SECURITY PROFESSIONALS CONFERENCE 2015

Back to the Future: What Will the Future of Information Security Look Like?

Minneapolis, Minnesota, and Online | Hilton Minneapolis
Thank you to our sponsors who enhance the conference experience through support of attendee activities.

It’s clear that today’s information security practitioners require a unique blend of a vision for the future, combined with the wisdom and experience of the past, in order to successfully steer organizations across the modern threat landscape.

This conference is brought to you by the EDUCAUSE and Internet2 Higher Education Information Security Council (HEISC) and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).
ON-SITE CONNECTIONS

WIRELESS ACCESS
Wireless connectivity is available throughout the conference meeting space.
Network SSID: EDUCAUSEAIR
Network password: educause (case sensitive)

NAME BADGES AND PERSONALIZATION
Your name badge verifies your registration and provides admission to functions. Please wear your name badge at all times. Customize yours with colorful stickers indicating your areas of interest, institutional role, and EDUCAUSE involvement. Stop by the Affinity Sticker Bar next to registration.

GET YOUR GAME ON!
TUESDAY, 8:00 P.M.–MIDNIGHT | DIRECTOR'S ROW 3, THIRD FLOOR
Join us for the Security Professionals Conference game night! It’s a great way to get to know your fellow conference participants. No experience is necessary. We’ll be sure to have something for everyone, from casual party games to serious board games. Games will start up throughout the evening, so come by whenever you like. Find a seat and get your game on!

RECEPTION
Sponsored by Kroll
TUESDAY, 5:30–6:30 P.M. | MINNEAPOLIS GRAND BALLROOM SALON D
One of the most valuable aspects of this event 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.

CORPORATE DISPLAYS
Companies providing technology solutions for higher education will be set up in the Minneapolis Grand Ballroom Foyer on Tuesday. Stop by to visit and learn more. A company directory including products and services is located in the back of this program.

FINANCIAL ASSISTANCE FOR PROFESSIONAL DEVELOPMENT
The EDUCAUSE Fellowship Advisory Committee awards fellowships and one scholarship each year to individuals who could not otherwise attend an EDUCAUSE professional development event without financial support. Applications are now being accepted for 2016 events. Apply now, or refer a colleague to educause.edu/Fellow.

WEBCASTS
Recordings Provided by Sonic Foundry, Platinum Partner
The general sessions and six concurrent sessions will be professionally streamed, recorded, and made available to you after the meeting. Webcasts are marked in the daily agendas with the screen icon above.

CERTIFICATIONS
You can claim credit for your privacy and security certifications when you participate in the Security Professionals Conference. Accrediting organizations include (ISC)2, IAPP, ISACA, and GIAC. Learn more at educause.edu/sec15/certifications.

E-MAIL AND PRINTER KIOSKS
Computer and print stations are available during registration hours in the Minneapolis Grand Ballroom Foyer.

SESSION RESOURCES
All presenters are requested to upload their session resources, including slides, videos, handouts, etc., to the session listing in the online agenda, available to participants through the Security Professionals Conference Proceedings web page.

EVALUATION FEEDBACK
Your input is vital to helping shape future events—from what’s offered through the program to who presents it. Please tell us what you think.
Sessions: Share your thoughts on sessions and presenters through the mobile app or the online event program: educause.edu/sec15/Agenda.
Overall: Watch for the overall evaluation e-mail shortly after the event.

MOBILE APP
Sponsored by Pearson, Platinum Partner
Available for: Android | iOS | Tablet
Download the EDUCAUSE Conference & Events mobile app to:
- Access the daily agenda
- Create a personal itinerary
- Review presenter bios
- View location maps
- Complete session evaluations
Download the app: educause.edu/sec15/mobile.

MOBILE DEVICE ETIQUETTE
As a courtesy to participants, we ask that you silence all mobile devices during event sessions. In addition, please limit your mobile device use so bandwidth is not exceeded.
AUDIOTAPING, DIGITAL RECORDING, AND PHOTOGRAPHY

Because all presentations and associated materials are the intellectual property of the presenters, attendees must obtain presenter permission to record a session or other activity in any medium. Attendees are allowed to record for commercial purposes only with prior permission from both EDUCAUSE and the presenters. EDUCAUSE reserves the right to ask attendees to move within or to leave a session venue if their use of technology is disruptive. By attending the event, attendees agree to the terms of the EDUCAUSE Image/Audio/Video Release Form, which allows images, audio, and video recorded on-site to be used for educational and promotional purposes.

Disclaimer: Content from event speeches, presentations, blogs, wikis, and feeds reflects the opinions of the authors and not necessarily those of EDUCAUSE or its members.

ADDITIONAL EXPERIENCES ON-SITE

RENS-ISC TWO-DAY MEMBER MEETING

The Research and Education Networking Information Sharing and Analysis Center is an integral part of higher education’s strategy to improve network security. REN-ISAC members will gather May 6–7, directly after the Security Professionals Conference. Separate registration and fee are required. Learn more at ren-isac.net/events/rimm.

MENTORING

As part of the Security Professionals Conference 2015 Mentoring Program, mentees and mentors are paired prior to the conference experience. Join us for the session “Mixing It Up: Tips for Successful Mentoring Relationships” on Monday, May 4, 4:45–5:45 p.m. in Minneapolis Grand Ballroom Salon F. Learn more at educause.edu/sec15/mentoring.

FUN RUN

WEDNESDAY, 6:00–6:45 A.M.

Join your colleagues for a leisurely 3-mile or 30-minute run. Enjoy the city by participating in a refreshing early morning jog.

PHOTO WALK

WEDNESDAY, 6:00–6:45 A.M.

Whether you are a DSLR master, a smartphone Instagram sharer, or a film traditionalist, enjoy the sights of Minneapolis and the company of fellow photographers during this morning walk. Join us in the hotel lobby and bring walking shoes and your camera of choice.

MAKE A DIFFERENCE BY OFFERING MORE THAN INFORMATION SECURITY

This year we’re partnering with the Ronald McDonald House Schools as part of our first-ever service project. You can give back by donating school supplies for children and families in need. Your generosity will go a long way to providing foundational security to kids struggling to meet basic educational needs.

Supplies wish list:

- Backpacks
- Books: Beginning Readers, Newberry Award winners, picture books
- Classroom single-serving snacks
- Colored pencils
- Construction paper
- Copy paper
- Crayola markers, skinny and wide
- Disinfecting wipes
- Dry-erase markers
- Erasers, pencil top and individual
- File folders, letter size
- Glue sticks
- Individual hand sanitizers
- Individual facial tissue packets
- Mechanical pencils
- Paper bowls
- Paper cups
- Paper plates
- Paper towels
- Pencil boxes
- Pocket folders
- Polymer clay
- Post-it Notes, all shapes and sizes
- Poster board
- Prong folders
- Tempura paints
- Ziploc bags

Labeled boxes are available near registration to collect these supplies.

WANT MORE CYBERSECURITY RESOURCES?


CONNECT THROUGHOUT THE YEAR

Engage in many ways with your EDUCAUSE community!

1. Give a Presentation: Submit a proposal to share your experience and “lessons learned” by answering a call for proposals at any of the available events at educause.edu/Events.

2. Serve on a Program Committee: Find information on program committees at educause.edu/Committees.

3. Contribute as a Session Proposal Reviewer, Convener, or Photographer: Click the “Volunteer Now” button at the bottom of educause.edu/Volunteer.

4. Participate in an EDUCAUSE Live! Webinar: Information and schedule can be found at educause.edu/Live.

5. Explore Professional Development Opportunities: Institute programs, conferences and events, constituent groups, mentoring, our Career Center, and more are outlined at educause.edu/PDopportunities.

6. Volunteer for a Working Group: Join HEISC and help develop information security resources for the higher education community at educause.edu/HEISC.
In addition to thanking the individuals above for their generous dedication and leadership, we’d like to offer a special thanks to the 2015 adjunct proposal reviewers for their contributions during the proposal review and evaluation process.
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30 AM</td>
<td>Registration</td>
</tr>
<tr>
<td>8:00 AM</td>
<td>8:30 AM Preconference Seminars</td>
</tr>
<tr>
<td>8:30 AM</td>
<td>Continental Breakfast for Seminar Participants</td>
</tr>
<tr>
<td>9:00 AM</td>
<td>9:30 AM Refreshment Break for Seminar Participants</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>10:00 AM Preconference Seminars</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>10:30 AM Refreshment Break for Seminar Participants</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>11:00 AM Lunch for Seminar Participants</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>12:00 PM HEISC Leadership Team Meeting</td>
</tr>
<tr>
<td>1:00 PM</td>
<td>1:30 PM Preconference Seminars</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>2:30 PM Refreshment Break for Seminar Participants</td>
</tr>
<tr>
<td>3:00 PM</td>
<td>3:30 PM Preconference Seminars</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>4:30 PM Mixing It Up: Tips for Successful Mentoring Relationships</td>
</tr>
<tr>
<td>5:00 PM</td>
<td>5:30 PM Dinner on Your Own</td>
</tr>
<tr>
<td>6:00 PM</td>
<td>6:30 PM Birds-of-a-Feather Sessions (BOFs)</td>
</tr>
<tr>
<td>7:00 PM</td>
<td>7:30 PM 2015 Program Committee Dinner</td>
</tr>
<tr>
<td>8:00 PM</td>
<td>8:30 PM 2015 Program Committee Dinner</td>
</tr>
<tr>
<td>9:00 PM</td>
<td>9:30 PM 2015 Program Committee Dinner</td>
</tr>
<tr>
<td>10:00 PM</td>
<td>10:00 PM 2015 Program Committee Dinner</td>
</tr>
</tbody>
</table>
May 4

7:30–8:30 a.m.

Continental Breakfast for Preconference Seminar Participants
MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

7:30 a.m.–5:30 p.m.

Registration Desk Open
MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

Connect Lounge Open
DIRECTOR’S ROW 3, THIRD FLOOR

Whether you want to connect with people, ideas, power, or all three, take advantage of our Connect Lounge to network, organize impromptu meetings, or simply recharge your mobile device or yourself.

