Security Professionals Conference 2012

Security Everywhere: Exploring the Expanding World of Security

MAY 15–17
INDIANAPOLIS, IN
JW Marriott
EDUCAUSE thanks the following sponsors for their valuable contributions to the conference:

**PLATINUM PARTNER**

![Jenzabar](image1)

**GOLD PARTNERS**

![Epson](image2)  ![Oracle](image3)

**BRONZE PARTNER**

![Qualys](image4)

**ADDITIONAL SPONSORS**

![323link](image5)  ![aegis identity](image6)  ![Caption Colorado](image7)  ![GFI](image8)  ![Modulo Solutions for GRC](image9)  ![OpenDNS](image10)  ![SonicWall](image11)  ![Stonesoft](image12)  ![Symplified](image13)
SECURITY PROFESSIONALS CONFERENCE 2012
PROGRAM COMMITTEE

Brian Basgen
Director of Client Services (Acting)
Pima County Community College District

Cathy Bates
University Information Security Officer
The University of Arizona

Joshua Beeman
Chief Information Security Officer
University of Pennsylvania

Kim Cary
Chief Information Security Officer
Pepperdine University

Gregory Hedrick
Director Information Security Service
Purdue University

Paul Howell (Vice Chair)
Chief Information Technology Security Officer
University of Michigan–Ann Arbor

Jodi-Ann Ito (Chair)
Information Security Officer
University of Hawaii System Office

Anthony Maszeroski
Information Security Manager
The University of Scranton

Doug Pearson
Technical Director, REN-ISAC
Indiana University Bloomington

Donald J. Schattle II
Information Security Officer
Providence College

David Seidl
Manager, Information Security
University of Notre Dame

Thomas Siu
Chief Information Security Officer
Case Western Reserve University

Joseph E. St Sauver
Nationwide Security Programs Manager, Internet2
University of Oregon
EDUCAUSE is a nonprofit membership association created to support those who lead, manage, and use information technology to benefit higher education. A comprehensive range of resources and activities are available to all EDUCAUSE members. For more information about EDUCAUSE, including membership, please contact us at info@educause.edu or visit educause.edu.

Internet2® is a member-owned advanced technology community founded by the nation’s leading higher education institutions in 1996. Internet2 provides a collaborative environment for U.S. research and education organizations to solve common technology challenges, and to develop innovative solutions in support of their educational, research, and community service missions. For more information, visit internet2.edu.

The Higher Education Information Security Council was established by EDUCAUSE and Internet2 in July 2000. HEISC’s mission is to improve information security, data protection, and privacy programs across the higher education sector through its community members and collaborations with partners from government, industry, and other academic organizations. HEISC actively develops and promotes leadership; awareness and understanding; effective practices and policies; and solutions for the protection of critical data, IT assets, and infrastructures. For more information, visit educause.edu/security.
The REN-ISAC mission is to aid and promote cybersecurity operational protection and response within the higher education and research communities. The mission is conducted within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large. REN-ISAC serves as the R&E trusted partner for served networks, the formal U.S. ISAC community, and in other commercial, governmental, and private security information sharing relationships.

This year’s conference marks the 10th anniversary of higher education security professionals gathering to network, share information, and strengthen the community’s ability to address cybersecurity threats and protect data.

Help us highlight the significant landmarks in information security and celebrate the accomplishments of higher education security professionals over the last decade. Add your comments to the timeline board you’ll find in public spaces during the conference.

EDUCAUSE 2012
ANNUAL CONFERENCE

NOVEMBER 6–9
DENVER AND ONLINE

The best thinking in higher education IT.
CONNECTIVITY
Wireless is available during registration hours.
LOGIN INSTRUCTIONS:
» Open up wireless connections
» View available networks
» Connect to EDUCAUSEAIR
» Enter case-sensitive security key: Indy2012
» Launch web browser (As a courtesy to all attendees, please limit your mobile
device usage so bandwidth is not exceeded.)

CONTRIBUTE AND CONNECT
Social media. Contribute to the dynamic conference backchannel conversa-
tion through blogs, social bookmarking sites, or photo-sharing ser-
VICES with the tag SEC12. You can also share your conference experience in "real time" on Twitter by tagging tweets with the general conference hashtag of #SEC12.
Mobile Site. Visit educause.edu/mobile for complete program information.

