Security Professionals Conference 2013

No Boundaries: Security in an Open World

APRIL 15-17
ST. LOUIS, MISSOURI, AND ONLINE
Hilton St. Louis at the Ballpark
Thank you to our sponsors who enhance the conference experience through support of attendee activities.

**PLATINUM PARTNER**

mediasite®
by sonicfoundry®

**GOLD PARTNER**

EPSON®
EXCEED YOUR VISION

**BRONZE PARTNER**

NetApp™

**ADDITIONAL SPONSORS**

aegisIDENTITY
www.aegisidentity.com | @aegisidentity

brinqa

Kroll Advisory Solutions™

QUALYS®
ON DEMAND SECURITY

Symantec

tenable
network security

umbrella
by OpenDNS

Together we’ll explore the inevitable changes to cybersecurity architecture and drivers, as well as new solutions for the multitude of security and privacy challenges.
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).

educause.edu | internet2.edu | educause.edu/Security | ren-isac.net
## CONNECTING ON-SITE

### Wireless Access

To access the wireless network in the meeting space, please follow the instructions below. Wireless is available during registration hours.

- Set your wireless adapter SSID to **EDUCAUSEAIR**.
- Launch a web browser.
- Enter the passphrase **educause** (case sensitive) on the splash screen inside your browser.

Please be respectful and limit your use of personal MiFi devices. These will disrupt the wireless experience for those around you.

### Mobile Device Etiquette

As a courtesy to the speakers and other participants, we ask that you silence all mobile devices during conference sessions. We also ask that you limit your mobile device use so bandwidth is not exceeded.

### E-Mail and Computer Kiosks

Computer and print stations are available during registration hours in the Walnut Foyer.

### Joint Reception

**SPONSORED BY OPENDNS**

One of the most valuable aspects of this conference is the opportunity to connect face-to-face with fellow attendees. This year you’ll also have the opportunity to connect with attendees from the Enterprise IT Leadership Conference and the Advanced Core Technologies Initiative Annual Meeting. Join us to relax over food and drinks, get to know your colleagues, and discuss enterprise security and infrastructure issues.

### Participant Lists

Visit [educause.edu/SEC13/Registration-List](educause.edu/SEC13/Registration-List) to search a list of your fellow participants and sort by their name, organization, or geographic location. Use this as an opportunity to connect with other attendees on-site. **NOTE:** Lists are for noncommercial use by conference participants only; login required.

### Social Media

Add your voice to the dynamic conference backchannel conversation through blogs, social bookmarking sites, or photo-sharing services with the tag **SEC13**. You can also share your conference experience in “real time” with others on Twitter using the hashtag **#SEC13**.
CONFERENCE FEATURES

Mentoring

The Security Professionals Conference 2013 Program Committee has launched a mentoring program for new security managers, directors, and CISOs. Learn more during the free session “Successful Mentoring Relationships for Career Development” on Monday, April 15, 4:45–5:30 p.m. Additional career development, mentoring, and community building opportunities will be available at Security 2013. Learn more at educause.edu/SEC13/Mentoring.

Webcasts

WEBCAST RECORDINGS PROVIDED BY SONIC FOUNDRY, PLATINUM PARTNER

The general sessions and seven 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.

Connect Lounge

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

Lunchtime Roundtables

SPONSORED BY BRINQA

Join a conversation while you lunch. A mix of important topics will be facilitated by committee members and members of HEISC.

Get Your Game On!

Join us for the premiere of the Security Professionals and Enterprise IT Leadership Conferences game night. This will be a great way to help you get to know your fellow conference-goers. 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. Find a seat, and get your game on!

Corporate Displays

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

This year, the program committee is encouraging attendees to participate in optional organized dinner outings for small groups. Sign-up sheets for a few local restaurant choices will be available near the conference registration desk on Monday and Tuesday. Any expenses incurred are the responsibility of the individual attendee. Groups will meet in the lobby and walk or take cabs to the restaurant of their choice. Don’t forget to be back at the hotel for the evening activities.

REN-ISAC 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. This meeting will gather REN-ISAC members for a face-to-face meeting. It will be held Wednesday, April 17, from 12:00 noon to 6:00 p.m. and Thursday, April 18, from 7:30 a.m. to 1:30 p.m. Please visit the REN-ISAC information desk in the Grand Foyer if you have questions or want more agenda details. Separate registration and fee required.

CONFERENCE POLICIES

Name Badges

Your name badge verifies your registration and provides admission to functions. Please wear your name badge at all times.

Audio/Videotaping, Digital Recording, and Photography

Because all presentations and associated materials are the intellectual property of the speakers, attendees must obtain speaker 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 speakers. 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 conference, 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 conference speeches, presentations, blogs, wikis, and feeds reflects the opinions of the authors and not necessarily those of EDUCAUSE or its members.
POSTCONFERENCE RESOURCES/PROCEEDINGS

All speakers have been invited to upload their presentations and handouts to the EDUCAUSE website. These resources will be posted after the conference at educeause.edu/SEC13. Participants will be notified by e-mail when they’re available.

EVALUATIONS

Your feedback is critical for continuous improvement. You can participate in four ways:

• Provide feedback anytime. Tell us anything that can help us improve the conference experience. Go to feedback.educause.edu or send a text message to 69302 that starts with “EDUCAUSE” followed by your comments.

• Answer a quick question. EDUCAUSE staff will be collecting feedback on specific aspects of the conference. Answer our question and get a sticker that shows you’re a contributor!

• Complete speaker and session evaluations. Evaluate individual sessions by Monday, May 6. Evaluation links can be found at net.educause.edu/SEC13/sesseval or by using your handheld device to scan the QR codes adjacent to the session title on the meeting room signs.

• Submit the final overall postconference evaluation. Shortly after the conference you’ll receive an e-mail invitation asking for your input—this is vital to improving future conferences (it should take only 10 minutes to complete).

BEING GREEN

EDUCAUSE has taken the following actions to minimize the conference’s impact on the environment:

Pens: Made from 100% recycled plastic

Print programs: Printed on 30% post-consumer recycled paper

Tote bags: Made from 50% recycled material
PARTICIPATE THROUGHOUT THE YEAR

Please consider engaging with your community in the following ways:

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 on educause.edu/Events.

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

3. **Contribute as a Session Proposal Reviewer, Blogger, or Photographer**: To get started, click the “Volunteer Now” button at the bottom of the page at 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**: Constituent groups, mentoring, Institute programs, a Career Center, conferences, 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.

FINANCIAL ASSISTANCE FOR PROFESSIONAL DEVELOPMENT

Professional development builds strong contributors in our higher education IT community. 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 2014 events. Apply now, or refer a colleague who could use this, at educause.edu/Fellow.
| **Paul Howell** *(Chair)*  
Chief Information Technology Security Officer  
University of Michigan–Ann Arbor |
|---|
| **Sanjeev Sah**  
Chief Information Security Officer  
University of North Carolina Charlotte |
| **Cathy Bates** *(Vice Chair)*  
Associate Vice Chancellor and CIO  
Appalachian State University |
| **Brian Smith Sweeney**  
Project Lead  
New York University |
| **Jon Allen**  
Information Security Officer  
Baylor University |
| **Todd Spahr**  
Information Security Officer  
Towson University |
| **John C. Borne**  
Director of Information Security  
Louisiana State University |
| **Joseph E. St Sauver**  
Manager, Internet2 Nationwide Security Programs and, Manager, InCommon Certificate Program  
University of Oregon |
| **michael G. Carr**  
Chief Information Security Officer  
University of Kentucky |
| **Beth Young**  
Lead Security Analyst  
RENS-ISAC |
| **John T. Hoffoss**  
Secure Systems Analyst  
Irdeto |
| **Nathan Zierfuss**  
Chief Information Security Officer  
University of Alaska Fairbanks |
| **Julie Myers**  
Chief Information Security Officer  
University of Rochester |
Save the Date!

The best thinking in higher education IT will take place in Anaheim, California, and concurrently online October 15–18. Join us! Visit educause.edu/E13 for details.
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:30–8:00 a.m.</td>
<td>Continental Breakfast (for seminar participants) Outside Salons A and B</td>
</tr>
<tr>
<td>8:00–8:30 a.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>8:30–9:00 a.m.</td>
<td>Refreshment Break (for seminar participants) Outside Salons A and B</td>
</tr>
<tr>
<td>9:00–9:30 a.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>9:30–10:00 a.m.</td>
<td>Refreshment Break (for seminar participants) Outside Salons A and B</td>
</tr>
<tr>
<td>10:00–10:30 a.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>10:30–11:00 a.m.</td>
<td>Lunch (for seminar participants) Arch View Ballroom</td>
</tr>
<tr>
<td>11:00–11:30 a.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>11:30 a.m.–12:00 noon</td>
<td>Higher Education Information Security Council Leadership Team Meeting by invitation only Broadway</td>
</tr>
<tr>
<td>12:00–12:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>12:30–1:00 p.m.</td>
<td>Refreshment Break (for seminar participants) Outside Salons A and B</td>
</tr>
<tr>
<td>1:00–1:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>1:30–2:00 p.m.</td>
<td>Successful Mentoring Relationships for Career Development (4:45–5:30 p.m.) Salon E/F</td>
</tr>
<tr>
<td>2:00–2:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>2:30–3:00 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>3:00–3:30 p.m.</td>
<td>Successful Mentoring Relationships for Career Development (4:45–5:30 p.m.) Salon E/F</td>
</tr>
<tr>
<td>3:30–4:00 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>4:00–4:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>4:30–5:00 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>5:00–5:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>5:30–6:00 p.m.</td>
<td>Organized Dinner Outings Meet in hotel lobby</td>
</tr>
<tr>
<td>6:00–6:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>6:30–7:00 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>7:00–7:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>7:30–8:00 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>8:00–8:30 p.m.</td>
<td>Mentoring Workshop Market Street Room</td>
</tr>
<tr>
<td>8:30–9:00 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>9:00–9:30 p.m.</td>
<td>Preconference Seminars</td>
</tr>
<tr>
<td>9:30–10:00 p.m.</td>
<td>Preconference Seminars</td>
</tr>
</tbody>
</table>
7:30–8:30 a.m.
Continental Breakfast for Seminar Participants
OUTSIDE SALONS A AND B

7:30 a.m.–5:30 p.m.
Registration Open
GRAND FOYER
Connect Lounge
SALON G

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
Preconference Seminars
PLEASE NOTE: Separate registration and fee are required to attend seminars.

