Monday, May 2

3:00 p.m. – 5:00 p.m.

Registration Desk Open

Convention Registration, 3rd Floor

Session Type: Service Desk

Delivery Format: Service Desk

Track:

Tuesday, May 3

7:30 a.m. – 8:30 a.m.

Continental Breakfast for Preconference Workshop Participants

Harborside Foyer, 4th Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues for a light breakfast and network informally.

7:30 a.m. – 5:30 p.m.

Registration Desk Open

Convention Registration, 3rd Floor

Session Type: Service Desk

Delivery Format: Service Desk

Track:

8:30 a.m. – 12:00 p.m.

Evolving Risk and Compliance Landscape in Higher Ed: Implications for Building and Maturing an IT Risk Management Program (separate registration is required)

Harborside Ballroom E, 4th Floor

Session Type: Industry Led

Delivery Format: Preconference Workshop

Track:

***Cam Beasley**, Chief Information Security Officer, University of Texas at Austin*
***Ryan Orren**, Sr. IT Compliance Manager, Virginia Tech*
***Allison Kay Henry**, Chief Information Security Officer, University of California, Berkeley*
***Andrew Scheifele**, Co-Founder and CEO, Salty Cloud PBC*

Higher Ed security and risk professionals are increasingly tasked with implementing and evolving campus risk programs. Join faculty from Virginia Tech, UT Austin and Berkeley to discuss emerging trends and lessons learned. In this workshop we will explore: emerging EDU regulatory requirements; assessment development; and risk reporting.

Security Log Analysis (separate registration is required)

Harborside Ballroom A, 4th Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

***Ishan Abhinit**, Senior Security Analyst, Indiana University Bloomington*
***Mark Krenz**, Chief Security Analyst, Indiana University*

The security log analysis workshop walks participants through the security log analysis life cycle, providing considerations for centralized log collection and log management tools, phases of compromise, and examples from real attacks. We will be analyzing logs from Zeek Network Security Monitor, the Apache web server, two-factor authentication systems, cloud service logs, and others. This workshop also includes a hands-on exercise that will demonstrate techniques to analyze logs to detect security incidents using both the command line and Elastic Stack (aka ELK). The hands-on exercise will provide an overview of investigation techniques to determine security incident logs of some common attacks like SQL injection, filesystem transversal, brute force attacks, command-line injection, and more. Recent security vulnerabilities, such as log4shell, will also be discussed, along with techniques for detection. This will be an interactive session allowing Q&A and will also feature interactive polls to enhance participants' learning experience.

What the HECVAT? An Introduction to HECVAT and Cloud Security Assessments (separate registration is required)

Harborside Ballroom D, 4th Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

***Charles Escue**, Extended Information Security Manager, Indiana University*
***Joshua Callahan**, Information Security Officer and CTO, Humboldt State University*
***Jon Allen**, Associate Vice President CIO & CISO, Baylor University*
***Nick Lewis**, Program Manager, Security and Identity, Internet2*

Campus IT environments are rapidly changing, and the speed of cloud service adoption has gotten almost out of control! How are campuses managing the risk posed by these services? This workshop will focus on how information security teams can work with stakeholders to manage and assess risks surrounding cloud services.

Wrangling an Ever-Changing Landscape: Cyber Insurance, Ransomware, and Your Security Posture (separate registration is required)

Harborside Ballroom B, 4th Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

***Amy Starzynski Coddens**, Strategic Partnerships Manager, Indiana University*
***Michael Davis**, REN-ISAC Principal Security Engineer, Indiana University*
***Susan Coleman Snyder**, Assessment Program Manager, Indiana University Bloomington*
***Krysten S Stevens**, REN-ISAC Director of Technical Operations, Indiana University*
***Jacquie Brager**, Director of Risk Management, Carroll Community College*

With growing ransomware threats against service continuity and data confidentiality, cyber insurance providers are becoming more discriminating about which organizations they cover or which claims they process. Obtaining cyber insurance requires completing extensive questionnaires detailing basic cyber hygiene practices and organizational safeguards, followed by periodic looks at new and evolving threats, and adjusting or adding institutional safeguards accordingly. This workshop provides: • Practical tips and techniques for understanding ransomware threats • Tools that help strengthen basic cyber hygiene • Recommendations around reducing risks to data and resources • Guidance for completing a cyber insurance risk assessment Join REN-ISAC's Cybersecurity Peer Assessment Service and Operations Team members in exploring this complex and ever-changing landscape.

10:00 a.m. – 10:30 a.m.

Refreshment Break for Preconference Workshop Participants

Harborside Foyer, 4th Floor

Session Type: Break

Delivery Format: Break

Track:

12:00 p.m. – 1:00 p.m.

Lunch for Preconference Workshop Participants

Harborside Ballroom C, 4th Floor

Session Type: Meal

Delivery Format: Meal

Track:

Lunch is provided for all preconference workshop attendees. *Lunch ticket is required.*

1:00 p.m. – 4:30 p.m.

An Advanced Perspective on What the HECVAT! (separate registration is required)

Harborside Ballroom D, 4th Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

***Joshua Callahan**, Information Security Officer and CTO, Humboldt State University*
***Jon Allen**, Associate Vice President CIO & CISO, Baylor University*
***Nick Lewis**, Program Manager, Security and Identity, Internet2*
***Charles Escue**, Extended Information Security Manager, Indiana University*

In the HECVAT 3 update, many changes behind the scenes were made to update the tools. This workshop will go into the tools, the updates, the inner workings on weighting, and all the gory details! We'll also work through your feedback and questions to help determine future plans for the HECVAT.

Creating a Campus Culture of Security and Privacy (separate registration is required)

Harborside Ballroom B, 4th Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

***Cara Bonnett**, Technology Risk Assurance Manager, Duke University*
***Ben Woelk**, Governance, Awareness, and Training Manager, Rochester Institute of Technology*

As security and privacy have become increasingly intertwined, it has 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, determine messaging, identify needed assets, and begin building an effective plan.

Cyber Defense Clinic (separate registration is required)

Harborside Ballroom E, 4th Floor

Session Type: Industry Led

Delivery Format: Preconference Workshop

Track:

***Helen Patton**, Advisory CISO, Cisco Systems, Inc.*
***Peter Romness**, Cybersecurity Solutions Lead - US Public Sector CT, Cisco Systems, Inc.*

Hacking and defense strategies are evolving at a rapid pace, and to truly understand them, students and professionals alike need hands-on interaction with the latest tools to hone their cybersecurity expertise. To help understand why cyber attacks occur and how to defend against them, Cisco Secure is hosting this Cyber Defense Clinic, a unique opportunity to work with an advanced set of automated, integrated cybersecurity technologies from multiple vendors. Participants will see popular hacking tools and gain experience defending critical data.

Security in the Shell (or, How I Learned to Think Before Forking) (separate registration is required)

Harborside Ballroom A, 4th Floor

Session Type: Additional Fee Program

Delivery Format: Preconference Workshop

Track:

***Ishan Abhinit**, Senior Security Analyst, Indiana University Bloomington*
***Mark Krenz**, Chief Security Analyst, Indiana University*

Although it is one of the oldest technologies in IT, the command line and terminal emulators continue to be in wide use for modern IT needs. Although people may think of these technologies as having a solid security footing, there are a number of ways someone can shoot themselves in the foot while using them, and I'm not just talking about running "rm -fr /". In this workshop, Mark Krenz, the creator of the popular Twitter account climagic, will demonstrate these and guide students through how to practice better command line security, from understanding the metadata that is generated by your favorite editor to knowing how to exploit SSH, knowing how to protect yourself when checking malware, and much more. There is something for everyone in this workshop, and you are sure to come away with a plethora of job-saving tips.

1:00 p.m. – 5:15 p.m.

Braindate

Harborside Foyer, 4th Floor

Session Type: Meeting

Delivery Format: Meeting

Track:

Braindates are about sharing knowledge. They are topic-driven conversations that you book with other participants, to have one-on-one or in small groups while you're at the Cybersecurity and Privacy Professionals Conference.

Braindate is sponsored by Menlo Security and Palo Alto Networks.

2:30 p.m. – 3:00 p.m.

Refreshment Break for Preconference Workshop Participants

Harborside Foyer, 4th Floor

Session Type: Break

Delivery Format: Break

Track:

3:00 p.m. – 4:00 p.m.

Higher Education Information Security Council (HEISC) Advisory Committee Meeting (by invitation only)

Dover AB, 3rd Floor

Session Type: Meeting

Delivery Format: Meeting

Track:

4:45 p.m. – 5:15 p.m.

Networking with Newcomers

Harborside Ballroom B, 4th Floor

Session Type: Meeting

Delivery Format: Meeting

Track:

***Sarah Reynolds**, Speaker Liaison, EDUCAUSE*

Whether it's your first time or your fifth time attending the conference, join us for our Networking with Newcomers, where first-time conference attendees will have the chance to mingle with returning conference attendees to learn how to make the best of the experience.

5:15 p.m. – 6:30 p.m.

Happy Hour Meet-Up Reception hosted by CrowdStrike

Laurel AB, 4th Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

Join the CrowdStrike team for a networking break with drinks, snacks, and casual conversations on what's going on in the world of cyber. We'll have members of our Executive Public Sector team on-site to take feedback on how we can improve our products for higher education.

Happy Hour Meet-Up Reception hosted by Gigamon

Kent AB, 4th Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

Join us and other conference attendees for drinks, snacks, and conversation around increasing network visibility and security while reducing risk, complexity, and cost. Come meet the Gigamon team and learn how you can safeguard your students, networks, resources, assets, and IP by gaining visibility into blind spots and east-west traffic.

Happy Hour Meet-Up Reception hosted by Netskope

Laurel CD, 4th Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

Netskope invites you to join your peers for drinks, snacks, and an evening of networking with other industry professionals. Chat with members of the Netskope team to learn more about how Netskope is redefining cloud, data, and network security with a market-leading security cloud platform that's fast and simple.

Wednesday, May 4

7:00 a.m. – 8:00 a.m.

Continental Breakfast - Sponsored by Fortinet

Harborside Foyer, 4th Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues for a light breakfast and network informally.

Click here for a message from Fortinet, the sponsor of this function.

7:00 a.m. – 6:00 p.m.

Braindate

Harborside Foyer, 4th Floor

Session Type: Meeting

Delivery Format: Meeting

Track:

Braindates are about sharing knowledge. They are topic-driven conversations that you book with other participants, to have one-on-one or in small groups while you're at the Cybersecurity and Privacy Professionals Conference.

Braindate is sponsored by Menlo Security and Palo Alto Networks.