NETWORK WITH COLLEAGUES
Check out the Networking Stickers located on the tote-stuffing table near
the registration desk to identify areas of interest to you and maximize your on-site interactions.
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 on
Wednesday, 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.
Use the Affinity Finder on the conference website’s registration page to
search the registration list of your fellow attendees and sort by their inter-
ests or geographical location. For noncommercial use by conference attendees
only; login required.
Connect with colleagues attending the online conference. Select sessions
from the face-to-face Security Professionals Conference are being streamed
live online. Both face-to-face and online participants are encouraged to con-
nect through Twitter about topics and sessions throughout the event.

CONFERENCE FEATURES
Lunchtime Roundtables
Join a conversation while you lunch. A mix of important topics will be facilitated
by committee members and members of HEISC.
Corporate Displays
Fifteen companies providing technology solutions for higher education will be set in the White River Ballroom Foyer on Wednesday. Stop by to visit and learn more. A company directory including products and services is located in the back of this print program.

EVALUATIONS
Session evaluations. Evaluate individual sessions and their speakers by Thursday, May 31. Evaluation links can be found on the individual session page online at educause.edu/sec12/program.

Postconference evaluation. Shortly after the conference you’ll receive an e-mail inviting you to complete an overall event evaluation online. Your input helps us understand your needs and develop next year’s event. Please give us your feedback and complete the overall conference evaluation by Thursday, May 31.

PROCEEDINGS
Conference proceedings. All presenters are asked to post their resources, including any handouts and slide sets, to their session in the online agenda located at educause.edu/sec12. These and other resources will comprise the event proceedings. Attendees will be notified by e-mail when they are available.

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

Mobile devices. As a courtesy to the speakers and to other conferees, we ask that you silence all cell phones and turn off the sound on laptops during conference sessions.

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.
CONFERENCE INFORMATION

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

**Notepads:** Printed on 30% recycled paper, 15% postconsumer waste
**Pens:** Made from 100% recycled plastic
**Print programs:** Printed on 30% postconsumer recycled paper
**Tote bags:** Made from 50% recycled material

PARTICIPATE THROUGHOUT THE YEAR
The greatest value derives from interaction with members through EDUCAUSE programs and events. Please consider engaging with your community in the following ways.

**Give a presentation.** Check the website later this year for 2013 presentation guidelines, the proposal form, and deadlines. Visit the Speaker Concierge at educause.edu/SpeakerConceirge for a head start.

**Serve on a conference program committee.** Find information on program committees at educause.edu/committees, or e-mail volunteer@educause.edu. Take an active community role and serve as a volunteer. Find your opportunities at educause.edu/volunteer.

**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.

**Participate in an EDUCAUSE Live! webinar.** Information and schedule at educause.edu/Live.

**Explore professional development opportunities.** Constituent groups, mentoring, Institute programs, a Career Center, conferences, and more are outlined at educause.edu/PDopportunities.

**Mark your calendar for the Security Professionals Conference 2013.** It will take place in St. Louis and concurrently online April 15-17.
## TUESDAY’S SCHEDULE AT A GLANCE