SEM01A
Point-to-Point Encryption and PCI Compliance: Big Promise, Hard Questions
SALON A
Walter Conway, Manager, 403 Labs, LLC

While there might not be any silver bullets to make your campus PCI compliant, Point-to-Point Encryption (P2PE) looks like it might come pretty close, at least in some situations. It can reduce a merchant’s PCI scope to the card reader, thereby removing payment applications and databases from PCI scope. The PCI Council has published its P2PE program details, and we can expect the first approved solutions soon. The questions for campuses are: what does it take for a P2PE solution to deliver the expected benefits; what will it cost; and, importantly, what alternative “approved solutions” might offer a better cost/benefit tradeoff with the same benefits?

In this session we will dive into the requirements and inner workings of P2PE, assess the real costs of implementation, and identify which campus merchants will benefit most. Then we will explore how campuses might achieve many of the same scope-reduction benefits from existing third-party encryption solutions. We will identify the hard questions to ask and describe the contract terms you must include. We also will look at possible changes to PCI version 3.0, which will take effect in 2013.

There are no silver bullets in PCI, including P2PE, but schools may have some practical options to reduce PCI scope and the cost of PCI compliance.
8:30 a.m.–4:30 p.m.

**SEM01F**

**Positioning the Information Security Program as an Enterprise Resource**

**SALON B**

**Cathy Hubbs**, CISO, and **Eric Weakland**, Director, Information Security, American University

This interactive session will provide an overview of areas such as expanding the information security program, gaining broad support, focusing direction, and planning for what comes next. Many information security seminars and classes focus either on specific areas of the security landscape or technical tools and methods. While these subjects provide useful information and skills needed to operate a security program, they do not offer sufficient guidance on the development of the information security program itself. This seminar will focus on the management and leadership issues necessary to launch and sustain a program. We will take a look at how to gain executive and institutional sponsorship, assess risk, examine staffing models, develop policy, raise campus-wide awareness, and explore measuring progress and resources available to virtually extend our institution’s workforce. Participants will be given an opportunity to discuss and potentially address security issues from their own institutions.

10:00–10:30 a.m.

**Refreshment Break for Preconference Seminar Participants**

OUTSIDE SALONS A AND B

10:00 a.m.–4:30 p.m.

**SEM02F**

**Hack in the Rack: Building and Using a Hacking Simulation Environment to Better Defend Your Network and Engage the Community**

**GATEWAY I**

**Marshall Graham**, Network Administrator, Carl Junction R-1 School District; **Ryan Halstead**, Security Services Manager, and **Albert Stadler**, CIO, Missouri Southern State University

This seminar is designed for beginning security ethical hacking participants or those interested in learning more about how to use hacking for a defensive advantage. It also explains how to start the conversation about information security awareness in your local community.
12:00 noon–1:00 p.m.
Lunch for Preconference Seminar Participants
ARCH VIEW BALLROOM

Lunch is provided if you’re attending both a morning and afternoon seminar or a full-day seminar. A lunch ticket is required.

12:00 noon–4:30 p.m.
Higher Education Information Security Council (HEISC) Leadership Team Meeting
(by invitation only)
BROADWAY

1:00–4:30 p.m.
SEM02P

From Romania with Love (and Forensics)
SALON A

Mark Shelhart, Manager–Incident Response and Forensics, 403 Labs, LLC

Very few companies are willing to share the details of their data compromise. In this session we are going to cover the full life cycle of a data breach. Instead of talking statistics, we’re going to use facts from current, active investigations. We’ll start with how the attacks are discovered and the human emotions that go along with them. We will go in-depth into how the attacker functions and operates within the victim’s environment. This will include views into real malware and the forensic tools used during the investigations.

While many presentations stop at this point, we’ll discuss the aftereffects of a breach within an organization, involving facts around financial and legal ramifications. We’ll also cover rarely discussed problems such as contracts with third parties pre- and post-breach. Unpublished details of law enforcement’s interactions will also be discussed as part of this life cycle.

Although the topic is forensics, this presentation will be presented in “plain English” for everyone to enjoy.
1:00–4:30 p.m. cont.

**SEM03P**

**Physical Security for the Security Professional**

**SALON E/F**

**Zach Campbell,** Senior Security Consultant, Fraternal Order of Lock Sport

Is that a wafer lock or a disk retainer lock guarding your filing cabinet? Do you have to badge out, or did that door just unlock automatically as you exited the building? Why does it matter anyway? In this seminar you will learn lock picking and what characteristics affect a lock’s security. You will also learn how to evaluate physical security for a room or building and what common mistakes are made.

2:30–3:00 p.m.

**Refreshment Break for Preconference Seminar Participants**

Outside Salons A and B

4:45–5:30 p.m.

**Meeting**

**Successful Mentoring Relationships for Career Development**

**SALON E/F**

**Theresa Semmens,** Chief IT Security Officer, North Dakota State University; **Brian Basgen,** Assistant Vice Chancellor for IT (Acting), Pima County Community College District; **David Seidl,** Director of Information Security, University of Notre Dame

Participation in mentoring activities can be a key success factor in your career development. But how do you start? How do you find the right mentor or set of mentors for your situation? What should the focus of your conversations be? This session will help you answer these questions and understand what to focus on in mentee/mentor conversations. We will cover important mentoring resources, benefits, styles, and functions, as well as setting expectations. Whether you want to find a mentor or a coach, or you want to be one, join this lively session; make a difference in your career planning and development.
MONDAY, APRIL 15

6:00–8:00 p.m.
Organized Dinner Outings
MEET IN HOTEL LOBBY

This year, the program committee is encouraging attendees to participate in optional organized dinner outings for small groups. A few local restaurant choices will be available for sign-up near the conference registration desk starting Monday morning. Any expenses incurred are the responsibility of the individual attendee. Groups will meet in the lobby to walk or take cabs to the restaurant for a 6:15 p.m. reservation. Don’t forget to be back at the hotel by 8 pm for the mentoring workshop!

Security Professionals 2013 Program Committee Dinner
(by invitation only)

8:00–10:00 p.m.
Mentoring Workshop
MARKET STREET ROOM

Brian Smith Sweeney, Project Lead, New York University; Beth Young, Lead Security Analyst, REN-ISAC

This informal session will allow speakers to spend some time practicing their presentations in front of program committee members and colleagues. Content will not be critiqued, but advice will be shared on presentation delivery, slide effectiveness, and session interactivity. Anyone speaking at the Security Professionals Conference is encouraged to attend, especially those who may be presenting for the first time. NOTE: A projector will not be available. Please bring your own laptop or a few printouts to share your presentation.
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:00–6:45 a.m.</td>
<td>Breakfast</td>
</tr>
<tr>
<td></td>
<td>Arch View Ballroom</td>
</tr>
<tr>
<td>6:45–7:15 a.m.</td>
<td>Connect Lounge</td>
</tr>
<tr>
<td></td>
<td>Open Salon G</td>
</tr>
<tr>
<td>7:15–7:45 a.m.</td>
<td>General Session</td>
</tr>
<tr>
<td></td>
<td>Salon C/D</td>
</tr>
<tr>
<td>7:45–8:15 a.m.</td>
<td>Refreshment Break and Corporate Displays</td>
</tr>
<tr>
<td></td>
<td>(9:45–10:30 a.m.)</td>
</tr>
<tr>
<td>8:15–8:45 a.m.</td>
<td></td>
</tr>
<tr>
<td>8:45–9:15 a.m.</td>
<td></td>
</tr>
<tr>
<td>9:15–9:45 a.m.</td>
<td></td>
</tr>
<tr>
<td>9:45–10:15 a.m.</td>
<td></td>
</tr>
<tr>
<td>10:15–10:45 a.m.</td>
<td></td>
</tr>
<tr>
<td>10:45–11:15 a.m.</td>
<td></td>
</tr>
<tr>
<td>11:15–11:45 a.m.</td>
<td></td>
</tr>
<tr>
<td>11:45 a.m.–12:15 p.m.</td>
<td></td>
</tr>
<tr>
<td>12:15–12:45 p.m.</td>
<td></td>
</tr>
<tr>
<td>12:45–1:15 p.m.</td>
<td></td>
</tr>
<tr>
<td>1:15–1:45 p.m.</td>
<td></td>
</tr>
<tr>
<td>1:45–2:15 p.m.</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Event</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>2:15–2:45 p.m.</td>
<td>Registration Open</td>
</tr>
<tr>
<td>2:45–3:15 p.m.</td>
<td>Corporate and Campus Solutions</td>
</tr>
<tr>
<td>3:15–3:45 p.m.</td>
<td>Refreshment Break and Corporate Displays</td>
</tr>
<tr>
<td>3:45–4:15 p.m.</td>
<td>Connect Lounge Open</td>
</tr>
<tr>
<td>4:15–4:30 p.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>4:30–5:00 p.m.</td>
<td>Concurrent Sessions</td>
</tr>
<tr>
<td>5:00–5:30 p.m.</td>
<td>Joint Reception</td>
</tr>
<tr>
<td>5:30–6:00 p.m.</td>
<td>PGP Key Signing</td>
</tr>
<tr>
<td>6:00–6:30 p.m.</td>
<td>Organized Dinner Outings</td>
</tr>
<tr>
<td>6:30–7:00 p.m.</td>
<td>Get Your Game On!</td>
</tr>
<tr>
<td>7:00–7:30 p.m.</td>
<td></td>
</tr>
<tr>
<td>7:30–8:00 p.m.</td>
<td></td>
</tr>
<tr>
<td>8:00–8:30 p.m.</td>
<td></td>
</tr>
<tr>
<td>8:30–9:00 p.m.</td>
<td></td>
</tr>
<tr>
<td>9:00–9:30 p.m.</td>
<td></td>
</tr>
<tr>
<td>9:30–10:00 p.m.</td>
<td></td>
</tr>
<tr>
<td>10:00–10:30 p.m.</td>
<td></td>
</tr>
</tbody>
</table>
7:15–8:15 a.m.
Breakfast
_Sponsored by Brinqa_
ARCH VIEW BALLROOM