8:30 a.m.–12:00 noon

MORNING SEMINARS

Please note: Separate registration and fee are required to attend seminars.

PCI Program Frameworks: Learning to Cope with Compliance
MINNEAPOLIS GRAND BALLROOM SALON G, THIRD FLOOR

David Escalante, Director of Computer Policy and Security, Boston College; Daniel Adinolfi, Senior Security Engineer, Cornell University

The Payment Card Industry Data Security Standard (PCI DSS) is an ever-evolving set of requirements that many schools have trouble working into their IT and business practices. Depending on the size and scope of each institution’s payment environment, the burden that the PCI DSS places on an institution can vary. The trick to coping with these requirements (and the resulting burden) is developing a program to manage the evolving rules and business practices while striving to reduce the scope of affected technologies wherever possible. We will offer frameworks for developing a PCI compliance program, guidance on scope definition and reduction, and practical examples of where outsourcing PCI technologies creates opportunities and limitations for your electronic payment program and practices.

Legal Structure and the Security Professional: A Practical Guide
CONRAD A, SECOND FLOOR

Patrick J. Feehan, Director, IT Policy and Cybersecurity Compliance, Montgomery College; Steven J. McDonald, General Counsel, Rhode Island School of Design

In 2015, higher education security professional are under the microscope as the threat landscape changes and grows more complicated. Technology consistently improves and reacts, which requires security professionals to view the legal basis of mitigation strategies and how they contract with vendors. This underpinning legal structure is present in security decisions, whether because of laws (e.g., FERPA, GLBA, HIPAA), contracts (e.g., cloud contracts or PCI compliance), or frameworks (e.g., NIST or ISO). Liability decisions attach to technology decisions, and contracting and process decisions impact liability. This seminar will feature higher education attorneys and discuss proper decision making and governance.

8:30 a.m.–4:30 p.m.

FULL-DAY SEMINAR

Please note: Separate registration and fee are required to attend seminars.

Imagining the Ideal Security Program
MINNEAPOLIS GRAND BALLROOM SALON F, THIRD FLOOR

Cathy Hubbs, Chief Information Security Officer, American University

Come prepared for a crowdsourcing experience that may have an epic impact on your security program. Together we will deconstruct, design, and build the ideal security program. What will it take to get there? We will explore preparing for the inevitable security disruptions, gaining executive sponsorship, developing campus relationships, delivering security awareness messages, and measuring your program’s maturity. The goal of this seminar is to engage, challenge, and expand your thinking of what it takes to lead and sustain a successful information program. Participants will discuss and potentially address security issues from their own institutions.

10:00–10:30 a.m.

Refreshment Break for Preconference Seminar Participants
MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR, AND CONRAD FOYER, SECOND FLOOR
12:00 noon–1:00 p.m.

Lunch for Preconference Seminar Participants

DULUTH ROOM, THIRD FLOOR

Lunch is provided for all preconference seminar attendees. Lunch ticket is required.

12:00 noon–4:00 p.m.

Higher Education Information Security Council (HEISC) Leadership Team Meeting

(By invitation only)

DIRECTOR’S ROW 1, THIRD FLOOR

1:00–4:30 p.m.

AFTERNOON SEMINARS

Please note: Separate registration and fee are required to attend seminars.

Next-Generation Information Security: Business Process and Information Management

CONRAD A, SECOND FLOOR

Tracy Mitrano, Director, IT Policy and Law, Cornell University

Learn about the formulation and ongoing work of an Information Security Office, from the CIO’s strategic vision, to partnerships with other campus offices and constituencies, to cross-campus organizational outreach through senior leadership committees. A comprehensive framework informs the more traditional functions of IT security in governance, policy formation, and internal organization, using a “security by design” functional approach within the IT organization and in support of the institution’s missions. Central to this approach is the creation of a next-generation information security policy that includes data classification, a mandated data-breach response, and support for technical security controls and device configuration standards, developed in collaboration with technical campus IT managers and system-wide IT ISOs, for protecting institutional information and research data. We will explore how campuses of both similar and different Carnegie classes could either create new or reform existing security programs for their next-generation governance, compliance, and risk management needs.

Breaches: Planning + Recovery = Resiliency

CONRAD B, SECOND FLOOR

Jodi-Ann Ito, Information Security Officer, University of Hawaii System Office

Higher ed information security professionals have to cope with very complex threat landscapes combined with open, networked environments and decentralized governance over information assets, which makes it extremely difficult to protect the institution from a data breach and equally difficult to recover from one. This seminar will focus on “breach resiliency” by looking at prevention, preparation, and recovery. The session will begin by looking at the current cyberthreat landscape including management of end-of-life issues (e.g., Windows XP) and zero-day vulnerabilities (Heartbleed, Shellshock, POODLE) to help prevent a breach. The session will then focus on strategies to help prepare for and recover from a breach. These resiliency strategies include risk/crisis/incident management, communications plans, and discussions around cyberinsurance/retainer contracts and the roles of the CIO/CISO and other administrators. Participants will have the opportunity to assess and discuss their institutions’ policies and procedures and identify gaps as they develop their own resiliency strategies.

Digital Forensics Foundations: Hands-On Workshop

MINNEAPOLIS GRAND BALLROOM SALON G, THIRD FLOOR

Alissa Torres, SANS Certified Instructor, The SANS Technology Institute

Join a SANS-certified instructor for a half-day workshop on digital forensics data acquisition and analysis. The digital footprints left behind by our daily routines are astoundingly detailed and revealing. Digital forensic examiners uncover artifacts from computer and mobile device operating systems, file systems, and application logs left behind to reconstruct the timeline, whether it is that of a successful malware infection of a smartphone or the covert communications and plannings of a crime ring. Join us to hone your skills at analyzing captured data for a startling look at how much can be retold from our interactions with today’s digital devices.

2:30–3:00 p.m.

Refreshment Break for Preconference Seminar Participants

MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR, AND CONRAD FOYER, SECOND FLOOR
4:45–5:45 p.m.

**Mixing It Up: Tips for Successful Mentoring Relationships**

*MINNEAPOLIS GRAND BALLROOM SALON F, THIRD FLOOR*

**Neal Fisch**, Information Security Officer and Director of Enterprise Services and Security, California State University, Channel Islands; **Theresa Semmens**, Chief Information Security Officer, North Dakota State University

Participation in mentoring activities can be a key success factor in your career development. The first 30 minutes of this session will focus on establishing rapport and building trust, setting expectations appropriately, and understanding how to develop meaningful conversations. The last 30 minutes will provide attendees with an opportunity to meet potential mentors and mentees through an informal “speed networking” format. Join us for this lively session and make a difference in your career planning and development!

6:00–8:00 p.m.

**Dinner on Your Own**

6:30–8:30 p.m.

**2015 Program Committee Dinner**

*(By invitation only)*

Members of the 2015 Program Committee should meet in the hotel lobby by 6:00 p.m.

8:00–10:00 p.m.

**BIRDS-OF-A-FEATHER SESSIONS (BOFS)**

*MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR*

Join colleagues this evening to discuss hot topics in an informal setting. You’ll be able to network and exchange ideas, insights, and experiences. You can establish a new topic by notifying us in advance (security-council@educause.edu).

**Security Program Roadmap Workshop (Beta)**

This interactive session will walk through a process for developing a 12–18 month roadmap for an information security program rooted in evaluation of threats/risks/mitigations and organizational goals (both institutional and departmental). The process leverages your organization’s existing risk models/definitions, but also offers one that can be used in the absence of these. Attendees will be expected to participate in the process of developing a roadmap during the session and receive supporting documents/worksheets to aid in their own roadmaps.

---

**Software Defined Perimeter: A New Approach to Stopping Network-Based Cyberattacks**

Software Defined Perimeter (SDP) is a research project supported by the Cloud Security Alliance (CSA) to stop network-based cyberattacks. The group comprises volunteers from the CSA and is led by Bob Flores (former CTO of the CIA) and Junaid Islam (CTO of Vidder). The goal of the group is to identify and validate the simplest solution (leveraging open standards) to stop network attacks. To date, the SDP Working Group has developed a 1.0 spec that combines single packet authorization, network access control, and data encryption into an integrated architecture. The SDP 1.0 spec has been validated in public hackathons (some of which have attracted hundreds of participants due to the $10,000 prize) to mitigate DDoS, man-in-the-middle, OWASP, and APT attacks. Based on the success of the 1.0 spec testing, the SDP Working Group is planning to launch an open-source initiative to develop a lightweight solution to stop DDoS attacks. Therefore, the SDP Working Group is reaching out to partner organizations such as Internet2 to seek volunteer support.
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:00 AM</td>
<td>Breakfast</td>
<td>Minneapolis Grand Ballroom Salon BC, Third Floor</td>
</tr>
<tr>
<td>7:30 AM</td>
<td>Registration</td>
<td>Minneapolis Grand Foyer, Third Floor</td>
</tr>
<tr>
<td>8:00 AM</td>
<td>Opening General Session: James Bamford</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>8:30 AM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>9:00 AM</td>
<td>Refreshment Break and Corporate Displays</td>
<td>Minneapolis Grand Foyer, Third Floor</td>
</tr>
<tr>
<td>9:30 AM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Lunchtime Roundtable Discussions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>10:30 AM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Refreshment Break and Corporate Displays</td>
<td>Minneapolis Grand Foyer, Third Floor</td>
</tr>
<tr>
<td>11:30 AM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Corporate and Campus Solutions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>12:30 PM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>1:00 PM</td>
<td>Refreshment Break and Corporate Displays</td>
<td>Minneapolis Grand Foyer, Third Floor</td>
</tr>
<tr>
<td>1:30 PM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>Refreshment Break and Corporate Displays</td>
<td>Minneapolis Grand Foyer, Third Floor</td>
</tr>
<tr>
<td>2:30 PM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>3:00 PM</td>
<td>Corporate and Campus Solutions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>3:30 PM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>4:00 PM</td>
<td>Refreshment Break and Corporate Displays</td>
<td>Minneapolis Grand Foyer, Third Floor</td>
</tr>
<tr>
<td>4:30 PM</td>
<td>Concurrent Sessions</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>5:00 PM</td>
<td>Reception</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
</tr>
<tr>
<td>5:30 PM</td>
<td>PGP Key Signing</td>
<td>Minneapolis Grand Ballroom Salon E, Third Floor</td>
</tr>
<tr>
<td>6:00 PM</td>
<td>Dinner on Your Own</td>
<td></td>
</tr>
<tr>
<td>6:30 PM</td>
<td>BOFs</td>
<td>Minneapolis Grand Ballroom Salon E, Third Floor</td>
</tr>
<tr>
<td>7:00 PM</td>
<td>Get Your Game On!</td>
<td>Director’s Row 3, Third Floor</td>
</tr>
<tr>
<td>7:30 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:00 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8:30 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:00 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9:30 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:00 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:30 PM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12:00 AM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
May 5

7:00–8:00 a.m.