7:15 a.m. – 5:00 p.m.

Registration Desk Open

Convention Registration, 3rd Floor

Session Type: Service Desk

Delivery Format: Service Desk

Track:

8:00 a.m. – 9:00 a.m.

Things You Learn the Hard Way from Doing 20 Years of Penetration Testing - Sponsored by Fischer Identity, Gold Partner

Grand Ballroom V-VI, 3rd Floor

Session Type: General Session

Delivery Format: General Session

Track:

Dave Aitel*, Partner, Cordyceps Systems*

The Cybersecurity and Privacy Professionals Conference opening general session speaker, Dave Aitel, will discuss long-term risk-mitigation strategies gleaned from decades of penetration testing. He will talk about which information security investments are needed and why, as well as how the landscape has changed over time.

Click here for a message from Fischer Identity, Gold Partner, the sponsor of this function.

9:00 a.m. – 6:00 p.m.

Corporate Displays

Harborside Foyer, 4th Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

Companies will be showcasing security technology solutions for higher education with dedicated visiting time scheduled during the morning and afternoon breaks. Stop by to learn more about their solutions and interact with company representatives.

Akamai Technologies

Akamai is the leading edge security platform for helping educational institutions provide secure, high-performing user experiences on any device, anywhere. The Akamai Intelligent Edge Platform provides extensive reach, coupled with unmatched reliability, security, visibility, and expertise to support the growing complexity of networks and applications.

BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

BIO-key International

More than 200 institutions trust BIO-key, an innovative provider of identity and access management (IAM) and identity-bound biometric solutions, including our award-winning PortalGuard platform, to reduce password reset calls by up to 95%, eliminate passwords, secure remote access, prevent phishing attacks, meet cyber insurance requirements, and improve productivity for the IT team.

CampusGuard

CampusGuard focuses on cybersecurity and compliance needs, with a team of responsive professionals who understand the requirements for protecting confidential and sensitive information. We also offer offensive security services, including vulnerability assessments, penetration/segmentation testing, and incident response plan testing. CampusGuard is certified Approved Scanning Vendor (ASV) and a Qualified Security Assessor Company (QSAC), and our team members hold a wide array of additional industry standard certifications.

Cisco Secure, Silver Partner

Cisco, the worldwide leader in enterprise cybersecurity, provides an open, integrated platform of products and services that accelerate IT initiatives. Cisco Secure is flexible, saves time, and is continuously updated and informed by the world's largest commercial threat intelligence team. Streamline detection, analysis, and response everywhere with intelligent automation and secure work, wherever it happens.

Corelight

Delivered by Corelight’s open NDR platform, our comprehensive, correlated evidence allows you to see and understand your network fully. Corelight evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.

CrowdStrike

Academic institutions need a solution that protects against all cyber threats, whether simple or sophisticated. CrowdStrike, a global cybersecurity leader, has redefined modern security with one of the world’s most advanced cloud-native platforms for protecting critical areas of enterprise risk: endpoints and cloud workloads, identity, and data.

Devo Technology

Devo is a cloud-native logging and security analytics platform empowering public-sector cybersecurity teams to log, detect, investigate, hunt, and stop threats to safeguard the nation. The platform provides unrivaled scale to collect all data, speed to give you immediate answers, and clarity to focus on the signals that matter.

Elastic

Elastic is a search-powered platform that maximizes data utility in real time for educational institutions. Higher education systems use our security solutions to achieve data-dependent use cases such as user behavior analysis, security investigations, and threat hunting. Deployable in the cloud or on-premises, Elastic delivers powerful insight, no matter the mission.

Fortinet

Fortinet secures the largest enterprise, service provider, government, and education organizations around the world. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments.

Fischer Identity, Gold Partner

Fischer Identity's 15 years of experience deploying identity for higher education provides our customers and partners with a solid and mature foundation to build and maintain successful identity programs. Fischer's tenure in higher education empowers institutions to deploy right-sized, affordable solutions focused on best practices for life-cycle management and identity security.

Identity Automation, Gold Parter

At Identity Automation, we understand the unique challenges that educators, faculty, students, and even parents face. That's why we created RapidIdentity, an identity and access management (IAM) platform used by hundreds of school districts, colleges, and universities to provide secure and agile online access that digitally connects students to their learning environment. By putting the unique identities of both educators and students at the heart of the learning process, RapidIdentity helps academic institutions unlock their potential and provide a safer, more personalized learning experience.

Indiana University OmniSOC

This display highlights the capabilities of the OmniSOC, the collaborative, shared cybersecurity operations center for higher education and research. Additional information will be provided by the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC), which serves member institutions within the higher education and research community.

Jamf

Jamf is the standard in Apple Enterprise Management (AEM). With more than 60,000 customers, Jamf is the only AEM solution of scale that remotely connects, manages, and protects Apple users, devices, and services. To learn more, visit www.jamf.com.

Moran Technology Consulting, Gold Partner

We enable transformative IAM programs and identity-focused cybersecurity solutions by providing assessments, strategic planning, roadmaps, platform selection, and implementation services. The MTC IAM Assessment Framework builds on international standards and InCommon's TAP reference architecture to assess and improve our clients' IAM programs: governance, operations, business processes, architecture, and technology.

NuHarbor Security

NuHarbor makes cybersecurity easier by eliminating the complexity and expense that make it hard. With deep security expertise and relationships with the best technology providers on the market, we are the industry's most comprehensive managed security provider. Clients trust us for strong and enduring protection.

Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

Rapid7

Rapid7 simplifies cybersecurity. With powerful automation and integrated threat intelligence from our industry-leading researchers and SOC analysts, our Insight Platform gives security teams the visibility they need to secure their environments, no matter the size or complexity. Don't just protect your business, drive it forward.

Splunk

Splunk is the data platform leader for security and observability. Our extensible data platform powers enterprise observability, unified security, and limitless custom applications. Splunk helps tens of thousands of organizations turn data into doing so they can unlock innovation, enhance security, and drive resilience.

Yakabod

Built for higher education, CISOBox (Yakabod Cyber Incident Manager) delivers efficient, secure information security incident management through intelligence agency–accredited technology. Colleges and universities use CISOBox to isolate and secure sensitive incident data, documentation, and communication; generate critical metrics; and gain NIST 800-61r2 compliance. And it now offers secure file sharing and ITSM integration!

Zscaler

Zscaler accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

9:15 a.m. – 10:00 a.m.

Creating Connections and Breaking Down Barriers with the Business Information Security Officer Role

Harborside Ballroom D, 4th Floor

Session Type: Breakout Session

Delivery Format: Facilitated Discussion

Track: Silo-Busting

***Janice Reese**, CEO, Network PDF Cloud*

***Amy Starzynski Coddens**, Strategic Partnerships Manager, Indiana University*

We have all heard the university Information Security Office referred to by many names, centered around the perception of the department of "no." In today's continually changing cyber threat landscape, strengthening the security objective through a business lens drives imperative change throughout organizations and across campuses. As information security continues to evolve to meet the cyber threats we face and the business needs of our organizations, new types of leadership roles are emerging. New security initiatives are most effective when they consist of technology and process. Business information security officers (BISOs) can assist in implementing the latest technology, helping define and operationalize the strategies working best within their unit. Meant to bridge the gap between security and the centralized CISO function, BISOs bring security initiatives from the CISO role and frame how that applies within the work done across units and schools on campus. The result is an understanding by those who are not always quick to adopt security initiatives and an opportunity for a more collaborative and communicative stasis. This session will provide a guided, thought-provoking conversation on the impact and role BISOs bring to develop cyber champions and advocates for security programs across higher education organizations. This session will cover what a BISO is and how to turn your security office from the office associated with "no" into the office of "collaboration."

Data Privacy Tech for Digital Learning and the LMS

Harborside Ballroom E, 4th Floor

Session Type: Breakout Session

Delivery Format: Demonstration

Track: Operations

***Kate McKain**, President & Co-founder, Willo Labs Inc.*

***Kyle Whitley**, Educational Technologist, University of Kansas*

LMS integrations with digital learning providers are one of the last unsecured sources of private data sharing between campuses and third parties. Learn how the University of Kansas is trading contracts for tech to lock down its digital learning PII with automated student anonymization and consent to share data.

Engaging and Developing the Cybersecurity Professional

Harborside Ballroom B, 4th Floor

Session Type:

Delivery Format: Presentation/Panel Session

Track:

***Sarah Brinker-Good**, Manager, Professional Learning, EDUCAUSE*

Since 2020, EDUCAUSE has been on a journey to create and enhance professional learning programs for cybersecurity and privacy professionals. Along the way, we have focused on the need for authentic learner engagement, modeling the way, and providing meaningful opportunities for choice in the online environment. Join us to hear about how professional pathways bring all the services together including mentoring, volunteering, micro-credentialing, and formal/informal learning. We'll conclude with a feedback discussion and ways of replicating and sharing the model.

How OmniSOC and REN-ISAC Joined Forces to Meet the Log4Shell Threat

Grand Ballroom I-III, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Silo-Busting

***Matthew Lutz**, Security Platform Engineer, Indiana University*

***Krysten S Stevens**, REN-ISAC Director of Technical Operations, Indiana University*

***Michael Davis**, REN-ISAC Principal Security Engineer, Indiana University*

***Rob Carlsen**, Lead Security Engineer, Indiana University*

The higher education and research threat landscape is complex and kaleidoscopic in nature, ever changing and unpredictable. The steady increase in both frequency and types of threats seen by our institutions, on top of the day-to-day challenges faced in the mission to ensure student success and support institutional research, highlights the importance and usefulness that membership in security organizations can serve. OmniSOC and REN-ISAC are on the frontlines of higher education and research's cybersecurity fight. Every day, these two premier cybersecurity organizations collaborate to protect the higher education and research communities and their members. In this session, team members from each organization will walk attendees through a behind-the-scenes look at what OmniSOC and REN-ISAC do individually, how they leverage their affiliation to best serve their members and

the community at large, and, most recently, how they expeditiously joined forces to address (and continue to address) the Log4Shell exploit.