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 7:30 a.m.–8:30 a.m. | Continental Breakfast  
 **for Seminar Participants**  
 **OUTSIDE MEETING ROOM 103** |
| 7:30 a.m.–5:00 p.m. | Registration Desk Open  
 **WHITE RIVER BALLROOM FOYER** |
| 7:30 a.m.–12:00 noon | Preconference Seminars  
 **Seminar 01A**  
 **Navigating the PCI DSS Jungle**  
 **WHITE RIVER BALLROOM A**  
 **Seminar 02A**  
 **Client Certificates**  
 **WHITE RIVER BALLROOM B**  
 **Seminar 03A**  
 **Minimizing Security and Legal Risks in the Cloud**  
 **MEETING ROOM 103/104** |
| 8:30 a.m.–4:30 p.m. | Preconference Seminars  
 **Seminar 01F**  
 **Establishing an Information Security Program**  
 **WHITE RIVER BALLROOM D**  
 **10:00 a.m.–10:30 a.m.** | Refreshment Break  
 **for Seminar Participants**  
 **OUTSIDE MEETING ROOM 103** |
| 10:00 a.m.–5:00 p.m. | Preconference Seminar  
 **SEM02F**  
 **SANS NetWars Tournament**  
 **WHITE RIVER BALLROOM C** |
| 12:00 noon–1:00 p.m. | Lunch  
 **for Seminar Participants**  
 **WHITE RIVER BALLROOM E** |
| 12:00 noon–4:30 p.m. | Higher Education Information Security Council (HEISC) Leadership Team Meeting  
 **by invitation only**  
 **MEETING ROOM 105** |
| 1:00 p.m.–4:00 p.m. | Preconference Seminars  
 **Seminar 01P**  
 **How Tokenization and Point-to-Point Encryption Can Reduce Your School’s PCI Scope (or Not)**  
 **WHITE RIVER BALLROOM A**  
 **Seminar 03P**  
 **Lock Picking and Other Skills for the Security Professional**  
 **WHITE RIVER BALLROOM B** |
| 2:30 p.m.–3:00 p.m. | Refreshment Break  
 **for Seminar Participants**  
 **OUTSIDE MEETING ROOM 103** |
| 4:45 p.m.–5:30 p.m. | How to Make the Most of the Conference  
 **WHITE RIVER BALLROOM E** |
| 5:45 p.m.–6:30 p.m. | Introduction to the REN-ISAC  
 **WHITE RIVER BALLROOM E** |
| 6:30 p.m.–8:30 p.m. | Dinner on Your Own Program Committee Dinner  
 **by invitation only**  
 **8:30 p.m.–10:00 p.m.** | Birds-of-a-Feather Sessions  
 **WHITE RIVER BALLROOM F** |
TUESDAY, MAY 15

7:30 a.m.–8:30 a.m.
Continental Breakfast for Seminar Participants
OUTSIDE MEETING ROOM 103

7:30 a.m.–5:00 p.m.
Registration Desk Open
WHITE RIVER BALLROOM FOYER

8:30 a.m.–12:00 noon
Preconference Seminars
NOTE: Separate registration and fee are required to attend seminars.

Seminar 01A

Navigating the PCI DSS Jungle
WHITE RIVER BALLROOM A
Tammy L. Clark, CISO, Georgia State University

Map reading and navigation skills don’t always come easy in the “PCI DSS jungle.” Before heading into the tangle of PCI DSS requirements (200+), you’ll want to be prepared and have all the resources you need at your disposal. From understanding the credit card process landscape to scoping your campus PCI reviews to building cross-campus collaborations, there’s much to take into consideration. Come to this introductory seminar to discuss a common-sense approach to developing a cost-effective and efficient PCI compliance review program at your institution.

Seminar 02A

Client Certificates
WHITE RIVER BALLROOM B
Joseph E. St Sauver, Nationwide Security Programs Manager, Internet2, University of Oregon

Client certificates (also known as personal certificates or S/MIME certificates) have been around for a decade, but they’re rarely seen in higher education, even though the federal government and large corporations have successfully deployed them for highly sensitive security environments involving millions of users. This seminar, taught by the manager of InCommon’s certificate program, will bring you up to speed on client certificates and give you the background and skills you need to successfully deploy client certificates at your school, whether for a small group of system administrators or campus-wide. Technical level: intermediate.
Seminar 03A

**Minimizing Security and Legal Risks in the Cloud**

**MEETING ROOM 103/104**

**David Escalante,** Director of Computer Policy & Security, Boston College;  
**Beth Cate,** Associate Professor and Adjunct Associate General Counsel, Indiana University

More and more applications and their data are being moved off-campus to cloud providers. This session will review what you need to do from a security and legal perspective before moving functions and data to a third-party provider. The focus will be on evaluating risk associated with a cloud service, using a standard methodology, and on considering contractual and compliance matters (complete with interactive exercises); we will not cover technical techniques to secure a cloud server.

8:30 a.m.–4:30 p.m.