7:15 a.m.–5:30 p.m.
Connect Lounge
SALON G
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.

7:15 a.m.–6:00 p.m.
Registration Open
GRAND FOYER

8:15–8:45 a.m.
General Session

**Welcome and Introductions**
SALON C/D

Fred H. Cate, Distinguished Professor School of Law and Director, Center for Applied Cybersecurity Research, Indiana University Bloomington; Michele Norin, CIO, The University of Arizona; Paul Howell, Chief Information Technology Security Officer, University of Michigan–Ann Arbor

8:45–9:45 a.m.
General Session

**Cyber War: You’re Doing It Wrong!**
_Sponsored by Aegis Identity Software_
SALON C/D

Marcus J. Ranum, CSO, Tenable Network Security

No matter how you slice it, cyber war is technologically and militarily impractical. We’ve been talking about it for a long time, but the discussion has been (and still is) misleading and inaccurate. Several issues (cybercrime, cyber espionage, cyber terror) are grouped under the rubric of cyber war, but they have different and sometimes conflicting agendas. This discussion looks past the hype.
9:45–10:30 a.m.

Refreshment Break and Corporate Displays
GRAND FOYER

Thirteen leading security technology companies will be available during the morning and afternoon breaks. Learn more about products and services and interact with company representatives showcasing security technology solutions for higher education.

**Aegis Identity Software**

Aegis Identity Software’s TridentHE Identity Manager is designed by our IdM experts with 100% focus on the education community, large and small. Leveraging open-standard technologies and higher education licensing, TridentHE offers colleges and universities cost-effective and supportable identity management.

**Authentify**

Authentify offers flexible out-of-band authentication (OOBA) services for strengthening the security of account access or verifying legitimate account activity. Authentication and verification are provided by engaging end users in synchronized exchanges between their online accounts and separate voice or data channels via their telephones, smartphones, or tablets. The end user’s phone or other smart device becomes an effective proxy for a security credential.

**CloudLock**

CloudLock provides an information security suite that lets organizations implement data privacy practices and data governance to manage data in Google Docs, Sites, and Drive. CloudLock also lets organizations implement governance for third-party apps. The largest Google Apps customers in the world trust CloudLock to secure their data.

**Cloudpath Networks, Bronze Partner**

Cloudpath Networks brings WPA2 enterprise wireless security to all, enabling campuses to increase the use of wireless security by students, faculty, contractors, and guests. Winner of the 2012 Best of Interop award, XpressConnect simplifies WPA2 enterprise and 802.1X through automated, self-service provisioning across a wide array of user-owned devices for both password-based and certificate-based networks.

**Identity Finder**

Identity Finder is a global leader in sensitive data discovery and security. Founded in 2001, we provide organizations with advanced technology to
help prevent data leakage. Our data loss prevention software finds and protects data at rest and in use, either centrally or at the end point, by searching files, e-mails, desktops, servers, databases, and websites.

Impulse Point

SafeConnect is the smart choice for controlling the chaos created by unmanaged devices demanding access to your network. Better control is possible through identity, visibility, and automated actions. Get smarter about mobile devices, user identity, guest access, and security posture. Visit www.impulse.com for more information.

Lancope

Lancope is a leading provider of network visibility and security intelligence to defend enterprises against today’s top threats. By collecting and analyzing NetFlow, IPFIX, and other types of flow data, Lancope’s StealthWatch system helps organizations quickly detect a wide range of attacks, from APTs and DDoS to zero-day malware and insider threats. Through pervasive insight across distributed networks, including mobile, identity, and application awareness, Lancope accelerates incident response, improves forensic investigations, and reduces enterprise risk. Lancope’s security capabilities are continuously enhanced with threat intelligence from the StealthWatch Labs research team. For more information, visit www.lancope.com.

OpenDNS

Leading colleges and universities choose Umbrella by OpenDNS for cloud-delivered Internet security that’s easy to manage and scale. Secure all your networks and users from malware, botnets, and phishing and manage everything through a single web-based dashboard. Our customers include Vanderbilt University and George Washington University.

Qualys

Qualys is a pioneer and leading provider of cloud security and compliance solutions, with over 6,000 customers in more than 100 countries and partnerships with leading managed service providers and consulting organizations worldwide. The QualysGuard Cloud Platform and integrated suite of solutions helps organizations simplify security operations and lower costs.

Symantec Corporation

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, ensuring confidence wherever information is used or stored.

**ThreatTrack Security**

ThreatTrack Security specializes in helping organizations identify and stop advanced persistent threats (APTs), targeted attacks, and other sophisticated malware designed to evade the traditional cyberdefenses deployed by businesses, enterprises, and government agencies around the world. We develop advanced cybersecurity solutions that analyze, detect, and remediate the latest malicious threats.

**TouchNet Information Systems, Bronze Partner**

Since 1989, more than 700 colleges and universities have relied on TouchNet to automate, streamline, and secure campus commerce transactions. Today, TouchNet U.Commerce is a premier software solution for higher education, helping institutions save, make, and manage money better throughout the campus enterprise.

**Websense**

Websense is a global leader in unified web security, e-mail security, mobile security, and data loss prevention (DLP). Websense TRITON content security solutions help institutions leverage social media and cloud-based communication while protecting them from advanced persistent threats and modern malware, preventing the loss of confidential information and enforcing Internet use and security policies.

10:30–11:15 a.m.

**Concurrent Sessions**

**Assess and Protect**

**The Security Challenges of Nonpersistent Virtual Desktops**

**SALON B**

Christopher A. Bennett, Director of Information Security and Infrastructure Support, Jonathan DeForest, Storage and System Administrator, and Quentin L. McCallum, Information Security Analyst, Lansing Community College

Virtual desktop infrastructure (VDI) can deliver many operational advantages, which include a consistent user experience and environmental savings (electricity, HVAC, etc.). An implementation of virtual desktops may introduce a challenge for the information security practitioner. A virtual desktop configured to return to the original starting point is generally called “nonpersistent.” A nonpersistent desktop allows for unwanted activity to be done with no digital footprint. A security professional must use network-level logging, targeted packet captures, and administrative tools within the virtual desktop solution to mitigate this risk.
10:30–11:15 a.m. cont.

**Detect and Respond**

**Using DNS to Identify, Mitigate, and Prevent Infections**

GATEWAY III

*Kevin Wilcox*, Networking Specialist, Appalachian State University

Most of our environments demand that we support almost every type of end-user device available (tablets, laptops, phones, Internet TVs, and more). One of the few commonalities among all these devices is their use of DNS. Through the use of passive DNS logging and DNS sinkholes we have another tool at our disposal to help identify compromises on any device and, in many cases, to even stop drive-by infections from ever occurring.

**HEISC and Partners**

**Avoid Reinventing the Wheel: Using the EDUCAUSE Information Security Guide to Help Address BYOD Risks**

SALON A

*Theresa Semmens*, Chief IT Security Officer, North Dakota State University; *Marcos Vieyra*, CISO, University of South Carolina

Do you have a BYOD-specific policy? Should you? Is BYOD an entirely new issue for security professionals, requiring radical new thinking, or can we apply already established principles and thought to this problem? Are you currently wrestling with these questions at your institution? If you sometimes have the nagging feeling that you might be reinventing the wheel, you are not alone! Don’t reinvent the wheel - join us for a brief overview of BYOD-related resources available in the Information Security Guide.