Breakfast
MINNEAPOLIS GRAND BALLROOM SALON BC, THIRD FLOOR

7:00 a.m.–5:30 p.m.

Registration Desk Open
MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

Connect Lounge Open
DIRECTOR’S ROW 3, THIRD FLOOR

Whether you want to connect with people, ideas, power, or all three, take advantage of our Connect Lounge to network, organize impromptu meetings, or simply recharge your mobile device or yourself.

8:00–9:00 a.m.

GENERAL SESSION

Everyone’s a Target: How America Lost Control of the National Security Agency, and Can It Be Reined In?
Sponsored by Aegis Identity Software
MINNEAPOLIS GRAND BALLROOM SALON D, THIRD FLOOR

James Bamford, Investigative Reporter, Best-Selling Author, and Expert on the National Security Agency

Last summer, James Bamford spent three days hanging out in Moscow with Edward Snowden, the most wanted man in America, for a cover story for Wired magazine. The author of three best-selling books on the NSA and, as a long profile in The New Yorker called him, “The NSA’s chief chronicler,” he was also one of the few people granted unlimited access to Snowden’s stolen documents. In his keynote address at the EDUCAUSE Security Professionals Conference, he will discuss his time with Snowden and take a close look at the agency and how it went out of control. From secretly collecting everyone’s telephone data (and storing it for years) on the theory that everyone who can pick up a phone is a possible criminal, to bugging the personal cell phones of friendly allied leaders, to keeping track of visits to porn sites of innocent Americans in order to secretly destroy their reputations, the NSA has gone far beyond what anyone could have imagined. The question is, can such a secret and powerful agency ever be reined in?

9:00 a.m.–3:15 p.m.

CORPORATE DISPLAYS
MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

Seventeen 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. Please see company names and descriptions on pages 12–13.

9:15–10:15 a.m.

CONCURRENT SESSIONS

“Save the Clock Tower!” (Awareness and Training)
Developing a Full-Spectrum Security Training Program
CONRAD C, SECOND FLOOR

Kevin Hayes, Information Security Officer, and Geoffrey S. Nathan, Policy and Privacy Coordinator, Wayne State University

After encountering resistance from executives to a single-pronged approach, WSU is implementing a three-way security training program for all executives and those with access to sensitive university data. Instead of a one-size-fits-all solution we are using a combination of a “placement/certificate” test, a full-length video program (purchased from a third party), and live lectures by a security team. Participants can choose either online or live training sessions and may “test out” either by successfully completing an online examination. The three-way approach addresses several complaints about simpler programs.

Outcomes: Explore obstacles to successful security training programs • Learn how to involve non-IT executives in security training and the associated planning • Share with other participants your experience in the development and rollout of security training
**“Harness the Lightning!” (Governance, Risk, and Compliance)**

**REI-SCAN Threat Analysis Briefing**

**CONRAD A, SECOND FLOOR**

Kim Milford, Executive Director, REI-SCAN, Indiana University

The Research and Education Networking Information Sharing and Analysis Center (REI-SCAN) gathers information about threats and analyzes them to provide actionable information to cybersecurity professionals in higher education. The information comes from higher educational institutions, governmental agencies, other ISACs, IT providers, cybersecurity research, and CERTs around the world. This briefing will provide an overview of the current global threat environment, focusing on trends and highlighting high-risk, high-probability threats while analyzing their potential impact on the R&E community. We will conclude with a discussion of best practices for cyberthreat defense and response and ways that REI-SCAN can assist information security practitioners.

**Outcomes:** Learn about current, evolving, and pervasive cyberthreats in general and specific to higher education
- Receive a general checklist of controls to mitigate the risks from these threats
- Understand how the REI-SCAN can help you in preparing and deploying operational security

**“Running at 88 MPH” (Program Management)**

**Rethinking and Simplifying Security: A Best Practices Roadmap**

**MINNEAPOLIS GRAND BALLROOM SALON G, THIRD FLOOR**

William Perry, Chief Information Management and Security Officer, California State University, Office of the Chancellor

Often ill-equipped with outdated defenses, education is a prime target for cybercriminals. In fact, a recent cybersecurity threat report names education as the sixth most targeted industry in the world. Amid budget restraints, security policies, and common misperceptions about risk, higher ed security professionals and business executives undoubtedly face a significant challenge. Attend this session to learn how the California university system is protecting its most sensitive information against today’s advanced cybercrime. The speaker will share his security roadmap as it relates to several key elements of developing an effective strategy.

**Outcomes:** Rethink defense-in-depth from a higher education perspective
- Learn how to measure the gap between compliance and risk mitigation
- Review why it’s critical to understand an organization’s business practices
- Learn how to develop a risk-based business case

**“Where We’re Going We Don’t Need Roads!” (Career Development)**

**So Ya Wanna Be a CISO**

**CONRAD B, SECOND FLOOR**

Michael G. Carr, CISO and Director, Enterprise Architecture, University of Kentucky; Jeffrey Gassaway, Information Security and Privacy Officer, University of New Mexico; Matthew C. Junod, Manager of Information Security, The University of Toledo

With security leaders leaving the ranks of higher ed for lucrative positions in the private sector, security leadership opportunities in universities will continue to become available. But do you really want to be a CISO, or do you simply want the fame and fortune? This panel’s members will review their paths to the security “corner office” and then discuss its rewards, challenges, and surprises in order to give up-and-coming security leaders ideas on what to expect in a CISO position, what to demand and what they’ll likely get, and how to recognize when it may be time to move on.

**Outcomes:** Understand career paths for university CISOs
- Learn about three distinctive CISOs pursued the security “corner office”
- Leave with a better idea of what a CISO does and how to become one

**“Flux Capacitor” (Technical)**

**From 0 to 34,000 Multifactor Users in Six Months**

**MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR**

Brad Judy, Director of Information Security, University of Colorado System

The University of Colorado was one of many institutions targeted with phishing to steal paychecks using direct deposit redirection at the end of 2013. To reduce risk while maintaining good employee self-service offerings, CU chose to deploy multifactor authentication to select employee self-service functions. In a project that began in February and went live in July, CU deployed mandatory phone-based multifactor for all 34,000 employees. This session will discuss both nontechnical and technical issues in deploying a widespread multifactor system on an enterprise application.

**Outcomes:** Learn to identify the stage and scale of your multifactor efforts
- Learn about reasoning and issues in the CU project
- Understand key questions when working on large-scale multifactor projects
“1.21 Gigawatts!” (Technical)

Security and the Infrastructure Life Cycle; or, Why Are You Still Using TLS 1.2?

MINNEAPOLIS GRAND BALLROOM SALON F, THIRD FLOOR

Steven Lovaas, IT Security Manager, Colorado State University

We as a community are good about at least considering the full life cycle of newly designed systems, and we talk about incorporating security in all phases of the cycle. However, as recent SSL woes have proven, there is a class of technology on which we rely heavily but whose useful lifetime we don’t regularly consider. We still use infrastructure applications and protocols that have been with us since the beginnings of the Internet. Session attendees will share experiences of supporting (and retiring) old technologies and consider how to craft policies and discussions about life cycles for our critical infrastructure.

Outcomes: Identify 10 archaic technologies ripe for retirement • Be able to approach your institution about infrastructure end-of-life strategies • Be motivated to assist best-practice and theory development for security implications of long-persisting technologies

10:15–11:00 a.m.

Refreshment Break and Corporate Displays

MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

While enjoying refreshments, join informal discussions with representatives from companies providing information security products and services. Get questions answered and find out more about the solutions they have to offer.

Aegis Identity Software

Designed specifically for the education marketplace, Aegis Identity Software’s TridentHE provides an identity management platform to automate provisioning/deprovisioning, identity synchronization, password management, and user self-service. We use contemporary technology and SOA-based open standard provisioning engines, resulting in a solution with a focus on cost savings, compliance, and optimal risk management. Please contact us at info@aegisidentity.com or call 303-222-1066.

Click Security

Click Security’s Breach Prevention solution enables customers to rapidly profile, investigate, and respond to cyberthreats and breaches. Our solution force multiplies today’s stretched security teams by automatically converting millions of alerts into high-risk actors, streamlining investigative efforts and converting findings into new continuous protection.

CloudLock

CloudLock empowers your university in the cloud without compromising security by providing a complete security fabric based on a cloud-native architecture to protect your university assets. By analyzing 15 billion+ objects for more than 5 million end users daily, CloudLock delivers the only complete, risk-appropriate, and people-centric approach to cloud security.

Cloudpath Networks

Cloudpath Networks brings unmatched usability, supportability, and security to educational Wi-Fi through the XpressConnect ES. Designed to overcome the nagging problems of password-based Wi-Fi, XpressConnect ES makes it simple to deploy certificate-based Wi-Fi in large BYOD environments through self-service, automated onboarding.

EventTracker

EventTracker is a leading provider of comprehensive IT security solutions. Our industry award-winning SIEM and log-management solutions enable higher education providers to meet compliance requirements with confidence, increase the security of their IT environments, and reduce overall risk.