*Preconference Seminars*

**NOTE:** Separate registration and fee are required to attend seminars.

Seminar 01F

**Establishing an Information Security Program**

**WHITE RIVER BALLROOM D**

**Cedric Bennett,** Emeritus Director, Information Security Services, Stanford University

This interactive session will provide an overview of areas such as growing the program, gaining broad support, finding resources, focusing direction, and planning for what comes next. We’ll take a look at staffing models, risk assessment, policy development, campus-wide security awareness, staff training, privacy issues, and operational and technical controls. Participants will be given an opportunity to discuss and potentially address security issues from their own institutions.

10:00 a.m.–10:30 a.m.

**Refreshment Break for Preconference Seminar Participants**

OUTSIDE MEETING ROOM 103

10:00 a.m.–5:00 p.m.

*Preconference Seminar*

**NOTE:** Separate registration and fee are required to attend seminars.

SEM02F

**SANS NetWars Tournament**

**WHITE RIVER BALLROOM C**

**Mark Baggett,** Certified Instructor, The SANS Technology Institute

NetWars is a collection of computer and network security challenges designed
to represent real-world security issues accompanied by their flaws and resolutions. NetWars is designed to challenge network and security staff and build the player’s skills through successive challenges. Players receive valuable feedback on tasks to help them improve their skills. Learn about NetWars at sans.org/cyber-ranges/netwars. EDUCAUSE is hosting a 6-hour SANS NetWars “tournament” at the EDUCAUSE Security Professional conference on May 15 in Indianapolis. Winners will receive a prize, courtesy of SANS.

NOTE: You must bring your own laptop in order to participate. View mandatory laptop hardware requirements at sans.org/sansfire-2012/laptop.

12:00 noon–1:00 p.m.
Lunch for Preconference Seminar Participants
(lunch ticket required)

WHITE RIVER BALLROOM E
Lunch is provided for preconference attendees attending both a morning and afternoon seminar or a full-day seminar.

12:00 noon–4:30 p.m.
Higher Education Information Security Council (HEISC) Leadership Team Meeting
(by invitation only)
MEETING ROOM 105

1:00 p.m.–4:00 p.m.
Off-Site Tour

SEM01T

Off-Site Tour of Indiana University Informatics Communications Technology Computing Building

Tour Indiana University’s computing and information security facilities in the Informatics and Communications Technology Complex (ICTC) on the IUPUI campus, just a short walk from the JW Marriott hotel. The walking tour includes: IU’s Data Center, a $32.7 million facility designed to ensure the safety and security of IU’s most prized networking, security, computer-processing, and data-storage equipment; the Advanced Visualization Facility, with its scientific visualization, virtual reality, high-end computer graphics, and visual telecollaboration technology running on SGI/Irix, Linux, and Windows systems; and the Global Research Network Operations Center, interconnecting the research and education networks in the United States with those in Asia/Pacific, Europe, Russia, and Latin America.

This tour is hosted by IU’s Information Security, Policy, and Privacy staff. Tours will end with a light reception before participants return to the hotel. Meet in the JW Marriott lobby by 1:00 p.m. Please wear your name badge for admittance.
TUESDAY, MAY 15

1:00 p.m.–4:30 p.m.

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

Seminar 01P

How Tokenization and Point-to-Point Encryption Can Reduce Your School’s PCI Scope (or Not)
WHITE RIVER BALLROOM A
Walter Conway, Manager, 403 Labs

Two emerging technologies have the potential to reduce campus merchants’ PCI scope while also reducing the risk of a damaging data breach: tokenization, the process whereby payment card data are replaced by surrogate values or tokens, and point-to-point encryption (P2PE), which potentially can reduce your PCI scope to the card reader, thereby removing your payment applications and databases from PCI scope. Neither technology is a silver bullet that makes PCI go away. Learn how these technologies work and how they address different requirements; what the PCI Council’s implementation guidance says and doesn’t say; how each can also increase your security; and some real-world implementation best practices so your institution can realize the scope reduction and cost savings you expected (and your vendor promised). We also will discuss changes in PCI DSS version 2.0 that can impact how your campus validates your PCI compliance.

Seminar 03P

Lock Picking and Other Skills for the Security Professional
WHITE RIVER BALLROOM B
Zach Campbell, Senior Security Consultant, and Nathan Heald, 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 course 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 p.m.–3:00 p.m.