Incorporating Social Engineering in Cybersecurity Education

Harborside Ballroom A, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Aunshul Rege**, Associate Professor, Director of the CARE Lab, Temple University*

Social engineering (SE) is a technique employed by cybercriminals that uses psychological manipulation to obtain sensitive information and gain unauthorized access to restricted areas or systems. Nearly 70% of US organizations experienced SE in 2017, resulting in a $2.76 million loss in operational downtime and revenues. The human factor is often regarded as the weakest link in cyberattacks, making SE a major concern for cybersecurity. Despite the significant threat posed by SE attacks, education, training, and general awareness of SE as a tool for cybercrime is low. This session examines one educator's efforts to incorporate SE into cybersecurity education via offering hands-on SE course projects, hosting a national collegiate SE cybersecurity competition, and providing educator workshops. This session will also address: (i) training students in the area of ethics, (ii) designing SE projects from the ground up with thorough instructions and rubrics, (iii) ensuring ethics compliance and risk management, (iv) developing partnerships with industry, government, and nonprofits, and (v) engaging the community to ensure equal accessibility to cybersecurity education, broadening participation from diverse domains. Enlarging and diversifying the pool of students learning (and teachers educating on) SE will cast a wider net to recruit the most talented students and foster their creative potential as they enter the cybersecurity workforce.

The Great Resignation and its Greatest Impacts to the Business

Grand Ballroom VII-IX, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Reet Kaur**, CISO, Portland Community College*

With the availability of vaccinations, there was a hope that business might become normal after having survived the tremors of huge financial losses and massive layoffs. However, organizations are experiencing the Great Resignation era, where millions of employees have either left or plan to leave their jobs. From a cybersecurity perspective, this is a significant business risk to the organization because whenever an employee leaves, you run the risk of your data, or access to it, leaving with them. Even when a worker parts ways with a company amicably, a vulnerability can arise if their access to your digital infrastructure is not efficiently terminated. Criminal hackers will try almost anything to get inside a profitable enterprise and secure a million-dollar payday from a ransomware infection. Apparently, now that includes Ransomware as a Service (RaaS) organizations that are emailing employees directly and asking them to unleash the malware inside their employer's network in exchange for a percentage of millions of dollars of ransom paid by the victim company. This has led the insider threat to become one of the critical risks to the organization that needs to be addressed quickly, before it's too late. This talk will focus on the risks and the steps organizations need to take to address and mitigate the risks caused by the Great Resignation.

Town Hall: Looking to the Future with the EDUCAUSE Strategic Plan

Essex A-C, 4th Floor

Session Type: Meeting

Delivery Format: Meeting

Track:

***Helen Norris**, Vice President & Chief Information Officer, Chapman University*

***John O'Brien**, President & CEO, EDUCAUSE*

***Nicole Marie McWhirter**, Chief Planning Officer, EDUCAUSE*

Join EDUCAUSE President and CEO John O'Brien, Board Chair Helen Norris, and Chief Planning Officer Nicole McWhirter in a discussion about the association's strategic planning process. Engage in this lively session focused on the EDUCAUSE commitment to a member-focused future, and be a part of clarifying and affirming the role EDUCAUSE plays and ensuring that our mission and vision are relevant and responsive to the challenges in a post-pandemic world. Come prepared to tell us what your hopes and dreams are for the future of EDUCAUSE!

10:00 a.m. – 10:45 a.m.

Refreshment Break and Corporate Displays

Harborside Foyer, 4th Floor

Session Type: Break

Delivery Format: Break

Track:

10:45 a.m. – 11:30 a.m.

Cybersecurity Provided at New Employee Orientation (NEO) and Beyond

Harborside Ballroom B, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Robert W Doyle**, Chief Privacy Officer/IT Compliance Officer, New Mexico State University*

All new employees at New Mexico State University (NMSU) must complete this training, making it a great place to see and present the idea of the institutional cybersecurity posture when they come into the organization. NEO is a daylong event. The morning session welcomes new employees to the NMSU community, introduces helpful offices, and provides essential information, including a session on cybersecurity and how it helps protect them and their data, and what to do if they are involved in a data breach and whom to contact. In addition, it provides the ability to let them know that cybersecurity is an institutional priority. This presentation will show what NMSU presents to new employees and how critical cybersecurity is to the organization and their personal lives. This is only a small part of NMSU's cybersecurity strategy, and other preparedness aspects can also be presented.

No Experience Needed: Addressing the Cybersecurity Skills Gap by Expanding Career Pathways

Harborside Ballroom E, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Workforce/Career Development

***Clar Rosso**, CEO, (ISC)2*

The security workforce gap stands at 2.72 million professionals globally, and the truth is that while there are plenty of available positions, there aren't enough qualified individuals to meet the industry's high demand and exacting standards. To make substantial progress toward narrowing this gap, the industry must widen its horizons by looking for talent who may not have direct experience but show an aptitude to learn on the job—such as those working in business, arts, or engineering. Bringing students, young professionals and career changers into cybersecurity careers at an entry level and setting them up on a pathway to success is essential for creating the growth the industry so desperately needs. However, the challenge for hiring managers becomes: How do we assess candidates' aptitude for and base knowledge of cybersecurity concepts if they have no direct experience? Until now, the cybersecurity industry has lacked a clear pathway for new entrants and career changers—unless a candidate had IT experience, it has been difficult for candidates to get their foot in the door. In this presentation, Clar Rosso, CEO of (ISC)², the world's largest nonprofit association of certified cybersecurity professionals, makes the case for establishing a clear and flexible pathway to cybersecurity careers, providing the audience with research-based insights, strategies, and tactics to galvanize efforts and bring more students and career changers into the profession.

Password Compromise Recovery: Partnering and Optimization

Harborside Ballroom A, 4th Floor

Session Type: Breakout Session

Delivery Format: Demonstration

Track: Operations

***Glenn Forbes Fleming Larratt**, Sr Security Engineer, Cornell University*

"We've just discovered over 1,000 compromised passwords" might be the first part of really unpleasant conversation. Learn how Cornell University's ITSO addressed this problem by partnering with stakeholders within and outside of IT, and got more efficient operations and better metrics through a custom web application.

Privacy in the Era of COVID-19: Lessons Learned

Harborside Ballroom D, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Silo-Busting

***Phil Reiter**, Associate Director, Privacy, University of Illinois at Urbana-Champaign*
***Mark A Werling**, Chief Privacy Officer, Indiana University*
***Joseph Gridley**, Chief Data Privacy Officer, University of Maryland*

Institutions of higher education are uniquely positioned to synthesize multiple datasets to enhance operational responses to a pandemic. Attend this panel to learn how the University of Maryland, Indiana University, University of Illinois Urbana-Champaign, and others used employee, student, and community data in their COVID-19 response efforts, including identifying hot-spots,

managing compliance, and supplementing contact tracing. Speakers will discuss the challenges faced in balancing individuals' privacy rights and expectations against their institutions' health and safety efforts. They will also explore their institutions' approach to using COVID-19 response data for generalizable research efforts, as well as lessons learned throughout the pandemic.

Security Recommendations for Science DMZs

Grand Ballroom I-III, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Kathy Benninger**, Manager of Networking Research, Pittsburgh Supercomputing Center*
***Mark Krenz**, Chief Security Analyst, Indiana University*

A Science DMZ is a special network architecture designed to improve the speed at which large science data transfers can be made. They have become a common solution to the issue of busy academic networks causing slowdowns or failures of large data transfers. A new paper published by Trusted CI on the security of Science DMZs provides an overview of this type of network architecture, summarizing the current best practice cybersecurity risk mitigations as well as providing additional security recommendations. This session is a brief introduction to the Science DMZ concept and presents an overview of the mitigations documented in the paper.

XR Security, Privacy, Safety, and Ethics Considerations in Higher Education

Grand Ballroom VII-IX, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Didier Contis**, Director Technology Services, Georgia Institute of Technology*
***Richard LaFosse**, Compliance and Policy Lead for Academic Innovation, University of Michigan-Ann Arbor*

This session provides an overview of critical XR security, privacy, safety, and ethical challenges that the higher education community will likely face in the short- to medium-term future. Drawing from the experiences with XR adoption at our respective institutions, as well as from collaborating with external advocacy groups—e.g., the XR Safety Initiative (xrsi.org) and the Immersive Learning Research Network's (iLRN) Champions in Higher Education for XR (CHEX) consortium—the presenters will offer insights and recommendations for navigating these challenges in the context of XR adoption in the teaching and learning environment. We will discuss critical security and privacy considerations when initiating and supporting XR initiatives and projects on campus. We will share the existing regulatory frameworks that impact XR learning experiences, with an emphasis on data privacy and security requirements. Our main intent is to encourage participants to engage with the broader higher education community and other relevant organizations to advocate on behalf of students (whether with vendors or policy makers) and support the development of an ethical framework of best practices for XR learning experience design and XR device and software procurement and management.

11:45 a.m. – 12:30 p.m.

Anonymous Shpanonymous: Not Your Grandmother's De-Identification Standards

Harborside Ballroom A, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Operations

***Scott Curtis Seaborn**, Privacy Officer, University of California, Berkeley*
***Pegah K Parsi**, Chief Privacy Officer, University of California San Diego*

If the difference between "de-identification," "pseudonymization," "anonymization," "aggregation," and other disclosure limitation methods is confusing for you, you're not alone! There is a lot of confusion in higher ed related to disclosure limitation methods. De-identification is a statistically rigorous process, unique to each situation, and "de-identified" datasets do not remain statically so. In this session, we'll discuss what each of these terms means, how they are (or aren't!) defined by law, and why our old disclosure limitation methods might not be appropriate for today's data-driven world. We will chat about challenges for various academic disciplines, strategies campuses have employed to provide clarity, and whether anonymization is truly possible. This session is especially useful for researchers, data custodians, research IT professionals, privacy professionals, IRB members, and those involved in their university's open scholarship/research initiatives.

HECVAT 2022 Updates

Grand Ballroom I-III, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Charles Escue**, Extended Information Security Manager, Indiana University*
***Brian Kelly**, Director of the Cybersecurity Program, EDUCAUSE*
***Joshua Callahan**, Information Security Officer and CTO, Humboldt State University*
***Jon Allen**, Associate Vice President CIO & CISO, Baylor University*
***Nick Lewis**, Program Manager, Security and Identity, Internet2*
***Sheryl Swinson**, IT Strategy Business Analyst, Indiana University Bloomington*

The higher education information security community and HECVAT working group worked together to launch the HECVAT to outer space and a HECVAT 3.0 release! Our session this year will go over the major HECVAT 3.0 update, future plans, and ask for your input into where to develop HECVAT in the future. We'll also go over where we need you to get involved to build more resources for the community and the service providers that support us.