FireEye

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyberattacks. FireEye’s Threat Prevention does not require the use of signatures to protect across the primary threat vectors and different stages of an attack.

Fischer International Identity, Silver Partner

Fischer delivers Identity Management Made for Higher Education that streamlines identity and governance. Cloud-based and on-campus solutions improve outcomes by quickly extending effectiveness, agility, compliance, and security across an institution. Visionary, rapidly-implemented technology delivers low-cost, no-risk solutions that provide unparalleled value: provisioning, identity governance, federated SSO, privileged access, and password management.
iboss Cybersecurity
iboss Cybersecurity defends organizations against malware, advanced threats, and data exfiltration with innovative web security, mobile security, and FireSphere Advanced APT defense.

Identity Finder
Identity Finder is a market leader in higher education for sensitive data management and DLP. Manage the entire sensitive information life cycle: discover, classify, and remediate nonpublic data anywhere it is stored within your enterprise. Centrally manage operations, track workflow, generate reports for compliance, and enforce remediation to reduce your risk.

Impulse Point
Impulse provides contextual intelligence and access control solutions in support of BYOD-friendly enterprises. Impulse securely and efficiently automates network access solutions for the mobile enterprise. Combining our real-time, context-aware, and simplified architecture with support services and a customer-centric business philosophy enables our customers' BYOD freedom. Our customers know this as the “Impulse experience.”

iScan Online
iScan Online is a provider of data-breach analytics and prevention solutions, enabling institutions to identify devices at risk before a breach occurs. iScan Online’s award-winning technology answers three critical questions: what data is at risk, how will attackers compromise the data, and what will it cost when the data is breached.

OpenDNS
OpenDNS (www.opendns.com) provides a cloud-delivered network security service that blocks advanced attacks, as well as malware, botnets, and phishing threats regardless of port, protocol, or application. Our predictive intelligence uses machine learning to automate protection against emergent threats before your organization is attacked. OpenDNS protects all your devices globally without hardware to install or software to maintain.

Qualys
Qualys (www.qualys.com) is a pioneer and leading provider of cloud security and compliance solutions, with over 7,700 customers in more than 100 countries. The Qualys Cloud Platform and integrated suite of solutions help organizations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand.

Security Architects
Security Architects’ mission is to deliver high-quality, cost-effective security solutions to mitigate risk and improve IT’s overall effectiveness across the institution. Our services include security risk assessments, identity management, security architecture and privacy strategy, cloud security strategy and planning, educational workshops, and security governance policy development.

Symantec Corporation, Silver Partner
Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

WinMagic Data Security
WinMagic provides the world’s most secure, manageable, and easy-to-use data security solutions. WinMagic’s SecureDoc is a comprehensive encryption and key management product that can manage data security across the enterprise. Our solutions help organizations to minimize business risks, meet privacy/ regulatory compliance requirements, and protect valuable information against unauthorized access.

Wisegate IT
What’s driving security programs? Wisegate interviewed IT leaders about what’s guiding their security programs to help determine what should drive yours. In this poster session, education professionals will learn how to focus on data-centric controls, leverage APIs and cloud computing capabilities, identify the right security metrics, and streamline operational capabilities.
"Save the Clock Tower!" (Awareness and Training)

**Vine-Like Security Awareness**

**CONRAD C, SECOND FLOOR**

Ellen Amsel, Chief Information Security Officer, and Angela Ratliff, OIT Administration Analyst, Princeton University

Using the Vine concept of six-second videos, we will demonstrate how it is possible to create security awareness by taking advantage of tools already available on the iPhone. We will give a 20-minute demo of an actual security awareness presentation that has been used at Princeton.

**Outcomes:** Learn about the opportunities to engage the user community in an entertaining manner • Understand the potential for delivering short, concise information security messages • See the results of this approach

"Harness the Lightning!" (Governance, Risk, and Compliance)

**PCI, A New Approach: How to Build Compliance without Rebuilding Your Network**

**MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR**

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

Columbia University has implemented a PCI-compliant network using a combination of outsourcing, Citrix, autodynamic scanning, and log retention to create a payment card network that runs over the same network as the university’s other functions. A typical PCI-compliance program requires the separation of network elements to segregate the credit card traffic from all other traffic on the network. Using this approach, Columbia was able to save hundreds of thousands of dollars in infrastructure costs.

**Outcomes:** Learn about PCI compliance • Understand the risks of not doing PCI • Discover a method of doing PCI compliance that doesn’t require building a network

"Running at 88 MPH" (Program Management)

**Leveraging Data to Improve Enterprise Security**

**CONRAD A, SECOND FLOOR**

James Perry, Chief Information Security Officer, and Tom Webb, Information Security Officer, University of South Carolina

As the saying goes, what gets measured, gets managed. Learn how the University of South Carolina’s current security initiatives have provided the foundation to leverage data for establishing strategic metrics to measure the efficacy of its security program; and, how data has improved operational decision making and the effectiveness and efficiency of monitoring and incident response procedures.

**Outcomes:** Learn about key security metrics and how to strategically use them • Learn how to use data to make risk-based decisions • Learn how to improve security processes using data

"Where We’re Going We Don’t Need Roads!" (Career Development)

**Information Security Benchmarking Using the Core Data Service**

**CONRAD B, SECOND FLOOR**

Scott Krajewski, Director of IT, Augsburg College; Rich Graves, Information Security Officer, Carleton College; Joanna Lyn Grama, Director of DRA Operations, IT GRC, and Cybersecurity Programs, EDUCAUSE; Carol Myers, Dean of IT, Paradise Valley Community College; Greg Hedrick, Director, Security Services, Purdue University

Learn how the EDUCAUSE Core Data Service can help you benchmark your information security program and practices against the programs and practices of peer institutions. This panel session will review information security data from the 2014 CDS (and compare how that data has changed in the past couple of years) and discuss how other institutions use CDS to benchmark their information security programs.

**Outcomes:** Learn more about the CDS Information Security Module • Discuss benchmarking against other institutions • Learn about information security metrics (if time permits)
Security Options for Restricted-Use Research Data

John E. Marcotte, Data Security Officer for ICPSR, University of Michigan–Ann Arbor

Research data often have special security requirements. This presentation will show a framework for categorizing and implementing these special requirements. Restricted-use research data can contain sensitive information as well as personally identifiable information (PII). Sensitive data can cause harm and legally jeopardize individuals and institutions or damage reputation. PII can lead to disclosure of individuals in research data. Even when PII may be removed or masked, reidentification may still be possible through inference and linkages. Researchers and institutions are obligated to protect these data. In some circumstances, legal mandates exist.

Outcomes: Gain awareness of the special security needs of research • Learn what options are available to comply with regulations • Understand what personnel are needed to maintain a secure research environment

Finding Badness in My 100G Network

Jay Krous, Cyber Security, Aashish Sharma, Cyber Security, and Vincent Stoffer, Cyber Security Engineer, Lawrence Berkeley National Laboratory

The intention of this talk is to equip the audience with knowledge and strategies to operate their own network security monitoring. We will showcase various techniques LBNL is using to monitor its 100Gb link to identify good and malicious activity. We will provide insights into the design decisions of security monitors and how we leverage various frameworks to automate dynamic firewalls capabilities. Network security monitoring is basically finding the proverbial needle in the haystack. This talk will focus on how to look into the right haystack and ways to find that elusive needle.

Outcomes: Understand how a large-scale NSM monitoring setup operates • Learn various strategies used to identify good and bad in the network • Learn how to prioritize response-based degrees of “badness” identified • Exchange stories from the battlefield

Lunch and Roundtable Discussions

Sponsored by Identity Finder

We invite you to join colleagues for a lunchtime roundtable discussion. At the roundtable, you can network with those who share similar interests or responsibilities and discuss topics of particular interest to you. A conference attendee will host each roundtable and facilitate the discussion. These sessions are designed to encourage you to exchange experiences and insights with colleagues; additional lunch tables will be available if you would like to eat and network informally.

Balancing Privacy and Security without a CPO

The Challenges of Adopting Federated SSO

Cloud Services: Authentication and Authorization Strategies

Collaboration with National Law Enforcement and Cybersecurity Organizations

Cybersecurity Risk Frameworks/President’s Cybersecurity Initiatives

eduroam: Tales from the Crypt(ic)

Executive Committees/Executive Briefings

Fraud Investigation: What’s the Role of the Security Team?

HEISC Volunteer Opportunities

Multifactor Authentication Management

Password Managers

PCI DSS 3.0

Security Policies

Sensitive Data Management

Small Colleges and Universities

What’s Next? New Tools, Methods, Architecture, and Ideas
“Save the Clock Tower!” (Awareness and Training)
Security Awareness Metrics: Measuring Change in Human Behavior
CONRAD C, SECOND FLOOR
Lance Spitzner, Director, SANS Securing the Human Program, The SANS Technology Institute

One of the primary goals of most security awareness programs is to reduce risk to institutions by changing human behavior. To ensure the success of their programs, organizations must be able to measure both their human risk and changes to faculty, staff, and student behavior. In this session, we will cover how organizations around the world are doing just that, enabling them to develop an effective security awareness metrics framework.

**Outcomes:** Understand the two categories of metrics for security awareness programs • Learn the key considerations to success • Learn how to identify the top metrics you should measure

“Harness the Lightning!” (Governance, Risk, and Compliance)
Organizing, Measuring, and Managing Information Risk at The Ohio State University
CONRAD B, SECOND FLOOR
Gary Clark, Associate Director of IT Risk Management, and Jim Herbeck, Senior Security Analyst, The Ohio State University

In 2013, the Enterprise Security team at OSU found itself in an unenviable position: its security program was narrowly focused on IT risk, not information risk; the program was not consistently implemented; and there were no metrics that documented how well information risk was being managed. In response, the team launched an ambitious new program to organize, measure, and manage information risk both for individual units and for the university as a whole. This session will discuss Ohio State’s process for developing and implementing a successful, prioritized, flexible, and metrics-driven risk management program in a university environment.