Refreshment Break for Preconference Seminar Participants
OUTSIDE MEETING ROOM 103
TUESDAY, MAY 15

4:45 p.m.–5:30 p.m.

How to Make the Most of the Conference: Content, Networking, and Next Steps
WHITE RIVER BALLROOM E

Michele Norin, CIO, The University of Arizona; Jodi-Ann Ito, Information Security Officer, University of Hawaii System Office; Larry D. Conrad, Vice Chancellor and CIO, University of North Carolina at Chapel Hill

Turn your best intentions into realities. This roadmap session will help you get the most out of your attendance at the Security Professionals Conference. Beyond the conference overview, we will cover how to make smart choices about which sessions to attend, network with colleagues in similar situations, be intentional about taking home what you learned, and become more professionally involved in EDUCAUSE/Internet2 HEISC activities.

5:45 p.m.–6:30 p.m.

Introduction to the REN-ISAC
WHITE RIVER BALLROOM E

Doug Pearson, Technical Director, REN-ISAC, Indiana University Bloomington

This session is intended for those interested in learning more about the REN-ISAC. Information will include a description of the membership model, benefits of membership, and the steps to join. Speakers from a cross-section of REN-ISAC member institutions will speak to REN-ISAC’s benefits from each of those perspectives. Plenty of time will be devoted to Q&A.

6:30 p.m.–8:30 p.m.

Dinner on Your Own

Program Committee Dinner
(by invitation only)

8:30 p.m.–10:00 p.m.

Birds-of-a-Feather Sessions
WHITE RIVER BALLROOM F

We invite you to join colleagues for birds-of-a-feather discussions. During this time you can network with those who share similar interests or responsibilities and discuss topics of particular interest to you. These sessions are designed to encourage you to exchange experiences and insights with colleagues. You can also establish a new topic by notifying us in advance (security-council@educause.edu) or signing up on the board near the registration desk.

Topics include: SANS InfoSec Standards for System Administrators
Wednesday’s Schedule at a Glance

7:30 a.m.–8:30 a.m.
Breakfast  
WHITE RIVER BALLROOM F  
SPONSORED BY STONESOFT

7:30 a.m.–5:30 p.m.
Registration Desk Open  
WHITE RIVER BALLROOM FOYER

8:30 a.m.–9:00 a.m.
Welcome and Introductions  
WHITE RIVER BALLROOM E

9:00 a.m.–10:00 a.m.
The Dynamic Landscape, from a Security Perspective  
WHITE RIVER BALLROOM E

10:00 a.m.–10:45 a.m.
Refreshment Break and Corporate Displays  
WHITE RIVER BALLROOM FOYER

10:45 a.m.–11:45 a.m.
Concurrent Sessions
Advanced Technology
Using OpenFlow and Commodity Clusters for Multi-Gigabit IDS  
MEETING ROOM 103/104
Winning the Battle against Phishing Scams  
WHITE RIVER BALLROOM A

Awareness and Training
Capture the Flag as a Tool for Training and Teaching  
WHITE RIVER BALLROOM B

Governance, Risk, and Compliance
There’s Data Lurking in Your Labs!  
WHITE RIVER BALLROOM D

Technology Concepts
IPv6 Security at Virginia Tech and WPI

11:45 a.m.–1:00 p.m.
Lunch and Roundtable Discussions  
WHITE RIVER BALLROOM F
SPONSORED BY ORACLE, GOLD PARTNER

1:00 p.m.–2:00 p.m.
Concurrent Sessions
Advanced Technology
DNS Sinkholing to Reduce Network Compromises  
MEETING ROOM 103/104
Two Approaches to Security Tools Using Flowlogs, IDS, Port Scans, Darknets, Honeypots, Passive DNS, and Much More  
WHITE RIVER BALLROOM B

Awareness and Training
Phishing Ourselves to Raise Awareness  
WHITE RIVER BALLROOM A

Governance, Risk, and Compliance
Ensuring Electronic Data Records Integrity through a Simple Audit Process  
WHITE RIVER BALLROOM D

Technology Concepts
Campus-Wide Vulnerability Scanning  
WHITE RIVER BALLROOM C
Enhancing Desktop Security in a Time of New and Evolving Threats  
WHITE RIVER BALLROOM E

2:00 p.m.–2:45 p.m.
Refreshment Break and Corporate Displays  
WHITE RIVER BALLROOM FOYER
2:45 p.m.–3:45 p.m.