Taking CMDB to the Next Level by Capturing Data Inventory on Assets that Will Automate GRC Efforts

Harborside Ballroom D, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Damon Armour**, Director of Information Security, Risk & Assurance, North Carolina State University*
***Chris Bradsher**, Information Security Analyst, North Carolina State University*

***Gary Li**, Director, Infrastructure Platform & Services, North Carolina State University*
***Mike Donathan**, Sr. ServiceNow Developer, North Carolina State University*
***Dan Grigg**, IT Project Manager II, North Carolina State University*

To improve compliance, IT risk management, and IT support within our decentralized IT structure at NC State University, our Office of Information Technology (OIT) is working with cross-campus IT stakeholders to establish a central inventory within our ServiceNow Configuration Management Database (CMDB). NC State is expanding this resource inventory to include data from all relevant IT assets. This inventory expansion has required customization to reflect how NC State leverages its data classification scheme. The data inventory will empower the business, IT support, compliance, and risk management teams a full understanding of compliance obligations, levels of sensitivity, and the data governance responsible for that data. This inventory expansion will also enable the institution's governance, risk, and compliance (GRC) tools to leverage that data to perform automated compliance attestations with the appropriate stakeholders, improve the use of risk management efforts, and enable the university's internal audit organization to improve its scope for audit plans. This project is kicking off in 2022 with proofs of concept being conducted within OIT along with the IT support group from the Division of Academic and Student Affairs. Full campus use is estimated by fall 2022.

11:45 a.m. – 12:45 p.m.

China's Personal Information Protection Law: Lessons for Compliance

Harborside Ballroom B, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Hunter Dorwart**, Policy Counsel, Future of Privacy Forum*

China's Personal Information Protection Law raises some novel compliance challenges for universities, vendors, and other controllers in a range of industries. While the PIPL shares many similarities with the GDPR and other global privacy laws, it diverges from this standard in a number of key ways. This session will provide an examination of the major differences between the PIPL and the GDPR to better help compliance officers modify their global privacy programs and better situate how privacy experts should approach the law. It will also identify minor differences and nuances with the GDPR as well as explain key enforcement trends and lessons for companies on China's unique administrative and regulatory system.

Learn by Doing: Recognizing Student Accomplishments in a Student-Enabled Security Operations Center

Grand Ballroom VII-IX, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Workforce/Career Development

***Jan Vazquez**, Information Security Analyst, California Polytechnic State University, San Luis Obispo*
***Douglas Lomsdalen**, Information Security Officer, California Polytechnic State University, San Luis Obispo*

According to numerous sources, the United States is experiencing a worker shortage in the cybersecurity field. To ensure our students have a leg up in the job hunt, it is the primary goal of the California Polytechnic State University's Information Security Office to ensure our students are ready and have a good start on filling their "security toolkit." Our hiring approach takes any

student passionate about cybersecurity and trains them to be the university's first line of defense in our Security Operations Center. Using our university's learning philosophy of "Learn by Doing," we've developed a training program to get the students up to speed and secure the campus quickly. We have a formal mentoring program and acknowledge students' accomplishments through a home-grown badging program.

This Job Feels Just Right: Finding Your Niche in Cybersecurity

Harborside Ballroom E, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Workforce/Career Development

***Carolyn A. Ellis**, CMMC Program Manager, University of California San Diego*
***Amy Starzynski Coddens**, Strategic Partnerships Manager, Indiana University*
***Krysten S Stevens**, REN-ISAC Director of Technical Operations, Indiana University*

Daily we hear about the need for cybersecurity talent, and yet we also hear stories about people at all levels who are not always able to find their fit. They include graduates trying to get their foot in the cyber door; to mid-level professionals with technical and non-technical skills looking to cybersecurity for a new career path; and seasoned leaders looking for a change. Is the issue the applicants, or is it the unchanged system they are trying to enter? In this session, we will address how applicants and hiring managers can move beyond the typical hiring process, start building up our cybersecurity resources, and enhance the makeup of our most valuable assets—our teams.

12:30 p.m. – 1:45 p.m.

Lunch - Sponsored by Moran Technology Consulting, Gold Partner

Grand Ballroom V-VI, 3rd Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues to eat lunch and network informally.

***Click here* for a message from Moran Technology Consulting, Gold Partner, the sponsor of this function.**

1:45 p.m. – 2:30 p.m.

Choosing the Road Less Traveled: One Institution’s Path to Privacy Compliance

Harborside Ballroom B, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Sean McKay**, Chief Information Security Officer, Portland State University*
***Max R.D. Parmer**, Information Security Analyst, Portland State University*

With the start of GDPR enforcement beginning in May 2018, the Information Security Office, Office of General Counsel and registrar developed a nascent awareness of the need to understand GDPR and to respond to the developing trends in global and US policy making and legislation that GDPR represents. Although appeals to the University Policy Committee in 2019 were based on normative research on the practices of peer universities and industry demonstrating the significance and need for formulating a specific and actionable privacy program, an overwhelming ambivalence prevailed. In early 2020, on the eve of the pandemic, with sponsorship from general counsel, PSU's IT and Information Security Office finally found a workable formula to build engagement across the key campus communities and to develop and implement a privacy program just in time before significant contractual impacts came to bear. With a DPO on board after two years of effort, and a year of policy process, we were ultimately successful in having our policy adopted. In this presentation we will walk you through the challenges, steps and tactics to drive adoption of a policy program from an IT risk and compliance team.

Increasing Security While Lowering the Tech Burden on End Users in a Modern IDP

Harborside Ballroom A, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Silo-Busting

***Jeremy Matthew Livingston**, CISO, Stevens Institute of Technology*
***Rafat Azad**, Cybersecurity Engineer, Stevens Institute of Technology*

Discuss the transformation of identity management at Stevens Institute of Technology in the wake of a ransomware attack. We'll outline the additional security of implementing a new IDP while making it easier for users to connect to needed services with adaptive MFA and SSO. Discuss the yearlong process to implement Okta and the benefits of automation in the account management process. As identity and access management are evolving into a security function for universities and businesses, this discussion can also cover some of those nuances.

Introducing Annual Cybersecurity Assessments to an Obstreperously Decentralized Campus

Harborside Ballroom D, 4th Floor

Session Type: Breakout Session

Delivery Format: Demonstration

Track: GRC for Privacy and Cybersecurity

***Cornelia Ann Bailey**, Director, Information Assurance, University of Chicago*
***Gabriel McElwain**, IT Risk Analyst, University of Chicago*
***Jessica Abra Sandy**, IT Risk Analyst, University of Chicago*

We will share lessons learned from launching the first campus-wide cybersecurity assessment program for the University of Chicago’s decentralized IT environment. We will describe the ways in which we: defined program scope, modeled our organization’s structure, identified units’ data assurance levels, selected an assessment tool and an assessment framework, created a communications strategy to incentivize unit participation, developed executive reporting requirements, and addressed feedback from unit IT staff, all while planning to expand our assessment process into a customizable certification program. We’ll discuss some assumptions we made at the outset, which ones proved true, and what’s next for our annual assessment program.

The Convergence of Cybersecurity and Data Privacy in Higher Education

Harborside Ballroom E, 4th Floor

Session Type: Breakout Session

Delivery Format: Facilitated Discussion

Track: GRC for Privacy and Cybersecurity

***Bhavesh Vadhani**, Principal, Cybersecurity, Technology Risk, and Privacy Leader, CohnReznick*

***Deborah Nitka**, Manager, Cybersecurity, Technology Risk, & Privacy Practice, CohnReznick*

At its most basic level, privacy has historically been defined as the right to be left alone. As higher education institutions become increasingly digital, the concept of data privacy has come to mean accountability for how personal information is used by institutions that collect it. Once the data resides on enterprise systems, a connection between data privacy and cybersecurity is formed. The institution is accountable for designing cybersecurity controls and programs that protect information from theft, unauthorized access, and damage.

Welcome to the Higher Education Cybersecurity and Privacy Community from EDUCAUSE, Internet2, and REN-ISAC

Grand Ballroom I-III, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Silo-Busting

***Susan Coleman Snyder**, Assessment Program Manager, Indiana University Bloomington*

***Nick Lewis**, Program Manager, Security and Identity, Internet2*

***Brian Kelly**, Director of the Cybersecurity Program, EDUCAUSE*

This panel discussion will focus on how Internet2, REN-ISAC, and EDUCAUSE work collaboratively and independently to provide support for cybersecurity professionals. The presenters will provide an update and showcase initiatives, projects, and resources each organization provides to the community and how they all collaborate.

What Will You Do Tomorrow? Career Path AMA with Higher Ed IT Leaders

Grand Ballroom VII-IX, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Workforce/Career Development

***Kirk Kelly**, Vice President for Information Technology and CIO, Portland State University*

***Patricia M Clay**, Chief Information Officer, Hudson County Community College*

***Cathy Hubbs**, Chief Information Security Officer, American University*

***Vijay Menta**, Vice President & CIO, Middlebury College*

Have you ever had a career or leadership question but didn't know who to ask? Are you considering your next career move, or wondering how to develop the skills to progress in your career? If this is you, join us for a fun, engaging session with dynamic and experienced IT leaders from across the higher education community. From questions about career progression and leadership development, to succession planning, management tips, and the future of careers in security and privacy, this Ask Me Anything (AMA) session will allow you to ask about the career path and leadership topics that you care about most. This unscripted session is designed to help young and early-career professionals, or professionals considering a jump from a technical role to a leadership role, get advice and insight in an informal setting.

2:30 p.m. – 3:15 p.m.

Dessert, Refreshment Break, and Corporate Displays

Harborside Foyer, 4th Floor

Session Type: Break

Delivery Format: Break

Track:

***Sarah Reynolds**, Speaker Liaison, EDUCAUSE*

3:15 p.m. – 4:00 p.m.

One Network Evidence Library: An Industry of Detection and Response

Harborside Ballroom A, 4th Floor

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Kevin Kerber**, Regional Sales Manager, Corelight Inc*
***Rob Carlsen**, Lead Security Engineer, Indiana University*

Transform network and cloud traffic into evidence so that data-first defenders can stay ahead of ever-changing attacks. Our belief is that a global community of contributors leveraging Zeek and Surricata, whether open-source or via Corelight, can establish a standard library of network evidence for security teams that is second to none, a library that can be easily leveraged by an industry of detection and response (XDR) platforms and teams. Rob Carlsen, Lead Security Engineer at OmniSOC, will discuss this approach and review how OmniSOC leverages this approach with review of real investigations within their member organizations.

Securing Remote Access In Higher Ed

Harborside Ballroom B, 4th Floor

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Heather Wasserlein**, VP Product Management, Apporto*
***Nick Cavalancia**, Microsoft MVP & CEO, Techvangelism*
***Antony Awaida**, CEO, Apporto*

Many educational institutions have relied on VPNs to establish communication and connectivity between staff and organizational resources during and after the pandemic. However, with the rise of sophisticated threat actors, VPNs have become the most likely entry point for malware and ransomware.