**Outcomes:** Learn how to structure and organize information risk • Learn how to create an information risk survey for performing light-weight risk assessments • Learn how to create 3-year risk management strategies

“Running at 88 MPH” (Program Management)
Establishing a Computer Security Incident Response Team
CONRAD A, SECOND FLOOR
Jane LeClair, Chief Operating Officer, National Cybersecurity Institute (NCI), Excelsior College

We will cover the establishment of a Computer Security Incident Response Team (CSIRT) in detail, including the involvement of individuals from all areas of your organization. Topics will include identifying the key steps for establishing notification procedures, recording/tracking of incidents, developing flowcharts, handling incident reporting and escalation procedures, collecting digital evidence, and reviewing forensic analysis rules of conduct. Table top and mock incident exercises will take place. Stimulation questions covering postincident discussion will engage you to help you get the most out of this learning opportunity. Incidents described will focus on best practices in developing a successful CSIRT within your organization.

**Outcomes:** Identify activities to establish a proficient CSIRT • Identify metrics to gauge the effectiveness of the CSIRT • Participate in hands-on activities to promote depth of learning/lessons learned

“Where We’re Going We Don’t Need Roads!” (Career Development)
Information Security and Records Management: Are They a Good Marriage?
MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR
Theresa Semmens, Chief Information Security Officer, North Dakota State University; Kathleen R. Kimball, Chief Information Security Officer, and Caroline J. Walters, University Records Officer, University of Virginia

Historically, in order to succeed in the role of CISO, strong technical skills have been required. A current trend is to meld managerial/business-oriented roles, such as records management, under the CISO. Trends that blend more than one function such as records management and information security are provoking debate among security professionals who are concerned that information security is no longer a primary focus. The University of Virginia and NDSU have combined these roles under the Information Security Office. This interactive presentation will provide two different institutional perspectives on how it works and how it can be woven into security.

**Outcomes:** Understand what knowledge and skills are needed for current and emerging job descriptions • Debate if additional business skills are needed for a CISO • Network with other CISOs who have successfully blended skills
“Flux Capacitor” (Technical)

University of Nebraska 2012 Breach

MINNEAPOLIS GRAND BALLROOM SALON F, THIRD FLOOR

Christopher Cashmere, Senior Security Analyst, University of Nebraska; Dan Buser, Senior Information Security Analyst, University of Nebraska–Lincoln

In 2012, the University of Nebraska experienced one of the largest breaches in higher education. NU staff will walk through the events of the breach from the first detection to the sentencing of the perpetrator. We will dive into some details of the investigation and our experiences with federal authorities, local law enforcement, and prosecutors. We will also cover the technical details of how our Oracle PeopleSoft student information system was exploited, along with what we learned and what we changed.

Outcomes: Take home a practical to-do list to make a breach less likely and lessen the impact of those that do occur • Understand some of the internal workings of Oracle PeopleSoft and how they were and can be exploited

“1.21 Gigawatts!” (Technical)

A University Uses an Intelligent Approach against Malicious Threats

MINNEAPOLIS GRAND BALLROOM SALON G, THIRD FLOOR

David Shipley, Director, Strategic Initiatives, University of New Brunswick

Universities are among the most frequently cyber-attacked institutions on the planet. Schools across North America are repositories of vast amounts of personal information, intellectual property, and a high-speed infrastructure that can be used to attack others. As such, they are under increasing pressure from domestic and international actors. To respond to these massive-scale threats, a new machine-powered approach that mimics the qualities of the body’s autoimmune system is required. Learn how the University of New Brunswick is evolving its network security, malware, NAC systems, and security event intelligent monitoring systems toward such an approach.

Outcomes: Understand how discovery tools capture, correlate, and respond to evasive threats in real time • Develop security plans for an increasingly automated future • Learn to create partnerships, processes, and practices to improve security posture

2:30–3:15 p.m.

Refreshment Break and Corporate Displays

MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

This is your last opportunity to visit with 17 security technology solutions providers. Please see pages 12–13 for company descriptions.

Aegis Identity Software
Click Security
CloudLock
Cloudpath Networks
EventTracker
FireEye
Fischer International Identity, Silver Partner
iboss Cybersecurity
Identity Finder
Impulse Point
iScan Online
OpenDNS
Qualys
Security Architects
Symantec Corporation, Silver Partner
WinMagic Data Security
Wisegate IT
CORPORATE AND CAMPUS SOLUTIONS
Building a Higher Ed Security Program from Scratch
CONRAD B, SECOND FLOOR

Rob McCurdy, CISO, Michigan State University; Renault Ross, Security Business Principal, Symantec

This session will share the building blocks of establishing an enterprise security program from scratch from the viewpoint of the chief information security officer in charge of securing the higher ed institution. Symantec will initially frame the discussion around five key principles to building a security program to establish a baseline for the discussion. The CISO will discuss the institution’s methodology (business buy-in, resource alignment and communication strategy, and cyber tooling decisions).

Outcomes: Obtain strategic direction from peers building a cybersecurity program • Obtain industry best practice from a cybersecurity leader • Collaborate and share practices with peers

Cloudy, with a Chance of...? Data Security in the Age of the Cloud
MINNEAPOLIS GRAND BALLROOM SALON F, THIRD FLOOR

Tina Thorstenson, Assistant Vice President and Chief Information Security Officer, Arizona State University; Eric Chaves, Senior Sales Engineer, CloudLock

It’s happening as we speak: more and more universities are moving away from traditional on-premises network infrastructure and legacy enterprise applications to cloud-based SaaS platforms including Google Apps, Office 365, Salesforce, Box, Workday, ServiceNow, Dropbox, and others. But how does this affect the future of data security in a public, cloud-enabled world? The truth is, the future is already here, and the impact is now. Join us for a lively talk on how forward-thinking organizations are balancing end-user enablement and organizational security with Zen-like sagacity.

Outcomes: Learn the potential impact of information already in the cloud • Learn the value and benefits of implementing multiple SaaS applications • Learn how to become a leader by moving your organization forward to the cloud

How Institutions Like Princeton Calculate Security Risk with Self-Assessment and Data-Breach Analytics
CONRAD C, SECOND FLOOR

Billy Austin, President and Co-Founder, iScan Online

It doesn’t take college-level math to understand this simple formula: Unprotected Data + Vulnerable Systems = A Breach Waiting to Happen. Most universities understand this but struggle to prioritize their limited resources, focusing their discovery and remediation on core infrastructure while while treating community self-assessments as an afterthought. The net outcome is a security policy that neglects those end users with the least security awareness. Leading institutions like Princeton are tackling this issue head-on. By deploying scanning solutions that work for end users as well as IT, they’re proactively identifying more risks without requiring more resources.

Outcomes: Learn why most security awareness programs fail to eliminate the human threat • Understand why universities need to prioritize threats by financial risk • Discover how to use this method of data-breach analytics and do more with less spend

Lessons Learned: Implementing a Vulnerability Management Program for Higher Ed
MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR

Michael W. Zimmer, Senior Information Security Analyst, Northern Arizona University; Grant Johnson, Technical Account Manager, Qualys

When it comes to keeping networks secure, universities, colleges, high schools, and other education and training facilities face a unique challenge. By their very nature, educational institutions are designed to be open communities; however, open environments leave sensitive data vulnerable to attack. In this presentation, Northern Arizona University and Qualys will discuss the importance of implementing a vulnerability management solution and discuss some of the challenges universities face in identifying security threats. Learn about NAU’s implementation of a vulnerability management process and how NAU was able to gain a more complete view of its network.

Outcomes: Learn about key drivers within higher ed impacting today’s security professional • Learn why taking an automated approach to vulnerability management can help simplify and reduce the cost of identifying and securing IT assets while ensuring compliance with internal policies and external regulations • Get best practices for building an effective vulnerability management program
Not Planning on Using Biometrics as Part of Your IAM and BYOD Strategies? Plan on Getting Breached

MINNEAPOLIS GRAND BALLROOM SALON G, THIRD FLOOR

Alan Dundas, Vice President of Product, Authentify;
Stephen J. Elliott, Associate Professor, Department of Industrial Technology, Purdue University

As BYOD becomes more prevalent in our world, enrollment in online higher education programs is on the rise. Mobility requires device-based authentication and certainty that any device is held by an authorized user, or inevitably a breach of the university network will occur. Biometrics ensures the right user, but there are risks such as relative authentication strength of different biometrics and movements like FIDO to consider. A wide range of biometrics is available, but selecting options and comparing them can be difficult. This session will discuss real-world tests, the risks and benefits of architecting biometric storage, and best practices for implementation.

Outcomes:
Understand the pitfalls, risks, and benefits of using biometrics • Understand the requirements needed to plan and architect device-based authentication • Get biometric data from the International Center for Biometric Research at Purdue

Security, Efficiency, and the Cloud for Today’s Threat Landscape

CONRAD A, SECOND FLOOR

Andrew Hay, Director of Security Research, OpenDNS;
Gina Allen, Communications and Information Security Policy Specialist, Tulane University

Today’s bad actors are finding new ways to cheaply automate their phishing and malware campaigns to target more end users than ever before. At the same time, institutions must protect a growing population of students, faculty, and staff against threats. In this asymmetrical threat landscape, how can university IT departments increase the scale of their operations without allowing costs to spiral out of control? The presenters will discuss how Tulane’s IT department is structuring its response to today’s security challenges.

Outcomes: Understand how attackers are scaling their operations to target more end users, both on and off campus networks • Understand how the cloud can help increase visibility and security on complex campus networks • Understand how Tulane has effectively (and efficiently) scaled its security operations to protect a growing university population

4:30–5:30 p.m.

