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.
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
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
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
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
Hybrid Campus Showcase | Topics | Insights | Conferences & Learning | Community | WiFi
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

GWE 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
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 ALL OF US

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

<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%
### 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>11</td>
<td>47.83%</td>
</tr>
<tr>
<td>LockBit 3.0</td>
<td>2</td>
<td>8.70%</td>
</tr>
<tr>
<td>BlanLian</td>
<td>2</td>
<td>8.70%</td>
</tr>
<tr>
<td>AvosLocker</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td>Snatch</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td>MONTI</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td>Nokoyawa</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td>Royal</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td>Medusa</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td>Play</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td>AlphVM</td>
<td>1</td>
<td>4.35%</td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td><strong>23</strong></td>
<td><strong>100.00%</strong></td>
</tr>
</tbody>
</table>

Mean Enrollment: 13258.48
Median Enrollment: 8735
RI Members Affected: 8.70%
## CSIRT ACTIVITY THROUGH 2023

<table>
<thead>
<tr>
<th></th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Q1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Notifications</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>compromised machines</td>
<td>3570</td>
<td>5137</td>
<td>4643</td>
<td>13350</td>
</tr>
<tr>
<td>compromised credentials</td>
<td>6791</td>
<td>9977</td>
<td>5995</td>
<td>22763</td>
</tr>
<tr>
<td>spam or phish</td>
<td>15</td>
<td>12</td>
<td>10</td>
<td>37</td>
</tr>
<tr>
<td>vulnerable machines</td>
<td>0</td>
<td>67</td>
<td>445</td>
<td>512</td>
</tr>
<tr>
<td>open recursive DNS resolvers</td>
<td>75</td>
<td>68</td>
<td>99</td>
<td>242</td>
</tr>
<tr>
<td>open mail relays</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>
</tr>
<tr>
<td>other</td>
<td>7</td>
<td>3</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td><strong>Total Notifications</strong></td>
<td>10,458</td>
<td>15,264</td>
<td>11,200</td>
<td>36,922</td>
</tr>
<tr>
<td><strong>SOC Interactions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>notification questions</td>
<td>10</td>
<td>31</td>
<td>9</td>
<td>50</td>
</tr>
<tr>
<td>password resets</td>
<td>90</td>
<td>7</td>
<td>2</td>
<td>99</td>
</tr>
<tr>
<td>notifications</td>
<td>23</td>
<td>26</td>
<td>31</td>
<td>80</td>
</tr>
<tr>
<td>other</td>
<td>7</td>
<td>261</td>
<td>198</td>
<td>466</td>
</tr>
<tr>
<td>SOC non-interactive tickets</td>
<td>1,026</td>
<td>498</td>
<td>278</td>
<td>1802</td>
</tr>
<tr>
<td><strong>Total SOC Tickets</strong></td>
<td>130</td>
<td>325</td>
<td>240</td>
<td>2,497</td>
</tr>
<tr>
<td><strong>Unique institutions contacted per period</strong></td>
<td>2,060</td>
<td>2,189</td>
<td>1,953</td>
<td></td>
</tr>
</tbody>
</table>
## CSIRT Activity Through 2022

<table>
<thead>
<tr>
<th>Vulnerabilities</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>compromised machines</td>
<td>145291</td>
</tr>
<tr>
<td>compromised credentials</td>
<td>14226</td>
</tr>
<tr>
<td>spam or phish</td>
<td>561</td>
</tr>
<tr>
<td>vulnerable machines</td>
<td>217</td>
</tr>
<tr>
<td>open recursive DNS resolvers</td>
<td>1155</td>
</tr>
<tr>
<td>open mail relays</td>
<td>0</td>
</tr>
<tr>
<td>ssh scanning</td>
<td>0</td>
</tr>
<tr>
<td>other</td>
<td>682</td>
</tr>
</tbody>
</table>
Security Event System Stats

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

- **ALL INDICATORS**
  - 6.3M unique indicators, all confidence levels

- **HIGHER EDUCATION**
  - 1.5M unique indicators contributed, all confidence levels

- **ALL INDICATORS HIGH CONFIDENCE**
  - 2.3M unique indicators, high confidence levels

- **HIGHER EDUCATION HIGH CONFIDENCE**
  - 800K unique indicators contributed, high confidence levels
Cyber Insurance

Higher expectations for less coverage

Separate riders for ransomware?

No coverage for nation state attributed attacks?

COMPLIANCE

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

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
COLLABORATION
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?
QUESTIONS AND FEEDBACK

Thanks!
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