Securing the Airwaves: The New Trust Frontier

Grand Ballroom VII-IX, 3rd Floor

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Daniel Basile**, Chief Information Security Officer, Texas A&M University*
***Neal Tilley**, Education Advisor, Cisco Systems, Inc.*

More and more universities are implementing multiple mobility solutions across wider areas to meet student, research, and community requirements. This includes Wi-Fi 6 (indoor and outdoor) 5G (public/private), some using 5G in a box/AAS through providers. Given the increased need of tougher compliance, a CISO needs to work closely with their infrastructure and telecommunication teams. This session looks from a CISO's perspective. What are the best strategies? How will micro segmentation and zero trust need to be supported across the wireless footprint in this future? And how that will be critical to support CMMC 2.0 imperatives as we move forward? Daniel Basile, CISO for Texas A&M's RELLIS campus, leads this discussion with assistance from Neal Tilley, Cisco's higher education strategic advisor and coordinator of Cisco's Research & CISO advisory councils.

Town Hall: Looking to the Future with the EDUCAUSE Strategic Plan

Essex A-C, 4th Floor

Session Type: Meeting

Delivery Format: Meeting

Track:

***Nicole Marie McWhirter**, Chief Planning Officer, EDUCAUSE*
***John O'Brien**, President & CEO, EDUCAUSE*
***Helen Norris**, Vice President & Chief Information Officer, Chapman University*

Join EDUCAUSE President and CEO John O'Brien, Board Chair Helen Norris, and Chief Planning Officer Nicole McWhirter in a discussion about the association's strategic planning process. Engage in this lively session focused on the EDUCAUSE commitment to a member-focused future, and be a part of clarifying and affirming the role EDUCAUSE plays and ensuring that our mission and vision are relevant and responsive to the challenges in a post-pandemic world. Come prepared to tell us what your hopes and dreams are for the future of EDUCAUSE!

Understanding the Assignment: Defending Against Ransomware

Harborside Ballroom E, 4th Floor

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: Operations

***Bryan Green**, CISO, Americas, Zscaler*

The education industry has unceremoniously emerged as the second most common target for ransomware. In 2020, at least 1,681 schools, colleges, and universities of all sizes and prestige were infected. Institutions face the difficult challenge of preserving academic freedom, easy access to information, and open collaboration while defending from threat actors who exploit these same characteristics. The acceleration of public cloud, Software as a Service, and the Internet of Things add additional layers of complexity and new cybersecurity challenges. This session will examine the characteristics that make higher education uniquely vulnerable to ransomware and why these institutions innately have a large attack surface. We'll explore challenges with legacy network architectures and why they have limited efficacy in preventing compromise. We'll then discuss how existing technology infrastructure can be transformed to a Zero Trust model to mitigate threats and scale to cloud native architectures.

Untangling "Security Spaghetti": How Virginia Community College System Automated Identity Management

Harborside Ballroom D, 4th Floor

Session Type: Industry Led

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Tim Till**, Principal Sales Consultant, Identity Automation*

With continuous strands of students and staff moving in and out of Virginia Community College System's (VCCS) network of 23 colleges, identity management can quickly become a tangled web. Identity-related tasks, such as delegating administrative access to critical systems and managing access for guests, contractors, and other third-party affiliates, simply aren't manageable at scale—without the right technology. So, when it came time to roll out multi-factor authentication (MFA) across the entire system, VCCS seized the opportunity to initiate digital transformation by migrating off of its legacy identity and access management (IAM) solutions. Discover how VCCS untangled its "security spaghetti" with a cloud-based IAM platform that automated the full identity lifecycle across the community college system's dynamic and fluid population of over 1 million identities and more than 200,000 active users. Attendees of this session will learn how modern IAM strengthens security, drives operational efficiencies, and delivers visibility and reporting on identity and access activities.

We Need to Talk About Ransomware

Grand Ballroom I-III, 3rd Floor

Session Type: Industry Led

Delivery Format: Demonstration

Track: Awareness and Education

***Brian S Dennis**, Principal Technologist-Public Sector, Akamai Technologies, Inc.*

***Douglas Holland**, Sr. Solutions Engineer, Akamai Technologies, Inc.*

By the end of 2021, ransomware is predicted to attack a business every 11 seconds. Novel, large-scale attacks that are nearly impossible to anticipate. SolarWinds, Kaseya, and Log4J reveal global vulnerability to sophisticated, state-sponsored attacks. In

this session we'll delve into the anatomy of a ransomware attack, show you how an attacker gains a foothold in your environment, and give you some strategies to lessen the severity of a ransomware attack, or prevent one altogether.

4:15 p.m. – 5:00 p.m.

An Analysis of 350 HECVAT Vendor Assessments Across 40 EDUs

Harborside Ballroom E, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Andrew Scheifele**, Co-Founder and CEO, Salty Cloud PBC*

***Cam Beasley**, Chief Information Security Officer, University of Texas at Austin*

The HECVAT is a widely used vendor assessment questionnaire created by the HEISC Shared Assessment Working Group. It is currently in its third major version. Last year at #CybersecPrivacy21 we presented summary data from over 200 completed HECVAT assessments, including analysis by categories, vendor verticals, and across specific high/critical weighted controls. This year we will expand the dataset analysis to include over 350 completed HECVATs from 40 separate EDUs with a continued focus on benchmarking vendor response to guide EDUs in HECVAT review, analysis, and interpretation. We will also do a subset analysis on the initial set of HECVAT v3s to provide an early comparative dataset for EDUs to use as a benchmark for interpretation of this latest HECVAT version. HECVAT assessments were collected and shared by EDUs in IsoraLite, a free-to-EDU assessment platform that allows EDUs to collect, manage, and view HECVATs and supporting documentation, as well as to share HECVATs with other EDUs. Since the rollout of IsoraLite by the University of Texas at Austin Information Security Office and Salty Cloud PBC at #SECURITY19, over 750 EDU users across 350+ EDUs have accessed IsoraLite to collect, view or otherwise manage HECVAT vendor assessments. Finally, we will also discuss EDU-specific examples of using the HECVAT assessment as part of a broader vendor risk management program, including implementing and maturing a vendor risk management program based on HECVAT at UT Austin.

Bridging the Research and Compliance Communities

Harborside Ballroom B, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Silo-Busting

***Claire Mizumoto**, Director, Research IT Services, University of California San Diego*

***Michael Corn**, CISO, University of California San Diego*

***Jackie Milhans**, Associate Director, Research Computing Services, Northwestern University*

***Carolyn A. Ellis**, CMMC Program Manager, University of California San Diego*

The cornerstones of modern research are collaboration, agility, entrepreneurship, and creativity. Yet institutions increasingly face expanding and rigorous security compliance regimes from both sponsoring agencies and commercial partners. Many universities are struggling to marry new security compliance obligations with active research programs, while avoiding throttling scientific exploration. Achieving this requires shedding historical preconceptions of compliance and security, and a broader understanding of the research mission. This interactive panel explores successes and challenges of Northwestern University and University of

California, San Diego when handling research compliance projects. Learn how to cultivate a culture with a shared vision for the research and compliance partnership.

Building Information Security Strategy: Lessons Learned

Harborside Ballroom D, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Saby Waraich**, CIO, Clackamas Community College*

Are you struggling to decide how to prioritize your scarce information security resources? How do you move from a reactive approach to security toward a proactive approach with strategic planning? A good strategy considers the full spectrum of information security, including people, processes, and technology. Security decisions should be made based on the security risks facing your organization, not just on “best practices." Your information security strategy should demonstrate the alignment between business goals and strategies. We will share our journey of building an information security strategy that helped us to get buy-in from our executive leadership and helped create an information security road map.

Framework for the Future: Connect Dots and Build Bridges with the New CIS Controls

Grand Ballroom VII-IX, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Randy Marchany**, University IT Security Officer, Virginia Tech*
***Cara Bonnett**, Technology Risk Assurance Manager, Duke University*

The Center for Internet Security (CIS) Critical Controls got a major rewrite in 2021, reflecting core changes in today's computing and infrastructure environments. This presentation will highlight what’s new in version 8, why it’s well-suited for higher ed, and how two universities are using the updated framework to gain new risk insights and improve security across siloes. The CIS framework maps to a wide range of other formal frameworks (NIST 800-171/CUI, HIPAA, PCI-DSS, among others) and is measurable, specific, and practical to operationalize, which can help identify and prioritize quick wins for tight budgets. Recent research shows that adopting CIS’ basic set of recommendations defends against 78 percent of the most common attack techniques.

Making Use of External Cybersecurity Information at Institutions of Higher Education of All Shapes and Sizes

Grand Ballroom I-III, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Operations

***Harry Hoffman**, AVP/CISO, Northeastern University*
***Darryl McGraw**, CIO, William Peace University*
***Mark F Herron**, CISO, Case Western Reserve University*

***Juha Haag**, Arctic Engineer, Arctic Security*

Gathering and taking action on external cybersecurity information about your organization offers a number of benefits, such as prevention of security incidents, a better understanding of the security posture and exposure, and insights into organizational security practices. This mostly untapped source of relevant and useful information regarding potential compromises and cybersecurity vulnerabilities is available and accessible for institutions of higher education. However, the universities and colleges that would be the consumers of the information truly come in all shapes and sizes. Some come with sizable security teams, but many who need this information do not have enough cybersecurity expertise or awareness to go look for it, let alone gather it and then quickly turn it into something useful in their daily struggle for a safe operating environment. In addition, the IT teams in smaller institutions might not have security-focused people, and if they do, they might not have the financial resources or management support to expand their efforts. So what can be done? In the past year-and-a-half, Arctic Security and EDUCAUSE have conducted research projects to study this topic and document the obstacles and effects of getting this information out to benefit higher education. Our panelists come from institutions both small and large, local and distributed, research and teaching focused. They will share their experiences and insights gathered as they started down on this path.