CONCURRENT SESSIONS

“Save the Clock Tower!” (Awareness and Training)

HEISC Information Security Guide Rebooted

CONRAD C, SECOND FLOOR

James Webb, Chief Information Security Officer, Appalachian State University; Tammy L. Clark, Chief Information Security Officer, The University of Tampa

Finding resources specifically tailored to higher education can be difficult when you’re developing information security programs and initiatives. That’s where the Information Security Guide comes in. Perhaps you are new to higher education or a new CISO just getting started, or maybe you’ve been around for a while but are looking for fresh perspectives. We’ll discuss our approach to providing actionable guidance to assist with challenges we’re all facing. Share your ideas with us. We’re listening.

Outcomes: Learn more about the HEISC online Information Security Guide • Understand how to access guide resources that can assist information security professionals • Engage in interactive discussions around getting started with key information security initiatives at your institution

“Harness the Lightning!” (Governance, Risk, and Compliance)

Cloud Service Procurement: Engaging the CISO for a Risk Assessment

CONRAD A, SECOND FLOOR

Walter Petruska, Information Security Officer, University of San Francisco

Everywhere you turn cloud service vendors are enticing colleges and universities with quick implementations and minimal internal support costs, convincing them that “the cloud” is the future. However, time and time again, critical questions are not asked or considered before signing on the dotted line. Is your CISO involved in the procurement process? Who assesses the risk of using these cloud services to store the university’s data or integrate it with existing systems? Learn what policies, guidelines, and processes are in place at University of San Francisco to properly assess cloud services before the contract is executed.

Outcomes: Learn how to critically assess a contract for cloud services • Understand why information security should be part of the process • Review an assessment framework used by USF
“Running at 88 MPH” (Program Management)

Continuous Improvement Built on Incident Management

MINNEAPOLIS GRAND BALLROOM SALON G, THIRD FLOOR

Kevin Lanning, Chief Information Security Officer, University of North Carolina at Chapel Hill

We hear and read about information security incidents in the daily news. Such situations are best prevented. They are difficult for all involved and can represent a significant drain on resources. Thoughtful program design, effective triage, timely decision making, and effective communications are required, but the potential opportunity for continuous improvement is sometimes overlooked. This session will explore these topics and discuss opportunities for continuous improvement of an incident management program. Feedback resulting in a more effective information security program and more effective controls is among the many possible opportunities presented by a comprehensive incident management program.

Outcomes: Learn a wide variety of new incident management program components • Understand the value of designing and provisioning such program components before an incident • Understand how to leverage incidents to improve information security program components

“Where We’re Going We Don’t Need Roads!” (Career Development)

The Higher Education CISO in 2014

CONRAD B, SECOND FLOOR

Wayne Brown, Vice President for Information Technology and Chief Information Officer, Excelsior College

In the summer of 2014, CHECS (www.cheecs.org) conducted a survey of higher education CISOs and CIOs about skills, education, and their place in the hierarchy. In addition, both groups were asked about the CISO role and the security program, maturity, and systems at their institutions. Over 250 people responded to the surveys. The results shed light on the importance of different CISO roles and CISO effectiveness operating in those roles. The research also provided information about position requirements according to the CISO and the CIO, who supervises the vast majority of the CISOs.

Outcomes: Learn about CISOs’ education and experience • Understand the expectations higher education CIOs have about CISOs regarding roles and background • Discover the reality of the CISO’s place in the organizational hierarchy and the ideal place, according to CISOs and CIOs

"Flux Capacitor" (Technical)

Reel 'Em In: Responding to (Successful) Phishing Attacks

MINNEAPOLIS GRAND BALLROOM SALON F, THIRD FLOOR

Gabriel Deleon, Network Security Analyst, New York University

Education is a great long-term solution to reduce phishing-based compromises; however, accounts still get owned, and if you’re on operations duty, you need to do something about it. We’ll go over how phishing sites have shifted their attacks over the past few years, review methods NYU uses to mitigate and respond to both big and small phishing attacks, and, if time permits, demo a tool you can use to push garbage data into phishing forms.

Outcomes: Learn about changes in phishing behavior • Learn techniques to mitigate against phishing attacks • Obtain a tool you can use to foil phishing sites

“1.21 Gigawatts!” (Technical)

Fun with Certificates: A Deep Dive into Cryptography for All Ages

MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR

Brian Epstein, Manager, Network and Security, Institute for Advanced Study

It is critical to understand the technologies we use to protect data. When trying to convey the importance of digital encryption, questions may arise about how the technology works and why it is important. This presentation will explain symmetric and asymmetric cryptography in such a way that the nontechnical person can understand. Using hands-on, fun aids, we will run through an example of ROT13 and RSA encryption and talk about the issues of key management and different programs like GNUpg/ PGP and OpenSSL. Using presentations of this type to spread security knowledge can ease the job of convincing people to use security technology.

Outcomes: Learn how RSA cryptography works using decoder rings and simple math • Explain and understand the complexities of certificate trust models using easy examples • Engage in discussion of how to apply this knowledge to real situations
5:30–6:30 p.m.

**Reception**

Sponsored by Kroll

**MINNEAPOLIS GRAND BALLROOM SALON D, THIRD FLOOR**

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. Wear a sweatshirt (or other apparel) with your institution’s name, mascot, or tagline—we love to see where everyone is from! A cash bar will be available; each attendee will receive one drink ticket.

**NOTE:** Please wear your name badge for admittance.

6:30–7:30 p.m.

**PGP Key Signing**

**MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR**

Brian Epstein, Manager, Network and Security, Institute for Advanced Study; Ken Connelly, IT Security Officer, University of Northern Iowa

This PGP Key signing is open to all interested conference attendees. Additional information is available at [www.ren-isac.net/events/spc_2015_keysigning](http://www.ren-isac.net/events/spc_2015_keysigning). Questions about this event should be directed to the presenters.

6:30–8:30 p.m.

**Dinner on Your Own**

8:00–10:00 p.m.

**BIRDS-OF-A-FEATHER SESSIONS (BOFS)**

**MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR**

Join colleagues this evening to discuss hot topics in an informal setting. You’ll be able to network and exchange ideas, insights, and experiences. You can establish a new topic by notifying us in advance (security-council@educause.edu).

---

**Evolving Attack Methodologies Observed in Higher Ed and Lessons Learned**

As organizational information security programs mature and the cybersecurity arms race continues, many organizations are starting to see attacks with increasing levels of sophistication. This BOF session is designed to allow institutions to share war stories, observed attack techniques, lessons learned, and effective defense strategies against some of these more advanced attacks. The Vegas rule applies in this session: anything shared in the room stays in the room.

**Internet2 NET+ Security and Identity Portfolio: Building a Portfolio with the Community, for the Community**

The Internet2 NET+ initiative has included trust- and identity-related service providers in coordination with InCommon since the NET+ program started. Information security is integrated into the service-validation process using the CSA CCM. Internet2 is expanding the initiative to increase the information security-related services available and starting to engage with the higher education information security community. Please join us to share suggestions on new service providers, provide feedback on existing providers, or ask questions about the NET+ initiative.

**Ivy-Plus**

All colleagues from an Ivy-Plus institution are welcome to join us for one of our semiannual gatherings of Ivy-Plus security and privacy professionals. We will be meeting at a local restaurant (TBD) for a night of reconnecting, getting to know new colleagues, and talking about our roles and lives on an Ivy-Plus campus. See any of the Ivy-Plus CISOs at the conference for more details, and plan on meeting in the hotel lobby at 6:45 on Tuesday night.

**Get Your Game On!**

**DIRECTOR’S ROW 3, THIRD FLOOR**

Brian Smith-Sweeney, Chief Information Security Officer, Columbia University

Join us for the third annual Security Professionals Conference game night! This is a great way to kick off the conference and help you 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 start up throughout the evening, so come by whenever you like. Grab a chair and get your game on!
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
<th>Location</th>
<th>Time Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:00 AM</td>
<td>Fun Run and Photo Walk</td>
<td>Meet in the Hotel Lobby</td>
<td>6:00 a.m.–6:45 a.m.</td>
</tr>
<tr>
<td>7:00 AM</td>
<td>Breakfast</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
<td>7:00–8:00 a.m.</td>
</tr>
<tr>
<td>7:30 AM</td>
<td>Concurrent Sessions</td>
<td></td>
<td>8:00–9:00 a.m.</td>
</tr>
<tr>
<td>8:00 AM</td>
<td>Registration</td>
<td>Minneapolis Grand Ballroom Foyer, Third Floor</td>
<td>7:00 a.m.–1:00 p.m.</td>
</tr>
<tr>
<td>8:30 AM</td>
<td>Pause</td>
<td></td>
<td>9:00–9:15 a.m.</td>
</tr>
<tr>
<td>9:00 AM</td>
<td>Concurrent Sessions</td>
<td></td>
<td>9:15–10:45 a.m.</td>
</tr>
<tr>
<td>10:00 AM</td>
<td>Refreshment Break</td>
<td>Minneapolis Grand Ballroom Foyer, Third Floor</td>
<td>10:45–11:00 a.m.</td>
</tr>
<tr>
<td>11:00 AM</td>
<td>Closing General Session: Christopher Buse</td>
<td>Minneapolis Grand Ballroom Salon D, Third Floor</td>
<td>11:00 a.m.–12:00 noon</td>
</tr>
<tr>
<td>12:00 PM</td>
<td>Lunch for Postconference Seminar Participants</td>
<td>Conrad D, Second Floor</td>
<td>12:00 noon–1:00 p.m.</td>
</tr>
<tr>
<td>1:00 PM</td>
<td>Postconference Seminar</td>
<td>Conrad C, Second Floor</td>
<td>1:00–2:30 p.m.</td>
</tr>
<tr>
<td>1:30 PM</td>
<td>Refreshment Break for Seminar Participants</td>
<td>Conrad Foyer, Second Floor</td>
<td>2:30–3:00 p.m.</td>
</tr>
<tr>
<td>2:00 PM</td>
<td>Postconference Seminar (continued)</td>
<td>Conrad C, Second Floor</td>
<td>3:00–4:30 p.m.</td>
</tr>
<tr>
<td>2:30 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:00 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:30 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:00 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:30 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
May 6

6:00–6:45 a.m.

