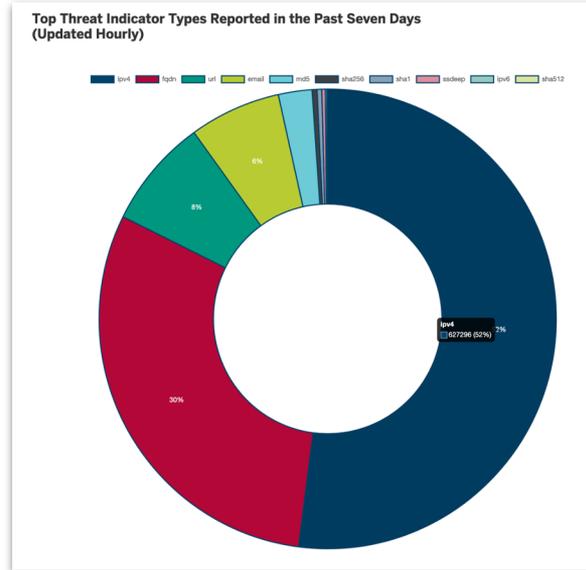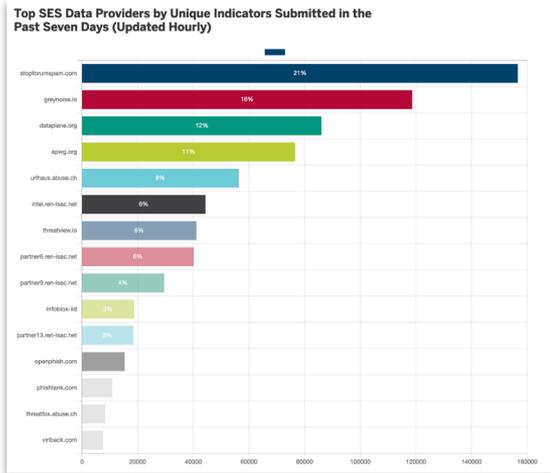
https://www.ren-isac.net/member-resources/SES/SES_Data_Feed.html

Security Event System Stats
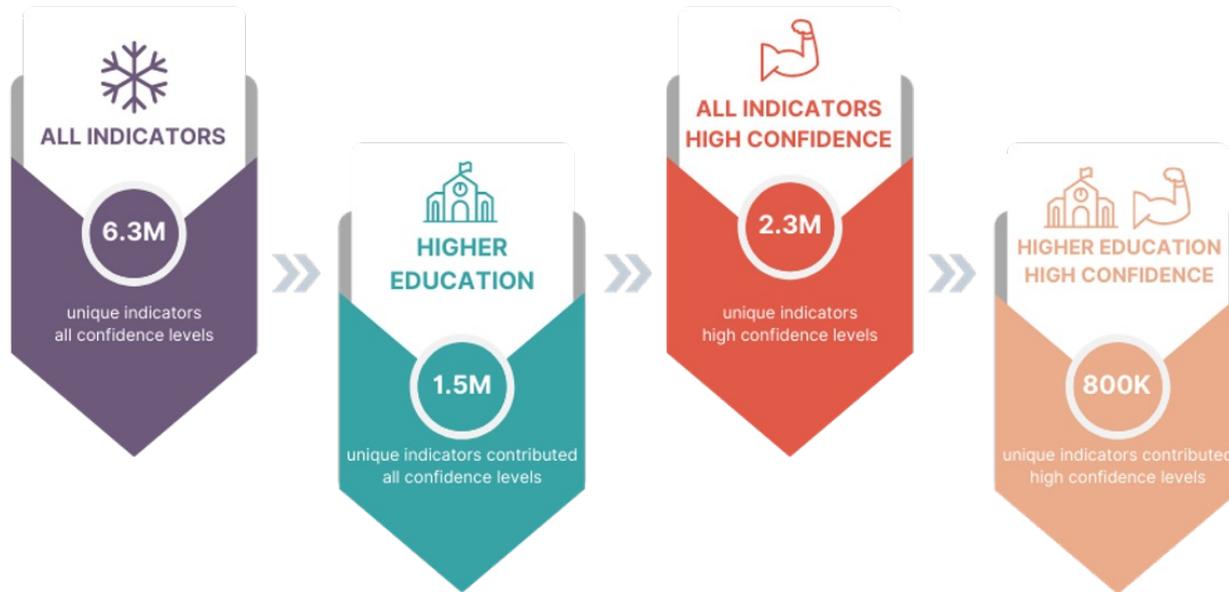
Cyber Insurance

Higher expectations for less coverage

Separate riders for ransomware?

No coverage for nation state attributed attacks?

C O M P L I A N C E

FTC Safeguards Rule

"The Safeguards Rule requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information."

Some provision deadlines extended

https://www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023

REN-ISAC - What Are We Doing?

- SES
- pDNS
- Active Discussion Lists
- Collaboration with other ISACs
- CSIRT Activities - all EDUs
- Alerts/Advisories/Best Practices
- The REN-ISAC Hub - *NEW*

REN-ISAC - How Can We Help?

info@ren-isac.net

AREAS OF COLLABORATION

- Conference planning

- Working Groups

- HECVAT

- Program Committees

- Feedback on each others' projects

Tell Us About It!

- What do you need?

- What is not getting done?

- Where do you see our coordination opportunities?

Thanks!

QUESTIONS AND FEEDBACK

CONTACT INFORMATION

- Chip Conner-Rondot, REN-ISAC - ctconron@iu.edu
- Joseph Potchanant - jpotchanant@educause.edu
- Paul Howell – phowell@internet2.edu
- Nick Lewis – nlewis@internet2.edu