**New to the Game**

**Congratulations! You’ve Just Been Named Your Institutions ISO, So What Do You Do Now?**

GATEWAY I

*Neal Fisch*, Director, Enterprise Services and Security, California State University, Channel Islands

 Newly appointed information security officers have a daunting task ahead of them. Walking into this new position, established or not, can have a paralyzing effect on you if you’re new to the area of information security. As a newly appointed ISO, the speaker experienced both trepidation and excitement. This session will discuss steps that will help you not only move forward but also succeed in your newly appointed role.
Privacy

**How Do I Get There from Here? Security-to-Privacy Career Migration**

**SALON E/F**

**Jane Rosenthal**, Director of Privacy, University of Kansas; **Michael G. Carr**, CISO, University of Kentucky

Privacy has quickly become an in-demand field that many security professionals aspire to, but how do you move from security to privacy, and what skills are needed to become a chief privacy officer? Following a brief review of the privacy field and framework, this session will focus on the presenters’ experience as security and privacy officers at major research institutions, a CPO’s requisite skill set, and a typical day in the life of a CPO, the pros and cons of having a dedicated privacy officer (or combining the role with security), and career roadmaps to move into privacy.

Strategic Security

**The 20 Critical Controls: A Campus Security Strategy**

**GATEWAY II**

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

The 20 Critical Controls are quick wins that allow you to rapidly improve your cybersecurity without major procedural or technical change. International cybersecurity experts developed the 20 Critical Controls to be the most effective and specific set of technical measures to counter the most common and damaging computer attacks. The controls address the root causes of these attacks to ensure your security measures are effective. This presentation will also discuss how VA Tech is implementing the 20 Critical Controls as part of its overall security strategy.

11:30 a.m.–12:15 p.m.

Concurrent Sessions

Assess and Protect

**Proven Strategies for Web Application Security**

**GATEWAY III**

**Justin C. Klein Keane**, Senior Information Security Specialist, University of Pennsylvania

Web application security is the Sisyphean task facing institutions of all sizes. Approaching web application security is an extremely daunting task. University of Pennsylvania’s School of Arts and Sciences has completed a multiyear initiative to secure our existing web applications and deploy a secured application development platform for the future. Learn about winning strategies for getting a handle on your existing web application portfolio as well as techniques for establishing a secure application base in order to migrate toward a secure, sustainable web application environment.
Detect and Respond

2012: p0wnage and Detections
SALON A


We will present an in-depth analysis of several security incidents from 2012 to showcase the intrusion detection and incident response techniques used at Berkeley Lab, highlighting how our security monitors clearly flagged some compromises while examining why others were missed. We’ll also highlight the interesting consequences of detection techniques that result in finding malicious but occasional events and discuss how the analysis we conducted on these incidents provides a basis for attack modeling and the design of new methods for security monitoring and response.

HEISC and Partners

Introduction to the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC)
GATEWAY I

Kerry Havens, Information Risk Manager, University of Colorado Boulder

Come learn how the REN-ISAC can help you protect your organization from the multitude of security and privacy challenges that we face as security professionals in higher education. Whether you’re looking to feed your intrusion detection system with threat intelligence data from trusted sources all over the world or needing ideas on writing an effective mobile device policy, the REN-ISAC organization and community can get you the resources you need to get your job done.

New to the Game

When to Declare an Information Security Incident and How to Respond Once You Do
SALON E/F

Cornelis Leune, Information Security Officer, Adelphi University; Robert K. Henry, CISO, Santa Clara University

This discussion session will examine the incident response process and apply it to a sanitized version of an actual web server compromise that took place at a real university. After an initial overview of the incident response process, attendees will be presented with a series of clues and will discuss how to respond as the clues accumulate.
Privacy

Information Security and Privacy Strategy Futures for Higher Education
GATEWAY II
Robert Ono, IT Security Officer, University of California, Davis

University security breaches are reported in our headlines on a regular basis. These security incidents may result in increasingly harsh regulatory sanctions and/or threaten public support of our teaching, research, and public service programs. Have higher education information security and privacy programs made sufficient progress? What types of security and privacy program initiatives could improve management of information threats within higher education? How could incentives ensure institutional participation so that lesser-resourced institutions can equally participate in and benefit from a broad higher education security program strategy? This session will explore these themes and offer suggestions for improvements for a national higher education security and privacy strategy.

Strategic Security

Administration of Data Loss Prevention Services in Higher Education
SALON B

This presentation will examine the challenges, shortcomings, potential solutions, and areas for improvement in deploying and administering a data loss prevention (DLP) tool in a highly distributed IT environment. The talking points will range from setting up the infrastructure and supporting the needs of IT staff and end users to how governance and enforcement (or lack thereof) impacts the service.
12:15–1:15 p.m.

Lunch and Roundtable Discussions

*Sponsored by Brinqa*

ARCH VIEW BALLROOM

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 discussions 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.

**Career Progression Plan for Security Professionals**

- CISO Networking
- Cloud Privacy and Security
- Compliance and Governance
- E-Discovery and Forensics
- Encryption
- Identity and Access Management
- InCommon
- InCommon Assurance
- Late-Breaking Topics
- Mobile Device Security and Privacy
- Multi-Factor/Two-Factor Authentication
- Network Security
- Privacy in Higher Education
- Risk Analytics
- Risk Assessment Strategies
- Security Awareness
- Security for Research
Concurrent Sessions

Assess and Protect

Security Smackdown: End-User Awareness Programs vs. Technology Solutions

SALON E/F

Christine Brisson, Senior IT Project Leader, and Justin C. Klein Keane, Senior Information Security Specialist, University of Pennsylvania

How effective is end-user security awareness education? Would it be better to allocate our scarce resources to improving our technology? Two members of the same information security team at the University of Pennsylvania will square off on opposite sides: “They’ll never learn and they shouldn’t have to!” versus “We’re only as strong as our weakest user!” In a point-counterpoint format, we will consider various types of end-user awareness tools (blogs, videos, etc.) and the sorts of problems they aim to solve. We’ll debate whether we are effectively reaching our end users and if technological alternatives are within our reach that can accomplish similar ends.

Detect and Respond

How Advanced Log Management Can Trump SIEM: Tales of Woe and Glory

SALON B

Donald Becker, Information Security Engineer, and Cornelis Leune, Information Security Officer, Adelphi University; Vlad Grigorescu, Senior Information Security Engineer, Carnegie Mellon University

Network situational awareness is a prerequisite for mature information security operations. Achieving and maintaining a sufficient level of situational awareness is a challenge, often amplified in higher education institutions having highly decentralized governance models. Application and system logs, even if available to an operational security group, have become less effective as the number of devices, services, and users has increased. The existing Security Information and Event Management (SIEM) solutions usually are too costly, time-intensive, or a poor fit for educational networks.

Adelphi University replaced their SIEM with a log management platform and haven’t looked back. Carnegie Mellon University uses open-source tools to index log data in near-real time and search terabytes of data in milliseconds, and a custom-built web interface lets analysts quickly drill down to unusual events.
Securing the App: Protecting Your Critical Data

Frank Kim, Curriculum Lead, The SANS Technology Institute

Institutions of higher education are a critical part of the innovation infrastructure. They are the gateway for important research. They hold personal records of future leaders of the country. And they are constantly under attack. Many of these attacks exploit weaknesses in the software and applications used to process critical research as well as faculty and student data. Properly securing the app against the backdrop of emerging cloud, mobile, and social paradigms is a key component in a university’s ability to reduce risk, protect its reputation, and ensure compliance.

Creating an IT Security Baseline

Cory Chrisinger, Information Security Risk Analyst, James Lowe, CISO, and Allen Monette, Endpoint Security Consultant, University of Wisconsin–Madison

The UW–Madison Office of Campus Information Security has worked with the campus community to develop a baseline information systems security standard that’s intended to help departments on campus create a measurable and minimally acceptable baseline security program. The technical controls have been developed collaboratively with campus departments and vetted through various on- and off-campus groups. The baseline security standard outlines security controls all campus IT departments should implement including controls for endpoint security, access control, physical security, policy and awareness, and application security for custom web applications.

BYOD as the Nexus of Security and Privacy

Patrick John Feehan, Director, IT Privacy and Cybersecurity Compliance, Montgomery College; Jane Rosenthal, Director of Privacy, University of Kansas

This session will look at legal and privacy issues as they intersect with security issues surrounding the proliferation of portable consumer devices, whether provided by a college or brought to campus by students, staff, or faculty. This consumerization trend on the part of users, as well as the growing demand for college-provided portable devices, requires that institutions possess full knowledge of the legal and privacy issues inherent in security controls that professionals deploy to secure college information. This session will encourage discussion about security, privacy, and policy as they apply to real-world use of devices.
Strategic Security

Information Security or Identity and Access Management?

GATEWAY I

Thomas J. Barton, Senior Director, Architecture, Integration, and CISO, University of Chicago; Christopher Misra, Associate CIO for Security, University of Massachusetts Amherst

Information security shares a complex and interrelated space with identity and access management. IAM forms the basis for many of the other security controls we deploy; however, often there are gaps in understanding or even adversarial relationships between the responsible parties. This session will discuss and explore approaches to solving this problem.

2:15–3:00 p.m.

Corporate and Campus Solutions

Built-In Security for Georgia Tech

SALON A

Jason Belford, Principal Information Security Engineer, Georgia Institute of Technology; Scott J. Simpson, Technical Account Manager, Qualys

As a top-ranked, internationally recognized college and research facility, Georgia Tech has a broad and vast IT network, with more than 75,000 IP addresses for its networked devices, including user endpoints, firewalls, servers, and routers. In this session, learn how Georgia Tech effectively manages IT security and compliance across its systems using QualysGuard cloud solutions, enabling Georgia Tech to empower systems owners, reduce system administration time, and lower costs. Hear how the “time to change” has been reduced from 48 hours to just a few minutes while ensuring security standards are met. We will also share the technology and workflows that help Georgia Tech accurately identify and organize its assets, scan them for vulnerabilities, and quickly remediate any issues.