Fun Run
HOTEL LOBBY
Meet in the hotel lobby and join your colleagues for a leisurely 3-mile or 30-minute run. Enjoy the city by participating in a refreshing early morning jog.

Photo Walk
HOTEL LOBBY
Meet in the hotel lobby and join fellow photography enthusiasts for a morning walk through downtown Minneapolis. Whether you are a DSLR master, a smartphone Instagram sharer, or a film traditionalist, enjoy the sights of Minneapolis and the company of fellow photographers during this morning walk. Bring walking shoes and your camera of choice.

7:00–8:00 a.m.

2016 Program Committee Breakfast
(By invitation only)
CONRAD D, SECOND FLOOR
Breakfast
Sponsored by CloudLock
MINNEAPOLIS GRAND BALLROOM SALON D, THIRD FLOOR

7:00 a.m.–1:00 p.m.

Registration Desk Open
MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

Connect Lounge Open
DIRECTOR’S ROW 3, THIRD FLOOR
Whether you want to connect with people, ideas, power, or all three, take advantage of our Connect Lounge to network, organize impromptu meetings, or simply recharge your mobile device or yourself.

8:00–9:00 a.m.

CONCURRENT SESSIONS

“How to Phish Higher Ed” (Awareness and Training)
How to Phish Higher Ed
CONRAD C, SECOND FLOOR
Steve Edwards, Senior Information Security Analyst, Eastern Michigan University
For more than a year, we have been sending spear phishing e-mails to our own campus as part of our security awareness campaign. In this presentation, we will share the contents of these e-mails and what the response from our user community shows: what the ingredients of a successful spear-phishing campaign when targeting higher education are, why technological controls may not be a sufficient defense against phishing, and how Eastern Michigan University uses these phising e-mails to deliver security education to the end user.

Outcomes: Learn what makes a phishing campaign successful when targeting higher education • View analytics from 14 phishing campaigns to understand how users respond • Understand how EMU uses phishing e-mails to educate its community

“Harness the Lightning!” (Governance, Risk, and Compliance)
Bring Your Own Cloud
CONRAD B, SECOND FLOOR
Eric Smith, Chief Information Security Officer, Bucknell University
BYOC (bring your own cloud) is here, and it’s eroding our institutional data classification controls. Unlike BYOD, which has been our standard operating procedure for decades, BYOC is a complex and potentially catastrophic security issue that can’t be solved by perimeter hardware alone. In BYOC, users research and test various cloud services, create individual accounts, then quickly use these tools to store, process, and share institutional data—usually without consent or knowledge of IT staff. In this session, we’ll discuss our consortium’s approach to this BYOC challenge, including initial assessment, policy and governance, and templates for evaluating potential cloud services.

Outcomes: Understand popular BYOC services and how they are being used at your institution • Absorb policy elements that ensure that ISO/IT is involved in services evaluation • Learn how to evaluate a potential cloud service
“Running at 88 MPH” (Program Management)

Never Waste a Crisis: Funding an Information Security Program into the Future

Conrad A, Second Floor

Cornelis Leune, Information Security Officer, Adelphi University; Doug Ooley, Director of Information Security/Information Security Officer, Boise State University; Paul Howell, Chief Cyberinfrastructure Security Officer, Internet2; Dave Nevin, Chief Information Security Officer, Oregon State University; Robert K. Henry, Chief Information Security Officer, Santa Clara University; Randy Marchany, University IT Security Officer, Virginia Tech

Panelists from schools both large and small, public and private will candidly discuss what has succeeded and what has failed in their efforts to fund an information security program. Surveys regarding IT security budgets for a variety of industries indicate the security budget is between 2% and 5% of the total IT budget. EDUCAUSE surveys find that the sweet spot in higher education averages 3% of the total IT budget. This value varies considerably, and obtaining the necessary funding to maintain and grow a security program requires deft skills at “selling up” the value of security to leadership.

Outcomes: Understand the fragility of information security budgets • Learn about a variety of ways to sustain an information security budget • Understand what metrics sell the value of security to university leadership

“Where We’re Going We Don’t Need Roads!” (Career Development)

Privacy Explained and the Role of the Privacy Officer in Higher Ed

Minneapolis Grand Ballroom Salon E, Third Floor

Susan A. Blair, Chief Privacy Officer, University of Florida; Sol Bermann, Privacy Officer, University of Michigan–Ann Arbor

Privacy as both a focused discipline and as a role is very new in general and in higher education in particular. Two university privacy officers will provide an overview of privacy and describe the varied role of university privacy officers. Attendees will explore how privacy intersects with information security, and how privacy and security officers can and should collaborate.

Outcomes: Learn about privacy’s evolution, history, and ongoing importance • Debate the public perceptions of privacy • Understand the privacy officer role and how privacy and security officers should collaborate

“Flux Capacitor” (Technical)

Breaking the Ubiquitous Two-Factor Barrier

Minneapolis Grand Ballroom Salon F, Third Floor

Quinn Shamblin, CISO, Boston University; Jane Drews, CISO, The University of Iowa

In a world where the only thing standing between the bad guys and their pay day is knowledge (of a password, of a security question answer, etc.), we are at risk. The problem is not phishing, weak passwords, shoulder surfing, or keystroke logging. These are types of attacks. The problem is compromised credentials. The only effective defense is to ensure that a compromise of credentials doesn’t compromise the security of institutional and personal information or the critical business processes of the institution. Learn how Boston University and the University of Iowa selected, piloted, and implemented a strategic solution for two-factor authentication using Duo Security. We will compare and contrast decisions made, tools used and developed, lessons learned, and the current status of our implementations. We will also review some of the challenges with phone-based two-factor authentication, and what we have planned for the future.

Outcomes: Learn about phishing attacks against higher education that led to widespread financial fraud and how to effectively protect your institution • Understand some key decisions involved when implementing two-factor authentication solutions • Hear highlights of the successes and challenges of a production implementation

“1.21 Gigawatts!” (Technical)

Techniques for and Consequences of Packet Filtering, Interception, and Mangling

Minneapolis Grand Ballroom Salon G, Third Floor

John Kristoff, Researcher, Team Cymru

Often in response to immediate threats of abuse and resource exhaustion, our networks have changed fundamentally. What has been the effect of these changes on protocols, network operations, applications, and information security? As the focus has shifted from interconnection to security, what have we gotten? We characterize various forms of packet filtering, inception, and mangling that have fundamentally changed our networks. For some who have never known a world without NATs, packet shapers, or intrusion prevention systems, this is part history. For all, it is a call for reflection and careful consideration about where we decide to go and what to do next.

Outcomes: Understand the effect certain network technologies and techniques are having on campus networks • Make better informed decisions about network infrastructure changes • Appreciate how security and networking often collide and cooperate in practice and in theory
CONCURRENT SESSIONS

“Save the Clock Tower!” (Awareness and Training)

Puzzle-Based Learning in Cybersecurity Education

CONRAD C, SECOND FLOOR

Dipankar Dasgupta, Director, Center for Information Assurance, The University of Memphis

Puzzle-based learning provokes the thinking process of participants by challenging them. The interactive process allows participants to seek alternative solutions to handle security situations in cyberspace, which makes the learning process enjoyable. Different forms of puzzles exist for people to think creatively, expand their knowledge, and stimulate their cognitive ability. We have developed several security puzzle exercises based on some guiding principles in order to simulate interactive real-life cyberattack scenarios for training in different aspects of computing, networking, and information security. All puzzles align with emerging technology to provide up-to-date knowledge on cybersecurity issues.

Outcomes:
- Learn how to deal with cybersecurity incidents, even if you have not encountered one before
- Understand different privacy issues when engaged in online social media
- Learn best practices while surfing the web

“Harness the Lightning!” (Governance, Risk, and Compliance)

Implementing a University Cyberisk Mitigation Policy: Lessons from IT-28

MINNEAPOLIS GRAND BALLROOM SALON E, THIRD FLOOR

Andrew Korty, Information Security Officer, and Kim Milford, Executive Director, REN-ISAC, Indiana University

In May 2013, Indiana University approved a new policy to reduce overall threat surface by decreasing the number of servers outside secure facilities and the number of total servers, ensuring all servers are sufficiently maintained and following IT security policies. The policy, which drew extensive discussion with deans, faculty, and IT staff, was a monumental exercise to implement at a comprehensive research university (including a large medical school). This session will cover the process used to communicate with many audiences about the policy, the lessons learned in implementation, and the resulting improvements to IT security.

Outcomes:
- Learn from the successes and challenges of this policy
- Get a feel for the possibility of such a policy at your institution
- Discuss honing the process for future iterations

Onboarding: The Challenges of Integrating New Personnel into Security Operations

CONRAD A, SECOND FLOOR

Daniel Adinolfi, Senior Security Engineer, Cornell University; Brian Epstein, Manager, Network and Security, Institute for Advanced Study; Andrew Weisskopf, Information Security Officer, Iowa State University of Science and Technology; Martin Manjak, Information Security Officer, University at Albany, SUNY; Wayland Morgan, IT Security Analyst, University of Illinois at Urbana-Champaign

This panel presentation will feature representatives from a cross section of Carnegie designations. All the members have extensive backgrounds in higher ed security operations, and all have had recent experience in integrating new hires into their operational environments. The discussion will focus on such issues as trust vetting (e.g., password sharing), documentation, “live” training, the institutional approach to risk, local tools and procedures (alerts, reports, incident management), mentoring, defining and assigning responsibilities, organizational structures, interactions and coordination with other security operations, the importance of interpersonal skills, and off-boarding (exit interviews).

Outcomes:
- Gain a greater understanding of the challenges associated with integrating new hires into your security operations
- Benefit from the experiences offered by the panel participants
- Define best practices for preparing new personnel
“1.21 Gigawatts!” (Technical)

p0wnage and Detections: 2014 Edition
MINNEAPOLIS GRAND BALLROOM SALON G, THIRD FLOOR

Jay Krous, Cyber Security, Aashish Sharma, Cyber Security, and Vincent Stoffer, Cyber Security Engineer, Lawrence Berkeley National Laboratory

For our third annual p0wnage and detections presentation, we will present an in-depth analysis of several security incidents from the past year, which showcase the intrusion detection and incident response techniques used at Berkeley Lab. We highlight how our security systems clearly flagged some compromises while examining the reasons that others were missed.