Corporate and Campus Solutions

Automated, Rapid Response to Botnets and Advanced Malware Infections in a University Environment

WHITE RIVER BALLROOM D

Cybercrime Threats: How Criminals Bypass Security Measures to Steal Your Sensitive Data, Money, and Reputation

MEETING ROOM 103/104

Do We Stand a Chance in the War against Spear Phishers?

WHITE RIVER BALLROOM B

Network Security That Works for IT and Users

WHITE RIVER BALLROOM C

Real-Life Use Cases for Vulnerability Management and Best Practices

WHITE RIVER BALLROOM A

Securing Hyperconnected Networks: Tales from the Frontlines of BYOD

WHITE RIVER BALLROOM E

Awareness and Training

Securing the Human on Your Campus: How to Successfully Deploy Your Security Awareness Program

WHITE RIVER BALLROOM E

Governance, Risk, and Compliance

Governance, Risk, and Compliance Systems in Higher Education

WHITE RIVER BALLROOM D

Technology Concepts

Gaming the System: A Business Continuity Tabletop Exercise Simulation

WHITE RIVER BALLROOM C

Tools, Techniques, and Practices: Lightning Round

WHITE RIVER BALLROOM B

5:30 p.m.–6:30 p.m.

Joint Reception

SPONSORED BY OPENDNS

WHITE RIVER BALLROOMS G-J

6:30 p.m.–7:00 p.m.

PGP Key Signing

MEETING ROOM 103/104

6:30 p.m.–8:30 p.m.

Dinner on Your Own

8:30 p.m.–10:00 p.m.

Birds-of-a-Feather Sessions

WHITE RIVER BALLROOM F
WEDNESDAY, MAY 16

7:30 a.m.–8:30 a.m.
  Breakfast  
  SPONSORED BY STONESOFT  
  WHITE RIVER BALLROOM F

7:30 a.m.–5:30 p.m.
  Registration Desk Open  
  WHITE RIVER BALLROOM FOYER

8:30 a.m.–9:00 a.m.
  Welcome and Introductions  
  WHITE RIVER BALLROOM E  
  Rodney Petersen, Senior Government Relations Officer and Managing Director, Washington Office, EDUCAUSE; Mark S. Bruhn, Associate Vice President, Public Safety and Institutional Assurance, Indiana University; Jodi-Ann Ito, Information Security Officer, University of Hawaii System Office; Larry D. Conrad, Vice Chancellor and CIO, University of North Carolina at Chapel Hill; Robert F. Brammer, Senior Advisor to the CEO, Internet2

9:00 a.m.–10:00 a.m.
  General Session  
  The Dynamic Landscape, from a Security Perspective  
  WHITE RIVER BALLROOM E  
  Brian Tillett, Chief Security Strategist, Symantec Public Sector  
  We will briefly cover the latest trends—which we all need to be aware of—from the Symantec Internet Security Threat Report. We’ll also take a look at how the overall information technology landscape has changed over the past 10 years, from the “Do I have my firewall installed in the right direction?” and “Are my antivirus signatures up to date?” of yesteryear, to how to tackle “Bringing your own device and still having a secure environment” coupled with “What should ‘the cloud’ mean to my organization, and how do we control sensitive information flow in this completely new open IT world?”

10:00 a.m.–10:45 a.m.
  Refreshment Break and Corporate Displays  
  WHITE RIVER BALLROOM FOYER  
  Fifteen 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. A company directory including products and services is located in the back of this print program.
WeDneSDay, May 16

10:00 a.m.–10:45 a.m. cont.

**CORPORATE DISPLAYS**

**Audible Magic Corporation**
As an industry leader in patented “fingerprinting” technology, Audible Magic’s CopySense products provide copyright-sensitive identification that accurately detects copyrighted material. The device is easy to install, easy to run, and easy to manage. It can also be customized to deliver the messages and sanctions that support your policies on unauthorized network downloads.