BYOD: Security, Mandates, Applications (Do You Have It Covered?)

GATEWAY III

Theresa Semmens, Chief IT Security Officer, North Dakota State University; Renault Ross, National Security and Privacy Architect, Symantec

With the rapid proliferation of mobile devices, universities are faced with developing policies and strategies around securely implementing BYOD into their existing environment. The session will discuss security threats and best practices to support BYOD initiatives that institutions should consider: app security, mobile payments, tablets, and data sharing across campuses and departments. We will also discuss recommendations on industry security capabilities to better help higher education address external mandates (HEOA, FERPA, PCI).
How Google Apps Changes the Way IT Is Delivered in Higher Education

**SALON E/F**

**Eric Chaves**, Solutions Engineer, CloudLock; **Robert K. Henry**, CISO, Santa Clara University

Google Apps lets universities transform the way they deliver IT. The platform extensibility and ecosystem of third-party applications allow students, staff, and faculty to work the way they live by adopting the web and mobile apps that make them most productive. Universities are taking advantage of the cloud’s collaboration and cost-savings benefits, but must still address information security and compliance. This presentation will discuss protecting PII, SSNs, and research data; addressing regulations like FERPA; enabling secure collaboration; creating content-based security policies; managing access rights to documents of departing faculty and staff; and managing third-party apps.

Managing Risk and Compliance by Implementing DLP to Ensure Data Security

**SALON B**

**Becky Maycock**, Director, Product Management and Marketing, Impact Technologies; **David Hendel**, Project Office Manager, Saint Louis University

Did a university e-mail contain employee PII data? Did we just FTP a file that contains alumni PCI data? In this seminar, you will learn how Saint Louis University increased its ability to prevent the loss of restricted, sensitive, and confidential data. Hear the university's strategy to use DLP to elevate compliance and win grants. Detection of data loss is the first step in preventing loss. In this session, we will discuss simple means to mitigate the risk and exposure of the data-loss problem.

A Model for Today: Partnering with Industry to Enhance Institutional Information Security Capabilities

**GATEWAY II**

**Brian Kenyon**, Senior Director, Solution Architecture, McAfee; **Jonathan Maurer**, Information Security Officer, and **Ben Woelk**, Information Security Policy and Awareness Analyst, Rochester Institute of Technology

Many academic organizations are facing the same problems: an aging decentralized computing infrastructure, growing use of mobile devices, increasing use of network resources, and ever-present external threats. To keep pace with growing security risks, higher education organizations must implement state-of-the-art core security components, enabling them to understand information security risks holistically and provide support for teaching, learning,
and research. Join representatives of the Rochester Institute of Technology and McAfee as they discuss their partnership and how it’s helping RIT use McAfee solutions to provide countermeasures and controls to understand and defend against the current and future threats.

NC State Chooses Next-Generation Identity, Access, and Mobile Social Platform

GATEWAY I

Connie Reifert, Director, Enterprise Integrated Systems, Identity and Access Management, North Carolina State University; Mike Price, Director, Security Software, Higher Education, Oracle

Like many higher education institutions, NC State had reached a tipping point with their existing identity management technology and aging infrastructure. Their previous in-house-developed solution was highly customized, inflexible, and costly to manage. With the ever-increasing demands of students, faculty, alumni, and affiliates for rapid, secure access to services on any device, NC State knew they had to make a change. They needed a highly extensible, standards-based, easy-to-implement system built to support mobile device access and substantial scale. Join this session to learn why NC State chose Oracle’s identity, access, and mobile social solutions for their next-generation security platform.

3:00–3:45 p.m.

Refreshment Break and Corporate Displays
GRAND FOYER

Aegis Identity Software
Authentify
CloudLock
Cloudpath Networks, BRONZE PARTNER
Identity Finder
Impulse Point
Lancope
OpenDNS
Qualys
Symantec Corporation
ThreatTrack
TouchNet Information Systems, BRONZE PARTNER
Websense
3:45–4:30 p.m.
Concurrent Sessions

Assess and Protect

**Vulnerability Management at UAB**

**GATEWAY III**

**Chris Green**, Information Security Architect, University of Alabama at Birmingham

The University of Alabama at Birmingham uses a unique vulnerability management system leveraging multiple Nessus scans to communicate with the departmental administration staff. The system is implemented using Python and has supported integration with WSUS and Metasploit. The system currently exports into Splunk for easy dashboard integration as well as leveraging vulnerability data in daily security operations. Come join this session for a history of our scanning efforts, implementation challenges, reporting challenges and solutions, supporting processes, and plans going forward.

Detect and Respond

**Centralized System Administration and Security Management in a Decentralized Computing Environment**

**SALON A**

**Alexander Merck**, Information Security Analyst, and **Chris Workman**, Associate Director, Office of Information Security, CISSP, University of Georgia; **Stan Waddell**, AVC I&O and CTO, University of North Carolina at Chapel Hill

This session illustrates two methods for centrally managing security events, beginning with malicious events or with vulnerability data. First, UGA has implemented a central SIEM, which greatly enhances the ability to monitor IT-related security events from various security devices (firewalls, authentication servers, etc.) that the individual devices might have overlooked. InfoSec grants departments access to view events for their networks in exchange for them logging security events to the SIEM. Second, UNC Chapel Hill created an approach whereby servers that contain sensitive information are scanned for vulnerabilities on a monthly cycle. A system administrator must then remediate the vulnerabilities before the end of the scanning cycle. If the vulnerabilities cannot be properly addressed within 90 days, a unit must outsource sysadmin functions to a qualified entity.
HEISC and Partners

What’s Your Number? Measuring the Maturity of Your Security Program with HEISC’s New Assessment Tool

Cathy Hubbs, CISO, American University; David Escalante, Director of Computer Policy and Security, Boston College; Adam Vedra, Information Security Officer, Calvin College; Cheryl Washington, Chief Information Security and Privacy Officer, University of California, Office of the President

Do you know how mature your security program is? EDUCAUSE has developed an enhanced information security program assessment tool to help you gauge your program. A panel of several early adopters will discuss the new tool and their experiences with it.

A Pragmatic Information Security Program for Small Institutions

Ben Marsden, Information Security Director, Smith College

When no one has “information security” in their job title, how can a small institution develop (and maintain) a reasonable IT security profile? An institution’s information security profile is increasingly important, and it’s not just IT’s problem anymore. But for smaller institutions with limited resources, effectively implementing a security program can be a real challenge. The goal of this session is to provide those who have ownership of information security oversight with a pathway to implement a security program with controls that are reasonable, sustainable, comprehensive, and effective—and with resources that probably aren’t tagged just for security.

Privacy

26 of 1: Compliance with the Red Flags Rule in Higher Education

Sarah D. Morrow, Chief Privacy Officer, The Pennsylvania State University; Maura A. Johnston, University Privacy Officer, University of Pennsylvania

Compliance with financial regulations in higher education, especially the Red Flags Rule, is as complex as it gets; it is a regulation with elusive requirements. Join two university privacy officers to hear how compliance was achieved at their respective institutions. This presentation will provide an overview of the Red Flags Rule and how IT is an integral part of university compliance in this area. Look forward to answers to questions you may have about where, when, and why this law applies to institutions of higher learning.
Finally, a Two-Factor Solution for the Rest of Us

Joshua Beeman, CISO, and Melissa Muth, Senior Information Security Analyst, University of Pennsylvania

In 2004 Bill Gates predicted “the death of the password,” yet reusable passwords persist because pragmatic alternatives have proven elusive, especially for the average user. Two-factor solutions have historically been considered the best complement to reusable passwords, but have been either too expensive or too complex for broad use. Penn has identified a two-factor solution based on Google’s open-source multifactor authentication software. This talk will review common two-factor problems and mistakes, how Penn’s research and pilot programs led us to pick the right solution, and what options and features are critical to ensuring success.

Using Students to Pen Test Your Network (for Credit)

Robert Maxwell, Manager, Security Operations, University of Maryland

We taught CMSC498L, an undergraduate class on penetration testing entitled “Secure Maryland” in spring 2012. The main novelty of the class was that students were able to discover, probe, and attempt to exploit live systems on the whole of the University of Maryland’s computer networks and act on what they found. This session will discuss the structure of the class, the vulnerabilities we found and the process we took to ensure they were fixed, and lessons learned for others who might like to try this exercise.

Rapid Windows Analysis

Warren Raquel, Senior IT Security Analyst, University of Illinois at Urbana–Champaign

Sometimes IT professionals can’t perform a full analysis of every system that is suspected of being compromised in a timely manner. This presentation will give IT pros some tips on performing a rapid analysis of a Windows system using resources available on the system itself to determine if there’s a potential compromise.
HEISC and Partners

Supporting High-Value, High-Risk Cloud Services with Federated Identity Management

GATEWAY II

Steve Devoti, Senior IT Architect, University of Wisconsin–Madison; Mary B. Dunker, Director, Secure Enterprise Technology Initiatives, Virginia Tech

The community has good approaches for handling access to simple cloud or third-party services. But what about higher-value services that require access to sensitive data, such as medical or financial records? These services require a solid confidence of the person’s identity. How are campuses using federated identity management, with its shared policy and technology standards, to meet these requirements? What are the security and policy considerations involved in extending federated IdM for use with these higher-value services? Join us and hear how colleagues have addressed this issue on their campuses and with their cloud partners.

