Collaboration in the Security Community

Marina Krenz - REN-ISAC
Paul Howell – Internet2
Nick Lewis – Internet2
Agenda

• Who are we and why are we here?

• Collaborative successes

• Your feedback!
Conferences

- EDUCAUSE Cybersecurity and Privacy Professionals Conference – May 1–3, 2024 Minneapolis, MN! CFP will open in early January.

- EDUCAUSE Annual next month - October 9–12, 2023 in Chicago, IL
EDUCAUSE

• EDUCAUSE Cybersecurity and Privacy Workforce Survey will be released in October 2023

• The new EDUCAUSE Cybersecurity and Privacy Guide will also launch in October 2023

• 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.
Welcome to EDUCAUSE Connect
Collaborate with peers to share strategic advice, solve challenges, and develop new approaches.

Explore
Discover communities to enrich your experience and learning opportunities.
Explore communities ▶

Connect
Find others with whom you may seek advice and share common challenges.
Connect with others ▶

Engage
Join in discussions with your peers and industry leaders to expand your knowledge.
Engage in discussions ▶

Latest Discussions
RE: hybrid graduation platforms
By Web Builder, 3 hours ago
Posted in: Small Colleges
We had great success using Marching Order at my previous institution. Graduation Ceremony Software

Quick Links
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
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.

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.

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.

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.

Positions and years spent at each professional level will vary.
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.

Education
Hybrid Campus Showcase | Topics | Insights | Conferences & Learning | Community | WI

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
INTERNET2
Cloud Services Updates

- Cloud Scorecard – over 50 service providers with many of interest to information security
- Institutional Profiles
- Vendor Risk Management service evaluation
- NET+ Miro now live!
- Service Evaluation for data migration tools
MY PORTFOLIO UPDATES

• CrashPlan (39), Duo (204), LastPass (69), Palo Alto Networks (3), Splunk (28) updates
  • MFA Community Report 2023 presentation this week!
  • Started NET+ LastPass Service Advisory Group

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

• Vendor Risk Management and Vendor Management call?

• Exploring new service providers
InCommon

- **BaseCAMP** provides a workshop for those new to identity and access management (IAM), new to InCommon, or both, that focuses on the basics, an introduction to the InCommon Federation, and overviews and demonstrations of the community-developed identity and access management suite.
- Participate in the [InCommon Academy for IAM training](#).
- Get involved in the [Community Success Program](#).
- Changes coming from NIH around potential areas of improvement in identify proofing processes for your campus.
- Get involved in the 2nd annual cybersecurity cooperation [exercise this fall](#)!
- InCommon kicked off Futures2, a [strategic planning project](#) being undertaken by the Steering Committee to help guide a vibrant future for InCommon.
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 developing recommendations for its adoption by R&E networks
EACH OF US PROTECTING

INTERNET2 ROUTING INTEGRITY MILESTONES

MAY 2023

(A) = Routing Integrity Assessment
(R) = RPKI-ROV
(M) = MANRS Participant
Nearly half of the US R&E IP addresses lack an ARIN agreement

What we see in the Internet2 R&E table:
- 2,203 ARIN direct IP address assignments
- 1,023 (46%) without an ARIN Agreement
- $1,876,124,160 Market value of IP numbers not covered by ARIN agreement!

Many mistakenly believe their IP addresses are covered by an ARIN agreement
- No agreement required to manage whois information (i.e., portal access doesn’t require an agreement)
- You may be receiving and paying ARIN bills for other resources
Benefits of the ARIN agreement

- Access to routing security services:
  - Authenticated IRR
  - Hosted RPKI-ROAs
- Participation in ARIN’s governance
- Better sleep knowing you have an agreement that specifies the registration services that announce to the Internet who holds your IP addresses

**NOTE:** Using ARIN Hosted RPKI-ROA service is, by far, the easiest way to mitigate the risk of outage due to route hijacking. No equipment changes required. It’s only a bit more complicated than filling out a simple web form!
ARIN agreement fee changes (for legacy resources)

For legacy resources in 2023, ARIN’s fees are $175/yr. That’s $175/yr for any number of legacy resources. **Signing an agreement this year locks in fee increases of $25/yr.**

Waiting until next year (or longer) to sign an ARIN agreement will result in fees subject to ARIN’s normal fee schedule. For a single /16, the current fee schedule is $4,000/yr (22 times higher than the legacy fee schedule).

Across the Internet2 community, this difference adds up to **$2M/yr** in fees for agreements signed after 2023, vs **$75K/yr** in fees for agreements signed this year.