Protecting CUI and Simplifying Compliance with CMMC 2.0, NIST 800-171, and ITAR

Harborside Ballroom A, 4th Floor

Session Type: Breakout Session

Delivery Format: Demonstration

Track: GRC for Privacy and Cybersecurity

***Raluca Ada Popa**, Associate professor at UC Berkeley and Co-founder at PreVeil, PreVeil*
***Katrina Biscay**, CISO, University of Cincinnati*
***Sanjeev Verma**, CEO, PreVeil*

The Department of Defense's (DoD) Cybersecurity Maturity Model Certification (CMMC) framework has undergone significant changes, and CMMC's implementation has been delayed until 2023. Until then, universities still need to comply with NIST 800-171, developed specifically to protect CUI. Further, university employees that exchange CUI with people in foreign countries (researchers, for example) need to comply with the State Department's ITAR regulations governing such communications. One key change that simplifies CMMC compliance is that DoD has aligned the requirements for the new CMMC 2.0 Level 2 with NIST 800-171, which has been in effect since 2017. Level 2 will indicate that an organization is able to securely store and share CUI. Key changes to the State Department's ITAR regulations that make them easier to comply with are that the exchange of CUI across borders is now permitted as long as the data is end-to-end encrypted, and no cloud services provider has access to keys, network access codes, or passwords that enable decryption. This panel will include a professor of computer science, a university CISO, and a cybersecurity industry expert. Their focus will be on how platforms built on modern cybersecurity principles can facilitate compliance with federal regulations governing CUI. The institutional use case will highlight practical steps to take toward compliance. The aim of the panel is to help your institution achieve CMMC Level 2 certification.

5:00 p.m. – 6:00 p.m.

Networking Reception

Harborside Foyer, 4th Floor

Session Type: Reception

Delivery Format: Reception

Track:

One of the most valuable aspects of this conference is the opportunity to connect face-to-face with fellow attendees. Join us for the reception, where you can relax over food and drink and get to know your colleagues. A cash bar will be available; each attendee will receive one drink ticket.
NOTE: Please wear your name badge for admittance.

8:00 p.m. – 11:59 p.m.

Get Your Game On! - Sponsored by ThreatLocker

Grand Ballroom V-VI, 3rd Floor

Session Type: Activity

Delivery Format: Activity

Track:

***Beth Fossum**, PM, CTI Meeting Technology*
***Sarah Reynolds**, Speaker Liaison, EDUCAUSE*

Join us for the eighth annual Cybersecurity and Privacy Professionals Conference game night! This is a great way to get to know your fellow conference-goers in a relaxed atmosphere. No experience necessary; we'll be sure to have something for everyone, from casual party games to serious board games. Games will startup throughout the evening so come by whenever you like. Grab a chair and get your game on!

Click here for a message from ThreatLocker, the sponsor of this function.

Thursday, May 5

7:00 a.m. – 8:00 a.m.

Continental Breakfast - Sponsored by Trellix

Harborside Foyer, 4th Floor

Session Type: Meal

Delivery Format: Meal

Track:

Join colleagues for a light breakfast and network informally.

Click here for a message from Trellix, the sponsor of this function.

7:00 a.m. – 10:30 a.m.

Braindate

Harborside Foyer, 4th Floor

Session Type: Meeting

Delivery Format: Meeting

Track:

Braindates are about sharing knowledge. They are topic-driven conversations that you book with other participants, to have one-on-one or in small groups while you're at the Cybersecurity and Privacy Professionals Conference.

Braindate is sponsored by Menlo Security and Palo Alto Networks.

7:15 a.m. – 8:00 a.m.

2023 Program Committee Breakfast (by invitation only)

Dover AB, 3rd Floor

Session Type: Meal

Delivery Format: Meal

Track:

7:15 a.m. – 11:00 a.m.

Registration Desk Open

Convention Registration, 3rd Floor

Session Type: Service Desk

Delivery Format: Service Desk

Track:

8:00 a.m. – 8:45 a.m.

Best Practices for Managing Cybersecurity Risks: An Urgent Call for Higher Ed Partnerships

Grand Ballroom I-III, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Bruce Maas**, Honorary Fellow-Information School, University of Wisconsin-Madison*

***Vincent Scheivert**, Director of Technical Strategy, SLED, Telos Corporation*

Higher education is a major target of bad actors in cybersecurity: Stealing student information. Exposing the private files of trustees and executive leadership. Hacking into researchers' intellectual property. Accessing an old, unpatched server to expand horizontally and hold hostage the institution's most critical IT assets. Everything is at risk. University leaders are increasingly challenged to balance their responsibility to identify and manage cyber risks with their mission to deliver high-quality research, teaching, and service. Universities have diverse constituencies along with governance that has been designed to ensure all stakeholders have a voice. This session will present the best practices for managing cybersecurity risks in higher education featuring Bruce Maas, retired CIO and vice provost for IT at UW-Madison, and a past EDUCAUSE board member; and Vincent

Scheivert, director of technical strategy at Telos Corp., an established cybersecurity company that has newly entered the higher education market.

Enough Talk! Making Security and Privacy Reviews Practical and Effective

Harborside Ballroom D, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Operations

***Pegah K Parsi**, Chief Privacy Officer, University of California San Diego*
***Isaac Straley**, Chief Information Security Officer, University of Toronto*

Do security and privacy assessments provide real value to researchers? We think so! And we want to show you how it can be done. Join us for an engaging conversation where a CPO and CISO collaborate with university leaders and researchers to enable a project to move forward. One important aspect of any security and privacy professional's role is to review and advise on university projects. Our CISO and CPO will talk through the security and privacy needs of a real-world project, including due diligence in vendor assessments. Attendees will become familiar with the value security and privacy professionals bring to the table with a real-world example.

Risky Business: Defending Universities at Scale

Harborside Ballroom B, 4th Floor

Session Type: Breakout Session

Delivery Format: Facilitated Discussion

Track: Silo-Busting

***Micah Czigan**, CISO, Georgetown University*
***Tina Thorstenson**, VP, Industry Business Unit, CrowdStrike*

Join two experienced university CISOs for a discussion on how they have implemented successful cybersecurity strategies. While creating a holistic cybersecurity plan can sometimes feel like a daunting task, building on two main pillars has helped guide our leaders, and they are here to share their stories and best practices. A main principle is to view cybersecurity as risk management, to assess, identify, and make informed decisions based on real-world threat intelligence. Another guiding principle is that cybersecurity takes a village and is about every person, every department being part of their school's cybersecurity success. We'll share how this extends beyond building bridges internally across the university to extended service and technology providers as well. Micah Czigan, CISO of Georgetown University, and Tina Thorstenson, former ASU deputy CIO and CISO, chat about key successful strategies for navigating today's complex university environment and the challenges of today's threat landscape.

Trailblazing the AI for Cybersecurity Discipline: Overview of the Field and Promising Directions

Harborside Ballroom A, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Sagar Samtani**, Assistant Professor, Indiana University*

In this talk, I will be summarizing the state of AI for cybersecurity and its promising future directions. I will also provide examples of recent research at the intersection of AI and cybersecurity. Finally, I will summarize promising mechanisms to help practitioners and academics make significant headway in tackling these grand AI for cybersecurity issues. Selected discussions around these mechanisms will include emerging conferences and journals to archive research, educational opportunities to help cultivate the next generation of "cyber AI" professionals, and federal funding opportunities to help financially support systematic streams of research and education for AI for cybersecurity.

Zero Trust: It's a Concept, Not a Product

Grand Ballroom VII-IX, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Operations

***Joel Rosenblatt**, Director, Computer and Network Security, Columbia University*

We have all been getting email from vendors selling the latest and greatest security product—Zero Trust. The problem is that you cannot buy zero trust, you have to build it. My talk will explain what it really is and how you can create a zero trust environment.

8:30 a.m. – 10:30 a.m.

Corporate Displays

Harborside Foyer, 4th Floor

Session Type: Industry Led

Delivery Format: Industry Led

Track:

Companies will be showcasing security technology solutions for higher education with dedicated visiting time scheduled during the morning break. Stop by to learn more about their solutions and interact with company representatives.

Akamai Technologies

Akamai is the leading edge security platform for helping educational institutions provide secure, high-performing user experiences on any device, anywhere. The Akamai Intelligent Edge Platform provides extensive reach, coupled with unmatched reliability, security, visibility, and expertise to support the growing complexity of networks and applications.

BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

BIO-key International

More than 200 institutions trust BIO-key, an innovative provider of identity and access management (IAM) and identity-bound biometric solutions, including our award-winning PortalGuard platform, to reduce password reset calls by up to 95%, eliminate passwords, secure remote access, prevent phishing attacks, meet cyber insurance requirements, and improve productivity for the IT team.

CampusGuard

CampusGuard focuses on cybersecurity and compliance needs, with a team of responsive professionals who understand the requirements for protecting confidential and sensitive information. We also offer offensive security services, including vulnerability assessments, penetration/segmentation testing, and incident response plan testing. CampusGuard is certified Approved Scanning Vendor (ASV) and a Qualified Security Assessor Company (QSAC), and our team members hold a wide array of additional industry standard certifications.

Cisco Secure, Silver Partner

Cisco, the worldwide leader in enterprise cybersecurity, provides an open, integrated platform of products and services that accelerate IT initiatives. Cisco Secure is flexible, saves time, and is continuously updated and informed by the world's largest commercial threat intelligence team. Streamline detection, analysis, and response everywhere with intelligent automation and secure work, wherever it happens.

Corelight

Delivered by Corelight's open NDR platform, our comprehensive, correlated evidence allows you to see and understand your network fully. Corelight evidence allows you to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.

CrowdStrike

Academic institutions need a solution that protects against all cyber threats, whether simple or sophisticated. CrowdStrike, a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk: endpoints and cloud workloads, identity, and data.

Devo Technology

Devo is a cloud-native logging and security analytics platform empowering public-sector cybersecurity teams to log, detect, investigate, hunt, and stop threats to safeguard the nation. The platform provides unrivaled scale to collect all data, speed to give you immediate answers, and clarity to focus on the signals that matter.

Elastic

Elastic is a search-powered platform that maximizes data utility in real time for educational institutions. Higher education systems use our security solutions to achieve data-dependent use cases such as user behavior analysis, security investigations, and threat hunting. Deployable in the cloud or on-premises, Elastic delivers powerful insight, no matter the mission.

Fortinet

Fortinet secures the largest enterprise, service provider, government, and education organizations around the world. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments.

Fischer Identity, Gold Partner

Fischer Identity's 15 years of experience deploying identity for higher education provides our customers and partners with a solid and mature foundation to build and maintain successful identity programs. Fischer's tenure in higher education empowers institutions to deploy right-sized, affordable solutions focused on best practices for life-cycle management and identity security.

Identity Automation, Gold Parter

At Identity Automation, we understand the unique challenges that educators, faculty, students, and even parents face. That's why we created RapidIdentity, an identity and access management (IAM) platform used by hundreds of school districts, colleges, and universities to provide secure and agile online access that digitally connects students to their learning environment. By putting the unique identities of both educators and students at the heart of the learning process, RapidIdentity helps academic institutions unlock their potential and provide a safer, more personalized learning experience.