New to the Game

Elevate Your Game: Develop Your Five-Year Personal Professional Development Plan

SALON A

Jenny Mehmedovic, Assistant to the Provost, University of Kansas

The adage failure to plan is planning to fail applies to our careers. No matter what your career level or financial and time constraints might be, there are many opportunities available for you to explore that will help you improve your skills and contribute to the higher education IT community. This session will help you put together a one-through-five-year professional development career plan, including the specific actions you can take to accomplish your goals and where to find professional development opportunities to support your plan.

Privacy

Third-Party Assessments: Not Just a Questionnaire

GATEWAY I

Andrew Korty, University Information and Security Officer, Indiana University

Four years ago, Indiana University began assessing the security of cloud vendors and other third parties using a simple questionnaire. Over time, the process has matured to take advantage of IU’s data-classification system and a more formal governance structure involving institutional data stewards and compliance groups. We’ve also improved our assessment questionnaire and the data-protection language that goes into our contracts. In this presentation, we will track IU’s progress on third-party assessments, including successes and obstacles, while encouraging attendees and online participants to share parallel experiences from their own institutions. We’ll also discuss goals for future improvements.
4:45–5:30 p.m. cont.

Strategic Security

IT Compliance Framework for Institutions of Higher Ed
SAISON B

Carlos S. Lobato, IT Compliance Officer, New Mexico State University

Institutions of higher education are increasingly expected to comply with various regulatory requirements specifically focused at data privacy and protection. Sometimes there could be overlap in effort that can be avoided if a university-wide IT compliance framework is implemented to ensure compliance at a high level with applicable federal and industry regulations such as FERPA, HIPAA, GLBA, the Red Flags Rule, and PCI DSS. New Mexico State University has developed an IT compliance framework model. We’ll share our lessons learned and this model to help other institutions benchmark their IT compliance efforts.

5:30–6:30 p.m.

Joint Reception
Sponsored by OpenDNS
ARCH VIEW BALLROOM

One of the most valuable aspects of this conference is the opportunity to connect face-to-face with fellow Security, Enterprise, and Advanced Core Technology Initiative attendees. Join us for the reception, where you can relax over food and drink and get to know your colleagues. NOTE: Please wear your name badge for admittance.

6:30–7:30 p.m.

PGP Key Signing
SAISON A

Brian Epstein, Computer Manager, Network and Security, Institute for Advanced Study; Ken Connelly, Associate Director, Security and Systems, University of Northern Iowa

PGP Key signing activity for all interested conference attendees. Additional information is available at www.ren-isac.net/events/spc_2013_keysigning. Questions about this event should be directed to the presenters.
TUESDAY, APRIL 16

6:30–8:30 p.m.

Organized Dinner Outings
MEET IN HOTEL LOBBY

This year, the program committee is encouraging attendees to participate in optional organized dinner outings for small groups. A few local restaurant choices will be available for sign-up near the conference registration desk on Tuesday morning. Any expenses incurred are the responsibility of the individual attendee. Groups will meet in the lobby to walk or take cabs to the restaurant for a 6:45 p.m. reservation. Don’t forget to be back at the hotel by 8:30 p.m. for our first-ever game night!

8:30–10:30 p.m.

Get Your Game On!
MARKET STREET ROOM

Join us for the premiere of the Security Professionals and Enterprise IT Leadership Conferences game night! This will be a great way to kick off the conference and help you get to know your fellow conference-goers. 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. Find a seat, and get your game on!
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:00–6:45 a.m.</td>
<td>Fun Run</td>
<td>Meet in hotel lobby</td>
</tr>
<tr>
<td>6:45–7:15 a.m.</td>
<td>Security Professionals 2014 Program Committee Breakfast (7:00–8:15 a.m.)</td>
<td>Arch View Ballroom</td>
</tr>
<tr>
<td>7:15–7:45 a.m.</td>
<td>Joint Breakfast</td>
<td>Arch View Ballroom</td>
</tr>
<tr>
<td>7:15–7:45 a.m.</td>
<td>Joint General Session (8:15–9:30 a.m.)</td>
<td>Salon C/D</td>
</tr>
<tr>
<td>7:45–8:15 a.m.</td>
<td>Joint Concurrent Sessions (9:45–10:30 a.m.)</td>
<td></td>
</tr>
<tr>
<td>8:15–8:45 a.m.</td>
<td>Joint Refreshment Break and Corporate Displays (10:30–11:15 a.m.)</td>
<td>Arch Foyer</td>
</tr>
<tr>
<td>8:45–9:15 a.m.</td>
<td>Joint Concurrent Sessions (11:15–12:00 noon)</td>
<td></td>
</tr>
<tr>
<td>9:15–9:45 a.m.</td>
<td>Registration Open</td>
<td>Grand Foyer</td>
</tr>
<tr>
<td>9:45–10:15 a.m.</td>
<td>Connect Lounge Open</td>
<td>Salon G</td>
</tr>
<tr>
<td>10:15–10:45 a.m.</td>
<td>Lunch for postconference and REN-ISAC member meeting participants (12:00 noon–1:00 p.m.)</td>
<td>Arch View Ballroom</td>
</tr>
<tr>
<td>11:15–11:45 a.m.</td>
<td>REN-ISAC Two-Day Member Meeting (1:00–6:00 p.m.)</td>
<td></td>
</tr>
<tr>
<td>11:45 a.m.–12:15 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting (1:00–6:00 p.m.)</td>
<td>Arch View Ballroom</td>
</tr>
<tr>
<td>12:15–12:45 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting (1:00–6:00 p.m.)</td>
<td></td>
</tr>
<tr>
<td>12:45–1:15 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting (1:00–6:00 p.m.)</td>
<td></td>
</tr>
<tr>
<td>1:15–1:45 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting (1:00–6:00 p.m.)</td>
<td></td>
</tr>
<tr>
<td>1:45–2:15 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting (1:00–6:00 p.m.)</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>2:15–2:45 p.m.</td>
<td>Registration Open&lt;br&gt;Grand Foyer&lt;br&gt;Connect Lounge Open Salon G</td>
<td></td>
</tr>
<tr>
<td>2:45–3:00 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting</td>
<td></td>
</tr>
<tr>
<td>3:00–3:30 p.m.</td>
<td>Refreshment Break&lt;br&gt;for postconference and REN-ISAC member meeting participants&lt;br&gt;Grand Foyer</td>
<td></td>
</tr>
<tr>
<td>3:30–4:00 p.m.</td>
<td>REN-ISAC Member Meeting continues Thursday, April 18, 7:30 a.m.–1:30 p.m.</td>
<td></td>
</tr>
<tr>
<td>4:00–4:30 p.m.</td>
<td>Postconference Seminar</td>
<td></td>
</tr>
<tr>
<td>4:30–5:00 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting</td>
<td></td>
</tr>
<tr>
<td>5:00–5:30 p.m.</td>
<td>Postconference Seminar</td>
<td></td>
</tr>
<tr>
<td>5:30–6:00 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting</td>
<td></td>
</tr>
<tr>
<td>6:00–6:30 p.m.</td>
<td>Postconference Seminar</td>
<td></td>
</tr>
<tr>
<td>6:30–7:00 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting</td>
<td></td>
</tr>
<tr>
<td>7:00–7:30 p.m.</td>
<td>Postconference Seminar</td>
<td></td>
</tr>
<tr>
<td>7:30–8:00 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting</td>
<td></td>
</tr>
<tr>
<td>8:00–8:30 p.m.</td>
<td>Postconference Seminar</td>
<td></td>
</tr>
<tr>
<td>8:30–9:00 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting</td>
<td></td>
</tr>
<tr>
<td>9:00–9:30 p.m.</td>
<td>Postconference Seminar</td>
<td></td>
</tr>
<tr>
<td>9:30–10:00 p.m.</td>
<td>REN-ISAC Two-Day Member Meeting</td>
<td></td>
</tr>
<tr>
<td>10:00–10:30 p.m.</td>
<td>Postconference Seminar</td>
<td></td>
</tr>
</tbody>
</table>
6:00–6:45 a.m.

Fun Run
MEET IN 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.

7:00–8:15 a.m.

2014 Program Committee Breakfast
(by invitation only)
MARKET STREET ROOM

7:15–8:15 a.m.

Breakfast
Sponsored by Symantec Corporation
ARCH VIEW BALLROOM

7:15 a.m.–5:00 p.m.

Registration Open
GRAND FOYER

Connect Lounge
SALON G

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.

8:15–9:30 a.m.

Joint General Session

Enterprise Risk Management in Higher Education: Implications for Enterprise IT
Sponsored by Kroll Advisory Solutions

SALON C/D

Cathy Hubbs, CISO, American University; Gary Langsdale, University Risk Officer, The Pennsylvania State University; Janice M. Abraham, President and CEO, United Educators

Moderated by: Peter J. Murray, CIO/VP, University of Maryland, Baltimore

Enterprise risk management (ERM) has matured as a discipline within higher education. Colleges and universities are subject to risks to their physical assets,
people assets, and cyber assets. The impact of risks can be strategic, operational, legal, financial, or reputational. Information technology on campus, especially enterprise systems and information security, is emerging as an important area for risk assessment and treatment. Cloud computing, mobile devices, and social media present new challenges and opportunities. This session will explore ERM and its application to enterprise IT in higher education.