Questions? Go to the ARIN table or email manrs@internet2.edu
REN-ISAC

Research & Education Networks
Information Sharing & Analysis Center
REN-ISAC - What Are We Seeing?

- Ransomware Tracker
- CSIRT Metrics
- Security Event System (SES)
- pDNS
### 2022-2023 Stats by Ransomware Group

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

**Mean Enrollment**: 8310.34  
**Median Enrollment**: 3231  
**RI Members Affected**: 19.00%
### CSIRT Activity in 2023

#### Master File: Current CSIRT Data 2023

<table>
<thead>
<tr>
<th></th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Q1</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised Machines</td>
<td>3570</td>
<td>5137</td>
<td>4643</td>
<td>13,350</td>
<td>2,858</td>
<td>4,313</td>
<td>4,244</td>
<td>11,415</td>
</tr>
<tr>
<td>Compromised Credentials</td>
<td>6791</td>
<td>9977</td>
<td>5995</td>
<td>22,763</td>
<td>1,893</td>
<td>3,947</td>
<td>9,234</td>
<td>15,074</td>
</tr>
<tr>
<td>Spam or Phish</td>
<td>15</td>
<td>12</td>
<td>10</td>
<td>37</td>
<td>9</td>
<td>19</td>
<td>3</td>
<td>31</td>
</tr>
<tr>
<td>Vulnerable Machines</td>
<td>0</td>
<td>67</td>
<td>445</td>
<td>512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Open Recursive Domain Resolvers</td>
<td>75</td>
<td>68</td>
<td>99</td>
<td>242</td>
<td>61</td>
<td>71</td>
<td>76</td>
<td>208</td>
</tr>
<tr>
<td>Open Mail Relays</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SSH Scanning</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Other Misc Notifications</td>
<td>7</td>
<td>3</td>
<td>8</td>
<td>18</td>
<td>3</td>
<td>8</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>10,458</td>
<td>15,264</td>
<td>11,200</td>
<td>36,922</td>
<td>4,824</td>
<td>8,358</td>
<td>13,560</td>
<td>26,742</td>
</tr>
</tbody>
</table>

#### SOC Interactions

<table>
<thead>
<tr>
<th>Category</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Q1</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>notification questions</td>
<td>10</td>
<td>31</td>
<td>9</td>
<td>50</td>
<td>55</td>
<td>58</td>
<td>22</td>
<td>135</td>
</tr>
<tr>
<td>password related</td>
<td>90</td>
<td>7</td>
<td>2</td>
<td>99</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>notifications</td>
<td>33</td>
<td>37</td>
<td>40</td>
<td>130</td>
<td>48</td>
<td>49</td>
<td>12</td>
<td>169</td>
</tr>
<tr>
<td>other</td>
<td>7</td>
<td>261</td>
<td>198</td>
<td>466</td>
<td>134</td>
<td>160</td>
<td>165</td>
<td>459</td>
</tr>
<tr>
<td><strong>Total Interactions</strong></td>
<td>140</td>
<td>356</td>
<td>249</td>
<td>745</td>
<td>237</td>
<td>267</td>
<td>203</td>
<td>707</td>
</tr>
</tbody>
</table>

#### SOC Non-Interactive Tickets

<table>
<thead>
<tr>
<th></th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Q1</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,026</td>
<td>498</td>
<td>278</td>
<td>1,002</td>
<td>163</td>
<td>192</td>
<td>222</td>
<td>577</td>
<td></td>
</tr>
</tbody>
</table>

#### Unique Institutions contacted per period

<table>
<thead>
<tr>
<th></th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Q1</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
<th>Q2</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,060</td>
<td>2,189</td>
<td>1,953</td>
<td>N/A</td>
<td>1,099</td>
<td>1,606</td>
<td>2,061</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
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)

https://www.ren-isac.net/member-resources/SES/SES_Data_Feed.html
Security Event System Stats 2022-2023

31MM+ **ALL** indicators

10MM+ High confidence indicators

7,7MM+ High confidence indicators from .edu providers

72% of High Confidence indicators are from .edu providers
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
- Peer Assessment
- PEN testing
REN-ISAC - How Can We Help?

info@ren-isac.net
COLLABORATIONS
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

- Krenz, Marina, REN-ISAC – <mvkrenz@iu.edu>
- Joseph Potchanant - jpotchanant@educause.edu
- Paul Howell – phowell@internet2.edu
- Nick Lewis – nlewis@internet2.edu