Indiana University OmniSOC

This display highlights the capabilities of the OmniSOC, the collaborative, shared cybersecurity operations center for higher education and research. Additional information will be provided by the Research and Education Networks Information Sharing and Analysis Center (REN-ISAC), which serves member institutions within the higher education and research community.

Jamf

Jamf is the standard in Apple Enterprise Management (AEM). With more than 60,000 customers, Jamf is the only AEM solution of scale that remotely connects, manages, and protects Apple users, devices, and services. To learn more, visit www.jamf.com.

Moran Technology Consulting, Gold Partner

We enable transformative IAM programs and identity-focused cybersecurity solutions by providing assessments, strategic planning, roadmaps, platform selection, and implementation services. The MTC IAM Assessment Framework builds on international standards and InCommon's TAP reference architecture to assess and improve our clients' IAM programs: governance, operations, business processes, architecture, and technology.

NuHarbor Security

NuHarbor makes cybersecurity easier by eliminating the complexity and expense that make it hard. With deep security expertise and relationships with the best technology providers on the market, we are the industry's most comprehensive managed security provider. Clients trust us for strong and enduring protection.

Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

Rapid7

Rapid7 simplifies cybersecurity. With powerful automation and integrated threat intelligence from our industry-leading researchers and SOC analysts, our Insight Platform gives security teams the visibility they need to secure their environments, no matter the size or complexity. Don't just protect your business, drive it forward.

Splunk

Splunk is the data platform leader for security and observability. Our extensible data platform powers enterprise observability, unified security, and limitless custom applications. Splunk helps tens of thousands of organizations turn data into doing so they can unlock innovation, enhance security, and drive resilience.

Yakabod

Built for higher education, CISOBox (Yakabod Cyber Incident Manager) delivers efficient, secure information security incident management through intelligence agency–accredited technology. Colleges and universities use CISOBox to isolate and secure sensitive incident data, documentation, and communication; generate critical metrics; and gain NIST 800-61r2 compliance. And it now offers secure file sharing and ITSM integration!

Zscaler

Zscaler accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

9:00 a.m. – 9:45 a.m.

Contracting for Privacy: Library Licensing and User Data Considerations

Harborside Ballroom A, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Silo-Busting

***Lisa Janicke Hinchliffe**, Coordinator for Info Lit, University of Illinois at Urbana-Champaign*

The licensing privacy initiative, made possible in part by a grant from the Andrew W. Mellon Foundation, aims to improve how academic libraries leverage licensing terms to advocate for reader privacy and has released two resources thus far: (1) View from Library Leadership, findings from research on how user privacy concerns are informing academic library leaders' strategies in negotiating with vendors, and (2) The Vendor Contract and Policy Rubric, which can be used to evaluate how well a given vendor platform follows library privacy guidelines, standards, and best practices, and to use advocates for privacy during vendor selection and contract negotiation. Emergent from these projects is the recognition that libraries have limited capacity to monitor vendor compliance with license terms for user data privacy, and the need to develop campus partnerships to work collaboratively to protect reader privacy and information security.

Finding and Funding Talent

Grand Ballroom I-III, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Workforce/Career Development

***Guy Albertini**, Associate Vice President and Chief Information Security Officer, Rutgers, The State University of New Jersey/Newark*

***Helen Patton**, Advisory CISO, Cisco Systems, Inc.*

***John Virden**, AVP, Chief Information Security Officer, Miami University*

Higher education, and the broader security industry, is dealing with a lot of movement of security people. Finding and keeping talent is tough. In this session the panel will discuss what they're doing to attract and retain talent, and how they're handling staff shortages.

The Hunt for PII: Unparalleled Visibility and Control Over the Environment

Harborside Ballroom B, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Steven Blankenship**, IT Director, Salisbury University*

Finding personally identifiable information (PII) is a lot like finding the perfect crab cake in a lot full of food trucks. Crab metaphors aside, without knowing where your most valuable and sensitive data is, it's impossible to protect it. This session will discuss the project roadmap and tools used by Salisbury University to successfully improve visibility and control into their environment to better identify and secure PII data. As a bonus, SU was able to leverage the same tools and methodologies for hunting PII to find hidden Log4j vulnerabilities and remediate them in real time. SU's use case focuses on a having unparalleled visibility as a critical component for its endpoint configuration to be able to identify and remediate real-time vulnerabilities in seconds. With this solution, SU has been able to dig inside files quickly and efficiently across all servers and clients, rooting out hidden pockets of sensitive data and automatically relocating it off endpoints and servers onto authorized encrypted repositories. Due to the new solutions architecture, SU has been able to immediately respond and control assets even as employees and students were forced to transition to work remotely through the pandemic. Having real-time access to answer questions about our environment (like a Google query) is an essential tool in SU's arsenal and helps the university meet regulatory compliance requirements, address security issues, and fulfil audit obligations.

The Magic of Harmonious Central and Local Privacy Management

Harborside Ballroom D, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: GRC for Privacy and Cybersecurity

***Robin Wilcoxen**, Information Risk Program Coordinator, University of Toronto*

***Rafael Eskenazi**, Director, Freedom of Information, University of Toronto*

***Andrew Wagg**, Incident Response Architect, University of Toronto*

The privacy acronyms are flying at you. You have complex decentralized governance and threat actors from all over the world trying to access your data! How do you create a harmonious privacy management system? The University of Toronto keeps privacy peace among 40 disparate academic and administrative divisions across three campuses with 95,000 students and 23,000 thousand staff and faculty. We do this with a central privacy office that coordinates among Freedom of Information Liaisons, or FOILs, who are senior officials from each division and also with central information security, data governance, legal counsel, research, Office of the President, Governing Council and other central offices and authorities. In this way, the university achieves institutional-level control and standards where appropriate, and also a reasonable level of local participation and a local expert check on required privacy actions. The solutions that this model creates are privacy protective, legally compliant, and strongly informed by divisional needs, while preserving the central oversight of the university FIPP Office and the likewise central institutional responsibility for compliance. This model is flexible enough to accommodate academic freedom for faculty and specific local projects and practices within an overarching set of central standards. It is also ideally structured to accommodate future requirements, challenges, and directions while preserving institutional harmony.

Vulnerability Management: Beyond Scanning and Reporting

Harborside Ballroom E, 4th Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Operations

***Kim Woodruff**, ISO Manager, Rice University*

Learn how Rice University built its vulnerability management program, improving processes and participation to protect its environment from the most critical vulnerabilities. Topics presented will include not only scanning and reporting strategies, but also risk analysis, remediation efforts, the exception process, and areas of improvement.

Zero Trust Is a Hot Topic: Understand It and Use It to More Easily Achieve Your Institution's Goals

Grand Ballroom VII-IX, 3rd Floor

Session Type: Breakout Session

Delivery Format: Presentation/Panel Session

Track: Awareness and Education

***Sharyne A. Miller**, Associate Vice Chancellor and CIO, University of North Carolina, Wilmington*

***Peter Romness**, Cybersecurity Solutions Lead - US Public Sector CT, Cisco Systems, Inc.*

Zero Trust is one of the hottest topics in cybersecurity. Unfortunately, it is also one of the most used and often abused buzzwords in cybersecurity these days. But if you understand it, you don't have to roll your eyes every time you hear it! This session will review the newly released article in the Cybersecurity and Privacy channel of the EDUCAUSE Review on Zero Trust Architecture (ZTA). We'll give you a brief overview of where ZTA came from and why it's needed. Then we'll cut through the hype and help you understand it based upon a simple definition from NIST SP800-207. Your path to Zero Trust will vary depending on your institution's goals, culture, and resources. We'll give you suggestions on how to develop a plan and ideas to get started while accounting for your institution's unique needs. If you have already started down a Zero Trust path, we'll highlight some critical success factors to help make your journey more successful. Zero Trust can also be a transformational enabler. With the ability to protect every connection, you can confidently introduce new capabilities to students, faculty, and staff to give them greater flexibility and productivity.

9:45 a.m. – 10:30 a.m.

Refreshment Break and Corporate Displays

Harborside Foyer, 4th Floor

Session Type: Break

Delivery Format: Break

Track:

10:30 a.m. – 11:30 a.m.

FBI, REN-ISAC, and CISA Threat Briefing - Sponsored by Armis

Grand Ballroom V-VI, 3rd Floor

Session Type: General Session

Delivery Format: General Session

Track:

***Ted Delacourt**, Supervisory Special Agent, Federal Bureau of Investigation*

***Krysten S Stevens**, REN-ISAC Director of Technical Operations, Indiana University*

The threat landscape may seem like more of the same, but new threats are constantly emerging and old exploits are being used in new ways. This session will provide you the freshest information REN-ISAC, FBI and CISA can share. We will discuss threats, trends, and ideas that we can't even imagine at the time of this proposal. You'll leave with a better understanding of specific cyberthreats from around the globe, as well as some insight into the malicious actors' methods, motives, and potential targets in the research and education community.

***Click here* for a message from Armis, the sponsor of this function.**

Wednesday, May 11

10:00 a.m. – 10:45 a.m.

Things You Learn the Hard Way from Doing 20 Years of Penetration Testing - Sponsored by Fischer Identity, Gold Partner

Session Type: General Session

Delivery Format: Live Session

Track:

***Dave Aitel**, Partner, Cordyceps Systems*

The Cybersecurity and Privacy Professionals Conference opening general session speaker, Dave Aitel, will discuss long-term risk-mitigation strategies gleaned from decades of penetration testing. He will talk about which information security investments are needed and why, as well as how the landscape has changed over time.

Click here for a message from Fischer Identity, Gold Partner, the sponsor of this function.

10:45 a.m. – 11:15 a.m.

Town Hall: Looking to the Future with the EDUCAUSE Strategic Plan

Session Type: Breakout Session

Delivery Format: Live Session

Track:

***Nicole Marie McWhirter**, Chief Planning Officer, EDUCAUSE*
***Helen Norris**, Vice President & Chief Information Officer, Chapman University*
***John O'Brien**, President & CEO, EDUCAUSE*

Join EDUCAUSE President and CEO John O'Brien, Board Chair Helen Norris, and Chief Planning Officer Nicole McWhirter in a discussion about the association's strategic planning process. Engage in this lively session focused on the EDUCAUSE commitment to a member-focused future, and be a part of clarifying and affirming the role EDUCAUSE plays and ensuring that our mission and vision are relevant and responsive to the challenges in a post-pandemic world. Come prepared to tell us what your hopes and dreams are for the future of EDUCAUSE!

11:30 a.m. – 11:50 a.m.