As part of the examination of the trends for this year, we will discuss how our analysis of these incidents provides a basis for attack modeling and the design of new methods for security monitoring and response.

Outcomes: Get a good idea of the security threats facing an open research network • Understand how security systems fail to catch some attacks • See the tools and techniques needed to do incident response at high speeds

10:45–11:00 a.m.

Refreshment Break
MINNEAPOLIS GRAND BALLROOM FOYER, THIRD FLOOR

11:00 a.m.–12:00 noon

GENERAL SESSION

Doomed by Design: Addressing the Problems with Government Security Programs
Sponsored by Bricata
MINNEAPOLIS GRAND BALLROOM SALON D, THIRD FLOOR

Christopher Buse, Assistant Commissioner and Chief Information Security Officer, MN.IT Services

Two recent studies by NASCIO and Deloitte paint a dismal picture of cybersecurity in the states. This presentation will review the key issues that inhibit the effectiveness of state government security programs. Participants also will gain insight into profound changes that Minnesota is undertaking to change the historical paradigm and deliver cybersecurity services more effectively.

Outcomes: Learn the top 3 things every CISO should be asking for • Understand what not to do in this situation • Engage with panelists and attendees to develop your own wish list
12:00 noon–1:00 p.m.

Lunch for Postconference Seminar Participants
CONRAD D, SECOND FLOOR

1:00–4:30 p.m.

POSTCONFERENCE SEMINAR
Please note: Separate registration and fee are required to attend seminars.

Building Awareness: A Guide to Establishing a Successful Information Security Education Program
CONRAD C, SECOND FLOOR

Daniel J. deBeaubien, Director, The SANS Technology Institute

This seminar will showcase the methodology and results of a multiyear human security risk assessment and security awareness initiative at Michigan Technological University. Attendees will discuss the risk assessment system, metrics, and scoring used to identify specific training needs by individual, department, and division to uncover high-risk behavior and to direct training and auditing where they are needed most. Multiyear data trends, combined with organizational structure data and training metrics, are used to measure the actual impact of awareness training. This process continues, and it is used to focus security resources based on institutional risk, rather than rumor, and to help calculate the business value of security awareness programs and other security initiatives and programs.

2:30–3:00 p.m.

Refreshment Break for Postconference Seminar Participants
CONRAD FOYER, SECOND FLOOR
Looking to learn more about the latest technology to serve your campus needs? Contact our participating companies for information.

**Aegis Identity Software**
*Participation: Corporate Display; Tuesday General Session Sponsor*
Ken Bero, Vice President of Sales and Field Marketing
ken.bero@aegisidentity.com, 303-222-1072
aegisidentity.com/identity-software
*Product Categories: Federated Identity Management; Identity and Access Management; Single Sign-On*

**Authentify**
*Participation: Presentation*
Brian Kregas, Sales Associate
Brian.Kregas@authentify.com, 773-243-0325
www.authentify.com
*Product Categories: Authentication; Identity and Access Management; Mobile Security*

**Bricata**
*Participation: Wednesday General Session Sponsor*
Joe Charron, Vice President, Marketing
jcharron@bricata.com, 949-280-9450
www.bricata.com
*Product Categories: Cloud Security; Intrusion Detection and Prevention; Network Security*

**Click Security**
*Participation: Presentation;*
James Foulk, Manager, Business Development
jfoulk@clicksecurity.com, 512-637-8500 x107
www.clicksecurity.com
*Product Categories: Incident Handling and Response; Intrusion Detection and Prevention; Network Security*

**CloudLock**
*Participation: Corporate Display; Presentation; Wednesday Breakfast Sponsor*
Brenton Newell, Sales Director, SLED
brenton@cloudlock.com, 781-966-4332
www.cloudlock.com
*Product Categories: Cloud Security; Encryption; Security Policies*

**Cloudpath Networks**
*Participation: Corporate Display*
Kevin Koster, Founder and CEO
kevin@cloudpath.net, 303-495-3374
www.cloudpath.net
*Product Categories: Identity and Access Management; Mobile Security; Network Security*

**Epson, Gold Partner**
*Participation: Projector Sponsor*
Sean Gunduz, Product Manager
sean_gunduz@ea.epson.com, 562-981-3840
www.epson.com/education
*Product Categories: Classroom Control Systems; Hardware; Wireless*

**EventTracker**
*Participation: Corporate Display*
Laurie Woolworth, SIEM specialist
LaurieW@eventtracker.com, 410-215-2979
www.eventtracker.com
*Product Categories: Critical Infrastructure Protection; Intrusion Detection and Prevention; PCI DSS*

**FireEye**
*Participation: Corporate Display*
Tom Guarente, National Director, Education
Tom.Guarente@fireeye.com, 216-509-1533
www.fireeye.com
*Product Categories: Cloud Security; Data Security; Network Security*

**Fischer International Identity, Silver Partner**
*Participation: Corporate Display*
Mark Cochran, Sales Director
mdc@fischerinternational.com, 603-566-7256
www.fischerinternational.com/edu
*Product Categories: Federated Identity Management; Identity and Access Management; Single Sign-On*

**iboss Cybersecurity**
*Participation: Corporate Display*
Tom Monreal, Inside Sales Manager
Tom.Monreal@iboss.com, 877-742-6832
www.iboss.com
*Product Categories: Cloud Security; Data Security; Network Security*

**Identity Finder**
*Participation: Corporate Display; Tuesday Lunch and Roundtable Sponsor*
Chris Arold, Senior Vice President, Higher Education Sales
chris.arold@identityfinder.com, 973-944-0626
www.identityfinder.com
*Product Categories: Data Security; Information Security Governance; PCI DSS*
Impulse Point
Participation: Corporate Display; Presentation
Tim Evans, Vice President, Sales
tevans@impulse.com, 508-330-8212
impulse.com
Product Categories: Identity and Access Management; Network Security; Security Policies

iScan Online
Participation: Corporate Display; Presentation
Billy Austin, President
austin@isconline.com, 214-276-1148
www.iscanonline.com
Product Categories: Data Security; Security Risk Management; Vulnerability Management

Jenzabar, Platinum Partner
Participation: Totebag Sponsor
Peter Denly, Business Development Representative
Peter.Denly@jenzabar.com
www.jenzabar.com
Product Categories: Cloud Computing and Services; CRM; ERP

Kroll
Participation: Tuesday Reception Sponsor
Steven Littleson, Director
steven.littleson@kroll.com, 615-577-6760
Kroll.com
Product Categories: Data Security; Network Security; Privacy

OpenDNS
Participation: Corporate Display; Presentation; Print Program Sponsor
Austin Bates, Higher Education Account Manager
austin@opendns.com, 415-344-3284
www.opendns.com
Product Categories: Cloud Security; Data Security; Security Architecture

Pearson, Platinum Partner
Participation: Mobile App Sponsor
Caroline Leary, Marketing Manager
caroline.leary@pearson.com
www.pearsononlinelearning.com
Product Categories: Learning Analytics; Online Learning; Student Retention

Qualys
Participation: Corporate Display; Hotel Room Key Sponsor; Presentation
Andrew Moore, Sales
info@qualys.com, 650-801-6100
www.qualys.com
Product Categories: Identity Theft; Security Risk Management; Vulnerability Management

Security Architects
Participation: Corporate Display
David Bailey, Vice President of Business Development
dtbailey55@gmail.com, 773-960-4175
www.security-architect.com
Product Categories: Identity and Access Management; Security Advisory and Consulting; Security Risk Management

Sonic Foundry, Platinum Partner
Participation: Webcast Sponsor
Sean Brown, Vice President of Education
getinfo@sonicfoundry.com, 608-443-1600
www.sonicfoundry.com
Product Category: Content Capture; Media Production, Preservation, and Storage; and Online Learning

Symantec Corporation, Silver Partner
Participation: Corporate Display; Presentation
Ben Orencia, Business Development Manager
ben_orencia@symantec.com, 503-614-7931
www.symantec.com

WinMagic Data Security
Participation: Corporate Display
Fiona Richardson, Field Marketing Manager
fiona.richardson@winmagic.com, 905-502-7000 x3220
www.winmagic.com
Product Categories: Cloud Security; Encryption; Privacy

Wisegate IT
Participation: Corporate Display; Hotel Door Drop Sponsor
Scott LeSueur, Global Director, Education and Academic Medical Centers
scott.lesueur@wisegate.org, 801-557-6115
www.wisegate.org
Product Category: Security Advisory and Consulting
Keep growing.

For a comprehensive list of upcoming events, please visit educause.edu/Events.

**MAY**

Security Professionals Conference
May 4–6
Minneapolis, MN, and Online

Leading Change Institute
May 31–June 5
Washington, DC

**JUNE**

Administrative IT Summit
June 22–24
Seattle, WA

**JULY**

Leadership Program
July 6–10
Philadelphia, PA

Breakthrough Models Academy
July 13–17
Chicago, IL

Learning Technology Leadership Program
July 13–17
Philadelphia, PA

Management Program
July 13–17
Philadelphia, PA

Breakthrough Models Incubator
July 28–31
Washington, DC

**SEPTEMBER**

ELI Focus Session
September 15–17
Online

**OCTOBER**

Annual Conference
October 27–30
Indianapolis, IN, and Online

Ongoing

EDUCAUSE Live! Webinar Series

ELI Online Courses
Easily extend threat protection on- and off-campus.

Proactive, Cloud-delivered network security and Web filtering protecting any device, anywhere.

- Eliminate malware and botnets, while providing an open internet environment
- Easily scales with your university’s bandwidth needs
- Deploy across your entire university in minutes

FREE TRIAL
GET STARTED IN 30 SECONDS: www.opendns.com