9:45–10:30 a.m.
Concurrent Sessions

Breaches and a Lawsuit: An Institution’s Road to Recovery
GATEWAY II

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

As a result of its breaches and a class action lawsuit, the University of Hawaii has undertaken extensive actions to transform its information security landscape. We will describe the timeline of events and our institutional responses and share strategies from our new information security program to prevent future exposures of sensitive information. The goal of this session is to enable other institutions to benefit from our experiences to help them develop their own preventive strategies and, should a breach occur, have the tools and procedures in place to quickly mitigate damages and communicate appropriately, thereby minimizing the risk of a lawsuit.

Community Guidance for Cloud Services: Security, Privacy, and Compliance
SALON B

Robert F. Brammer, Senior Advisor to the CEO, Internet2; Michele Norin, CIO, The University of Arizona; Paul Howell, Chief Information Technology Security Officer, University of Michigan–Ann Arbor

Internet2 has announced a series of new cloud-based services to meet the needs of higher education institutions through partnerships with commercial providers. To meet the objectives of the NET+ program, including the security requirements of NET+ participants, Internet2 organized the NET+ Security initiative. The primary objective for this initiative is to develop guidance that, with proper implementation, will meet the security needs of our NET+ participants while helping enable the service providers to manage their costs and to offer discounted prices. This presentation will describe the NET+ Security guidance and summarize experience to date with the implementation.
9:45–10:30 a.m. cont.

The Enemy Is Us: Doing the Work of Information Security Better
GATEWAY III

Phillip Deneault, Information Security Officer, Worcester Polytechnic Institute

Within information security departments, staff often get so bogged down in “getting the job done” that they can never assess how they are doing their job and whether they can do anything to improve the quality and efficiency of their work. If you’re part of an information security group, this presentation will help you evaluate how things get done, figure out how to make policies and regulations work for you, teach you new techniques for getting a better sense of the problem, and help you set up relationships that can assist any group with achieving its goals.

How to Think Like a Risk Manager
GATEWAY I

Gary Langsdale, University Risk Officer, The Pennsylvania State University

Having heard the enterprise risk management (ERM) panel, you are now wondering what is going on in the Risk Management department across the street from your office, how they view you and your issues, and how to make them an ally. This session will explain the risk manager’s role, thought processes and tools, and resources they call upon such as URMIA (University Risk Management and Insurance Association), the EDUCAUSE of risk management.

Navigating the Clouds with an Enterprise IT Strategy
SALON A

Clayton Burton, Senior Programmer Analyst, Jason Long, Web Programmer Analyst, and Fredrick Miller, CIO, Furman University

Should your institution be a cloud services leader? How do you balance the risks of innovation with the possible benefits? What about managing identity in the cloud? Furman University’s IT Strategic Plan is guiding an aggressive move to cloud services. This session will look at lessons learned, opportunities, and challenges ahead. An enterprise IT strategy can guide strategic innovations using cloud services for your institution. We will discuss the forces that drove us at Furman University to pursue cloud solutions and cloud service models, as well as how identity management tied everything together. The lessons we’ve learned can help your institution’s planning efforts for cloud services.
A Practitioner’s Approach for Developing Information Security Policy

SALON E/F

David Wilhite, Senior IT Security Engineer, University of South Carolina

An institution developing its information security policy by basing it on lofty ideals and stringent standards may demand far more than its staff is capable of delivering, which risks frustrating staff to the point of resistance, outright rebellion, or clandestine noncompliance. This strategy can also create a risk of legal liability, as an institution may instantly place itself out of compliance with its own documented policy. This session will outline a strategy for phasing in policy provisions, inclusive of key executive, managerial, and technical staff members, and provide a template of policies, standards, and procedures.

10:30–11:15 a.m.

Refreshment Break and Corporate Displays

GRAND FOYER

Authentify

Authentify offers flexible out-of-band authentication (OOBA) services for strengthening the security of account access or verifying legitimate account activity. Authentication and verification are provided by engaging end users in synchronized exchanges between their online accounts and separate voice or data channels via their telephones, smartphones, or tablets. The end user’s phone or other smart device becomes an effective proxy for a security credential.

CloudLock

CloudLock provides an information security suite that lets organizations implement data privacy practices and data governance to manage data in Google Docs, Sites, and Drive. CloudLock also lets organizations implement governance for third-party apps. The largest Google Apps customers in the world trust CloudLock to secure their data.

Cloudpath Networks, Bronze Partner

Cloudpath Networks brings WPA2 enterprise wireless security to all, enabling campuses to increase the use of wireless security by students, faculty, contractors, and guests. Winner of the 2012 Best of Interop award, XpressConnect simplifies WPA2 enterprise and 802.1X through automated, self-service provisioning across a wide array of user-owned devices for both password-based and certificate-based networks.
10:30–11:15 a.m. cont.

**Code 42 Software**

Code 42 Software has been protecting the world’s information since 2001. Our enterprise backup solution, CrashPlan PROe, provides people-friendly, enterprise-tough backup. Engineered with laptops in mind, it offers continuous backup that won’t slow you down and self-service restores that free up IT.

**Identity Finder**

Identity Finder is a global leader in sensitive data discovery and security. Founded in 2001, we provide organizations with advanced technology to help prevent data leakage. Our data loss prevention software finds and protects data at rest and in use, either centrally or at the end point, by searching files, e-mails, desktops, servers, databases, and websites.

**Lancope**

Lancope is a leading provider of network visibility and security intelligence to defend enterprises against today’s top threats. By collecting and analyzing NetFlow, IPFIX, and other types of flow data, Lancope’s StealthWatch system helps organizations quickly detect a wide range of attacks, from APTs and DDoS to zero-day malware and insider threats. Through pervasive insight across distributed networks, including mobile, identity, and application awareness, Lancope accelerates incident response, improves forensic investigations, and reduces enterprise risk. Lancope’s security capabilities are continuously enhanced with threat intelligence from the StealthWatch Labs research team. For more information, visit www.lancope.com.

**OpenDNS**

Leading colleges and universities choose Umbrella by OpenDNS for cloud-delivered Internet security that’s easy to manage and scale. Secure all your networks and users from malware, botnets, and phishing and manage everything through a single web-based dashboard. Our customers include Vanderbilt University and George Washington University.

**Red Hat**

As a Red Hat Partner, CITYTECH delivers integrated solutions unique to your business model. We excel at designing practical solutions that address immediate needs and are scalable for future growth. We have extensive experience with Red Hat and JBoss as a reseller of subscriptions and a provider of services around application development and deployment. For more information, see www.citytechinc.com.
Symantec Corporation

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, ensuring confidence wherever information is used or stored.

Unanet Technologies

Unanet PSA helps organizations of all sizes better manage project, product, and services work. With an anytime, anywhere 100% web-based interface, Unanet customers increase corporate value through improved utilization, delivery, revenue, and profitability. Unanet PSA is available as an on-premises or cloud-based solution, facilitating resource planning, skills management, time and billing, expense reporting, project reporting, and management dashboards. For more information, visit www.unanet.com.

Websense

Websense is a global leader in unified web security, e-mail security, mobile security, and data loss prevention (DLP). Websense TRITON content security solutions help institutions leverage social media and cloud-based communication while protecting them from advanced persistent threats and modern malware, preventing the loss of confidential information and enforcing Internet use and security policies.

WTC Consulting

WTC Consulting Inc. is a national firm delivering consulting services to higher education and academic medical centers since 1983 with expertise in strategic technology planning, rate and funding strategies, IT cost and service alignment, mobility planning, and implementation oversight. WTC has conducted more than 860 engagements for 250 campus clients.
11:15 a.m.–12:00 noon

**Concurrent Sessions**

**Bring Your Own Cloud: Data Management Challenges in a Click-Through World**

*SALON E/F*

*Sherry Michael Weller,* IT Project Leader, University of Pennsylvania

Consumer cloud-based services are easy to set up, low cost, and familiar. It’s understandable why clients would automatically turn to them for their data-storage needs. But what happens when data security challenges expediency? We will explore a complex case study to examine a university group that turned to free cloud services to share sensitive data. Our discussion will focus on challenges conducting distributed research with limited resources and computing personnel. Solutions to the case will be considered, including working across organizational borders to advocate for customers, building client awareness, and conducting routine security assessments.

**Effective Data Governance Practices**

*GATEWAY I*

*Michael J. Chapple,* Senior Director, Enterprise Support Services, University of Notre Dame

Data stewardship and governance are complex topics in higher education due to the distributed nature of our organizations. At Notre Dame, we’ve built an effective information governance program in collaboration with our colleagues across the administration. We embrace five pillars in this program: quality and consistency; policies and standards; security and privacy; compliance; and retention and archiving. We believe that our program’s success is largely attributable to its integration with the university’s business intelligence program. In this presentation, you will learn about our approach to data governance and how you might apply the lessons we’ve learned at your institution.

**Lessons Learned in Managing IT Risk**

*GATEWAY III*

*Jane Drews,* CISO, The University of Iowa

This session will cover “understanding risk”: what IT risk is, where it comes from, and what we can do about it. We’ll also present a model that can be used for evaluating risk responses and examine three different areas of IT risk in the “lessons learned” section: information risk, endpoint risk, and system/server risk. We’ll review examples and apply our understanding of risk, look at lessons learned when trying to manage it, and finally review some recommendations for lowering risk in those areas.
Managing Information Privacy Risk: A Multi-institutional Panel Discussion

**Salon A**

**Merri Beth Lavagnino**, Chief Privacy Officer and Compliance Coordinator, Indiana University; **Sarah D. Morrow**, Chief Privacy Officer, The Pennsylvania State University; **Marcos Vieyra**, CISO, University of South Carolina; **Geoffrey S. Nathan**, Faculty Liaison for Computing and Information Technology, Wayne State University

**Moderated by:** Jane Rosenthal, Director of Privacy, University of Kansas

The distinction between information security and information privacy is a topic that many of us are increasingly confronted with on a regular basis. Even if we have a satisfying understanding of what that distinction is and what it means in practice, what can we in higher education do about it? Join our panelists, who are charged with broad information privacy responsibility, as they discuss how their respective institutions approach information privacy risk management and governance. As you will learn, information privacy governance and risk management are topics that will become increasingly important in the coming years.