Enough Talk! Making Security and Privacy Reviews Practical and Effective

Session Type: Breakout Session

Delivery Format: Simulive Presentation

Track: Operations

***Pegah K Parsi**, Chief Privacy Officer, University of California San Diego*

Do security and privacy assessments provide real value to researchers? We think so! And we want to show you how it can be done.Join us for an engaging conversation where a CPO and CISO collaborate with university leaders and researchers to enable a project to move forward.One important aspect of any security and privacy professional's role is to review and advise on university projects. Our CISO and CPO will talk through the security and privacy needs of a real-world project, including due diligence in vendor assessments. Attendees will become familiar with the value security and privacy professionals bring to the table with a real-world example.

12:00 p.m. – 12:20 p.m.

Bridging the Research and Compliance Communities

Session Type: Breakout Session

Delivery Format: Simulive Presentation

Track: Silo-Busting

***Michael Corn**, CISO, University of California San Diego*

***Carolyn A. Ellis**, CMMC Program Manager, University of California San Diego*

***Jackie Milhans**, Associate Director, Research Computing Services, Northwestern University*

The cornerstones of modern research are collaboration, agility, entrepreneurship, and creativity. Yet institutions are increasingly facing expanding and rigorous security compliance regimes from both sponsoring agencies and commercial partners. Many universities are struggling to marry new security compliance obligations with active research programs, while avoiding throttling scientific exploration. Achieving this requires shedding historical preconceptions of compliance and security, and a broader understanding of the research mission.This interactive panel explores successes and challenges of Northwestern University and University of California, San Diego when handling Research Compliance projects. Learn how to cultivate a culture with a shared vision for the research and compliance partnership.

12:20 p.m. – 1:30 p.m.

Birds-of-a-Feather Sessions (BOFs)

Session Type:

Delivery Format: Live Session

Track:

***Beth Fossum**, PM, CTI Meeting Technology*

Join colleagues during this engaging Birds of Feather session to discuss hot topics in an informal setting. You'll be able to network and exchange ideas, insights, and experiences. *Topics coming soon!*

1:30 p.m. – 1:50 p.m.

Framework for the Future: Connect Dots and Build Bridges with the New CIS Controls

Session Type: Breakout Session

Delivery Format: Simulive Presentation

Track: GRC for Privacy and Cybersecurity

***Randy Marchany**, University IT Security Officer, Virginia Tech*

***Cara Bonnett**, Technology Risk Assurance Manager, Duke University*

The Center for Internet Security (CIS) Critical Controls got a major rewrite in 2021, reflecting core changes in today's computing and infrastructure environments. This presentation will highlight what's new in version 8, why it's well-suited for higher ed, and how two universities are using the updated framework to gain new risk insights and improve security across siloes. The CIS framework maps to a wide range of other formal frameworks (NIST 800-171/CUI, HIPAA, PCI-DSS, among others) and is measurable, specific, and practical to operationalize, which can help identify and prioritize quick wins for tight budgets. Recent research shows that adopting CIS' basic set of recommendations defends against 78 percent of the most common attack techniques.

2:00 p.m. – 2:45 p.m.

FBI, REN-ISAC, and CISA Threat Briefing - Sponsored by Armis

Session Type: General Session

Delivery Format: Live Session

Track:

***Ted Delacourt**, Supervisory Special Agent, Federal Bureau of Investigation*

***Krysten S Stevens**, REN-ISAC Director of Technical Operations, Indiana University*

The threat landscape may seem like more of the same, but new threats are constantly emerging and old exploits are being used in new ways. This session will provide you the freshest information REN-ISAC, FBI and CISA can share. We will discuss threats, trends, and ideas that we can't even imagine at the time of this proposal. You'll leave with a better understanding of specific cyberthreats from around the globe, as well as some insight into the malicious actors' methods, motives, and potential targets in the research and education community.

***Click here* for a message from Armis, the sponsor of this function.**

2:45 p.m. – 3:15 p.m.

Meet the Speakers

Session Type: Breakout Session

Delivery Format: Live Session

Track:

***Ted Delacourt**, Supervisory Special Agent, Federal Bureau of Investigation*

3:30 p.m. – 3:50 p.m.

A Whole Lotta BS (Behavioral Science) About Cybersecurity

Session Type: Breakout Session

Delivery Format: Simulive Presentation

Track: Awareness and Education

***Maren Muxfeld**, High School Student Leader, Cushman/Amberg Communications, Inc.*

***Lisa Margaret Plaggemier**, Executive Director, The National Cyber Security Alliance (NCSA)*

People often don't do things they know they should, even when they can benefit. What's the reason behind this? Do our strategies of scaring students and faculty into taking precautions about cybersecurity issues actually work? Should our approach for building awareness differ between high school students and college students, or between students and baby boomer faculty? New research from the National Cybersecurity Alliance reveals the public's attitudes and beliefs about security, and potential drivers and barriers towards the adoption of secure data security habits. We will share the highlights of this revealing research, and how we can apply such behavioral science insights to develop more effective awareness and behavior change initiatives. In this session, National Cybersecurity Alliance Executive Director Lisa Plaggemier and high school cybersecurity student leader Maren Muxfeld will explore the findings from the organization's annual survey and outline what can be learned when creating awareness programs.

4:00 p.m. – 4:20 p.m.

Zero Trust: It's a Concept, Not a Product

Session Type: Breakout Session

Delivery Format: Simulive Presentation

Track: Operations

***Joel Rosenblatt**, Director, Computer and Network Security, Columbia University*

We have all been getting email from vendors selling the latest and greatest security product—Zero Trust. The problem is that you cannot buy zero trust, you have to build it. My talk will explain what it really is and how you can create a zero trust environment.

4:30 p.m. – 4:50 p.m.

Learn by Doing: Recognizing Student Accomplishments in a Student-Enabled Security Operations Center

Session Type: Breakout Session

Delivery Format: Simulive Presentation

Track: Workforce/Career Development

***Douglas Lomsdalen**, Information Security Officer, California Polytechnic State University, San Luis Obispo*

***Jan Vazquez**, Information Security Analyst, California Polytechnic State University, San Luis Obispo*

According to numerous sources, the United States is experiencing a worker shortage in the cybersecurity career field. To ensure our students have a leg-up in the job hunt, it is the primary goal of the California Polytechnic State University's Information Security Office to ensure our students are ready and have a good start on filling their "security toolkit." Our hiring approach takes any student passionate about cybersecurity and trains them to be the university's first line of defense in our Security Operations Center. Using our university's learning philosophy of "Learn by Doing," we've developed a training program to get the students up-to-speed and secure the campus quickly. We utilize the California Cybersecurity Institute (CCI) as a student pipeline to the SOC. We'll share some of the projects we've had our students work on at the CCI and within the SOC. We have a formal mentoring program and acknowledge students' accomplishments through a home-grown badging program.

11:59 p.m. – 12:19 a.m.

Security Recommendations for Science DMZs

Session Type: Breakout Session

Delivery Format: On-Demand Session

Track: Awareness and Education

***Mark Krenz**, Chief Security Analyst, Indiana University*

A Science DMZ is a special network architecture designed to improve the speed at which large science data transfers can be made. They have become a common solution to the issue of busy academic networks causing slowdowns or failures of large data transfers. A new paper published by Trusted CI on the security of Science DMZs provides an overview of this type of network architecture, summarizing the current best practice cybersecurity risk mitigations as well as providing additional security recommendations. This session is a brief introduction to the Science DMZ concept and presents an overview of the mitigations documented in the paper.

This Job Feels Just Right: Finding your Niche in Cybersecurity

Session Type: Breakout Session

Delivery Format: On-Demand Session

Track: Workforce/Career Development

***Krysten S Stevens**, REN-ISAC Director of Technical Operations, Indiana University*

***Amy Starzynski Coddens**, Strategic Partnerships Manager, Indiana University*

***Carolyn A. Ellis**, CMMC Program Manager, University of California San Diego*

Daily we hear about the need for cybersecurity talent, and yet we also hear stories about people at all levels who are not always able to find their fit. They include graduates trying to get their foot in the cyber door; to mid-level professionals with technical and non-technical skills looking to cybersecurity for a new career path; and seasoned leaders looking for a change. Is the issue the applicants, or is it the unchanged system they are trying to enter? In this session, we will address how applicants and hiring

managers can move beyond the typical hiring process, start building up our cybersecurity resources, and enhance the makeup of our most valuable assets—our teams.

We've Had a Ransomware Attack, Now What? GTCC's Survival Story and How to Thrive after an Attack

Session Type: Breakout Session

Delivery Format: On-Demand Session

Track: Awareness and Education

***Ron Horn**, Chief Information Officer, Guilford Technical Community College*
***Kimberly Johnson**, VP of Product, BIO-key International*

If you've been following any of the headlines out there today, you've seen the rapid growth of ransomware attacks. Despite an increase in focus on tracking, targeting, and disrupting ransomware, the volume of attacks has not seemed to decline, with a new ransomware attack estimated to happen every 11 seconds. In the last two years that included over 2,500 individual schools. In 2020, one of those schools was Guilford Technical Community College (GTCC). Join this session to hear from GTCC's Associate Vice President and CIO Ron Horn as he shares his experience of surviving a ransomware attack and how he continues to thrive after. Ron will share how his team detected the ransomware and their six-month journey to recover from it. He'll talk about what it was like after the attack, including the improvements he's since made to his cybersecurity program, and the hurdles he's had to overcome to keep his cyber insurance. As it's often said when it comes to ransomware attacks, "it's not a matter of if, but when." This is your chance to share your experiences and work together to share best practices on how to survive and thrive after an attack.

XR Security, Privacy, Safety, and Ethics Considerations in Higher Education

Session Type: Breakout Session

Delivery Format: On-Demand Session

Track: GRC for Privacy and Cybersecurity

***Didier Contis**, Director Technology Services, Georgia Institute of Technology*

This session provides an overview of critical XR security, privacy, safety, and ethical challenges that the higher education community will likely face in the short- to medium-term future. Drawing from the experiences with XR adoption at our respective institutions, as well as from collaborating with external advocacy groups—e.g., the XR Safety Initiative (xrsi.org) and the Immersive Learning Research Network's (iLRN) Champions in Higher Education for XR (CHEX) consortium—the presenters will offer insights and recommendations for navigating these challenges in the context of XR adoption in the teaching and learning environment. We will discuss critical security and privacy considerations when initiating and supporting XR initiatives and projects on campus. We will share the existing regulatory frameworks that impact XR learning experiences, with an emphasis on data privacy and security requirements. Our main intent is to encourage participants to engage with the broader higher education community and other relevant organizations to advocate on behalf of students (whether with vendors or policy makers) and support the development of an ethical framework of best practices for XR learning experience design and XR device and software procurement and management.