**Mitigating the Top Human Risks to EDUs**

**Gateway II**

**Lance Spitzner**, Director, SANS Securing the Human Program, The SANS Technology Institute

People have become one of the greatest risks to academic environments, especially with the growth of new technologies such as BYOD, social media, and cloud. This short talk identifies the top human risks to institutions and what you can do to effectively mitigate them.

**Practical Project Management for Security Implementation in Enterprise Systems**

**Salon B**

**Paula Brossard**, UITS Infrastructure Project Manager, and **Tanya Choice-Henry**, IS Privacy and Awareness Analyst, Information Technology Services, University of Wisconsin–Milwaukee

Security implementation is, or should be, a part of every enterprise system, not an add-on after the fact. One of the best ways to ensure effective IT security is to have a seat at the table throughout the life cycle of the project. Project management strategies provide a systematic approach for including the appropriate areas while assigning responsibility and accountability for projects. Join University of Wisconsin–Milwaukee staff to learn how project management strategies are improving information security in enterprise systems and how to employ the same strategies at your institution.
WEDNESDAY, APRIL 17

12:00 noon–1:00 p.m.
Lunch for Postconference Seminar and REN-ISAC Member Meeting Participants
ARCH VIEW BALLROOM

Postconference Seminars
PLEASE NOTE: Separate registration and fee are required to attend seminars.

1:00–6:00 p.m.
SEM02Z

REN-ISAC Two-Day Member Meeting
Daniel Adinolfi, Senior Security Engineer, Cornell University; Doug Pearson, Technical Director, REN-ISAC, Indiana University Bloomington

The Research and Education Networking Information Sharing and Analysis Center is an integral part of higher education’s strategy to improve network security. This meeting will gather REN-ISAC members for a face-to-face meeting. (REN-ISAC members only)

The two-day member meeting will be held Wednesday, April 17, from 12:00 noon to 6:00 p.m. and Thursday, April 18, from 7:30 a.m. to 1:30 p.m. Your registration fee includes lunch and a refreshment break on Wednesday; breakfast and a refreshment break on Thursday; and all program materials.

Please visit the REN-ISAC information desk in the Grand Foyer if you have questions or want more agenda details.
1:30–5:00 p.m.

**SEM01Z**

**Privacy and Data Security in Higher Education**

GATEWAY II


Privacy is a major and often underappreciated risk area for higher education. Professor Solove will provide advice on how institutions of higher education can reduce the risk of having a privacy fiasco by discussing several actual incidents. How can schools develop the kinds of privacy programs currently in place at businesses, hospitals, and financial institutions? The learning objectives for this session include learning how to (1) identify privacy risks and their costs, (2) understand the various privacy laws that all institutions of higher education must be aware of, and (3) prevent or minimize privacy risks.

3:00–3:30 p.m.

Refreshment Break for Postconference Seminar and REN-ISAC Member Meeting Participants

GRAND FOYER
Looking to learn more about the latest technology to serve your campus needs? Contact our participating companies for information.

**Aegis Identity Software**
Janet Yarbrough, Director of Business Development
janet.yarbrough@aegisidentity.com, 303-589-5435
www.aegisidentity.com
*Product Categories:* Data Security; Identity and Access Management; Information Security Governance

**Authentify**
Dan Zurawski, Midwest Regional Manager
dan.zurawski@authentify.com, 773-243-0329
www.authentify.com
*Product Categories:* Access Control; Authentication; Cloud Security

**Brinqa**
Rich Skinner, Director, Security Risk Analytics and Big Data
rskinner@brinqa.com, 260-312-1958
www.brinqa.com
*Product Categories:* Security Management; Security Metrics; Security Risk Assessment and Analysis

**CloudLock**
Elizabeth Eagleston, Regional Sales Director, Higher Education
elizabeth@cloudlock.com, 978-448-0507
www.cloudlock.com
*Product Categories:* Access Control; Cloud Security; Firewalls

**Cloudpath Networks, Bronze Partner**
Jeff Grimm, Sales Executive
jeff@cloudpath.net, 303-647-5412
www.cloudpath.net
*Product Categories:* Authentication; Identity and Access Management; Network Security and Applications
Code 42 Software
Enterprise Sales Team
sales@crashplanproe.com, 612-333-4242
www.code42.com
Product Categories: Business Continuity, Disaster Recovery, Emergency Planning; Data Security; Mobile Computing

Epson, Gold Partner
Bill Bilkey, Commercial Account Management
bill_bilkey@ea.epson.com, 562-981-3840
www.epson.com/brighterfutures
Product Categories: Document Imaging and Management; Hardware; Wireless

Identity Finder
Joe Caceres, Vice President of Sales
joe.caceres@identityfinder.com, 646-397-0055
www.identityfinder.com
Product Categories: Data Security; PCI DSS; Privacy

Impact Technologies
Becky Maycock, Director, Product Management and Marketing
beckym@impacttech.com, 314-743-1414
www.impacttech.com
Product Categories: Cloud Security; Data Security; Information Security Governance

Impulse Point
Tim Evans, Vice President of Sales
tevans@impulse.com, 508-330-8212
www.impulse.com
Product Categories: Identity and Access Management; Security Management; Security Policies

Kroll Advisory Solutions
Greg Brown, Client Executive
greg.brown@kroll.com, 800-697-7189 x 20752
www.krollcybersecurity.com
Product Categories: Incident Handling and Response; Security Advisory and Consulting; Security Risk Assessment and Analysis
Lancope
David Rudd, Territory Account Manager
drudd@lancope.com, 770-225-3139
www.lancope.com
**Product Categories:** Network Security and Applications; Security Risk Assessment and Analysis; Incident Handling and Response

McAfee
Chuck Bruce, Regional Account Manager
chuck_bruce@mcafee.com, 850-830-8814
www.mcafee.com/us/
**Product Categories:** Intrusion Detection and Prevention; Mobile Security; Network Security and Applications

NetApp, Bronze Partner
Ann James, Field Marketing Manager, State and Local Government and Education Marketplace
ann.james@netapp.com, 408-591-4138
www.netapp.com/edu
**Product Categories:** Data Administration and Warehousing; Data Security; Virtualization

OpenDNS
Marc Gemassmer, Vice President of Sales
marc@opendns.com, 877-811-2367
www.umbrella.com
**Product Categories:** Cloud Security; Mobile Security; Network Security and Applications

Oracle Corporation, Silver Partner
Pete Angstadt, Vice President, Security
peter.angstadt@oracle.com; 703-597-9461
www.oracle.com
**Product Categories:** Data Security; Encryption; Identity and Access Management

Qualys
Scott Rachford, Regional Vice President
info@qualys.com, 650-801-6100
www.qualys.com
**Product Categories:** Network Security and Applications; Network Vulnerability Assessment; Vulnerability Scanning
Red Hat
Gina Nist, Account Executive
gnisti@citytechinc.com, 614-395-6872
www.citytechinc.com
*Product Categories:* Cloud Computing and Services; Consulting; Mobile Computing

Sonic Foundry, **Platinum Partner**
Sean Brown, Vice President of Sales Operations
getinfo@sonicfoundry.com, 608-443-1600
www.sonicfoundry.com
*Product Categories:* Content Capture; Content Management Systems; Mobile Computing

Symantec Corporation
Caroline Rinker, Practice Manager, Education
caroline_rinker@symantec.com, 612-250-3372
www.symantec.com
*Product Categories:* Mobile Security; Critical Infrastructure Protection; Security Policies

Tenable Network Security
Mark Fox, Regional Sales Manager
marketing@tenable.com, 410-872-0555
www.tenable.com
*Product Categories:* Network Security and Applications; PCI DSS; Vulnerability Scanning

ThreatTrack Security
Gill Langston, Sales Manager
VIPRESales@ThreatTrack.com, 888-688-8457
www.ThreatTrackSecurity.com
*Product Categories:* Identity Theft; Mobile Security

TouchNet Information Systems, **Bronze Partner**
John Murphy, Vice President
john.murphy@touchnet.com, 800-869-8329
www.touchnet.com
*Product Categories:* Authentication; PCI DSS; Security Architecture
Unanet Technologies
Kate Ogden, Vice President, Business Development
kogden@unanet.com, 703-689-3417
www.unanet.com
*Product Categories:* Cloud Computing and Services; ERP; Portfolio and Project Management

Websense
Brandon Andrews, Director, Sales
bandrews@websense.com, 858-735-3818
www.websense.com
*Product Categories:* Data Security; Mobile Security; Network Security and Applications

WTC Consulting
Ginny Schroeder, Practice Director
gschroeder@wtc-inc.net, 213-689-5324
www.wtc-inc.net
*Product Category:* Consulting
Free Security at Your Fingertips

Visit qualys.com/secure today!

Find out if you are secure from hackers and compliant with regulations. Audit the security of browsers, systems and web applications in your organization.

Qualys makes these free security tools available at your fingertips at www.qualys.com/secure.

© 2013 Qualys, Inc. All rights reserved.