**Cherwell Software**
Noted by Forrester as an emerging leader, Cherwell Service Management software provides help desk professionals with out-of-the-box ITSM processes, a self-service portal, real-time metrics/dashboards, mobile access, and social media integration—all at competitive pricing. Get up-and-running in just weeks with incident, service catalog, problem, change, and service-level management.

**CloudLock**
CloudLock’s data security suite gives organizations the enterprise-class visibility and control they need for their data in the cloud. Its flagship product, CloudLock for Google Apps, lets companies implement secure collaboration and enforce acceptable use policies. The largest Google Apps customers in the world trust CloudLock to secure their data.

**Cloudpath Networks**
Cloudpath Networks connects users effortlessly to WPA2 wireless and 802.1X wired networks. Let us show you how universities large and small use XpressConnect to enable industry-standard wireless security with minimal support overhead and ensure a great end-user experience.

**Corero Network Security**
Corero Network Security is a leading global provider of distributed denial of service (DDoS) attack defense and network intrusion prevention systems (IPS) solutions that enable enterprise organizations to protect their critical online assets against risks associated with network-borne cyberthreats. Our solutions have been deployed at educational institutions throughout the United States and abroad.

**Damballa: Advanced Cyberthreat Protection**
Damballa is the leader in advanced cyberthreat protection, pinpointing active breaches in networks from advanced malware, APTs, botnet agents, and zero-day threats that have bypassed traditional and virtual defense layers. Damballa spots threats entering a network or trying to communicate out of a network and confirms the risks.

**Fischer International Identity**
Fischer International provides cloud-based and on-premise identity management solutions for today’s business climate: low cost, no risk, rapid time-to-value, no capital expenses, and interoperability at its core to quickly and
WeDneSDay, May 16

inexpensively extend security, user access control, business efficiency, and regulatory compliance benefits to all parts of your enterprise.

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 flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem onset and resolution. Enterprises worldwide rely on Lancope to make better network decisions and avoid costly outages and downtime.

PhishMe

PhishMe.com provides organizations with the ability to train their employees and customers about the risks of spear phishing. With over one and a half million individuals trained, PhishMe has proven that its trainings can reduce the threat of employees and customers falling victim to phishing attacks by up to 80 percent.

Proofpoint

Proofpoint is a pioneering security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving and governance, and secure communications. Organizations around the world depend on Proofpoint’s expertise, patented technologies, and on-demand delivery system to protect against phishing, malware, and spam; safeguard privacy; encrypt sensitive information; and archive and govern messages and critical enterprise information. More information is available at proofpoint.com.

Qualys, Bronze Partner

Qualys is a pioneer and leading provider of information security and compliance cloud solutions with over 5,500 customers in 85 countries, including 51 of the Forbes Global 100. The QualysGuard Cloud Platform and integrated suite of applications helps businesses simplify security operations and lower costs, delivering critical security intelligence on demand.

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 the premier software solution for higher education, helping institutions save, make, and manage money better throughout the campus enterprise.

Trusteer

Trusteer is a leading provider of endpoint cybercrime prevention solutions that protect organizations from financial fraud and data breaches. Hundreds of organizations and millions of end users rely on Trusteer to protect their
10:00 a.m.–10:45 a.m. cont.

computers and mobile devices from online threats that are invisible to legacy security solutions. Trusteer’s Cybercrime Prevention Architecture combines multilayer security software with real-time threat intelligence to achieve sustainable protection against malware and phishing attacks.

**Trustwave**

Trustwave is a leader in information security and compliance management solutions. We tailor our higher education business unit’s products and services to meet the unique needs of over 400 colleges and universities. Learn how we can help your institution address its web, network, application, and data-security needs.

10:45 a.m.–11:45 a.m.

Concurrent Sessions

*Advanced Technology*

**Using OpenFlow and Commodity Clusters for Multi-Gigabit IDS**

**Meeting Room 103/104**

Ali Khalfan, Programmer/Analyst, Indiana University; Keith Lehigh, Lead Security Engineer, Indiana University-Purdue University Indianapolis

Multi-gigabit network connections are proliferating, and commercial monitoring solutions can be prohibitively expensive for budget-constrained institutions. We’ll discuss a cost-effective and open-source approach using OpenFlow load-balancing switches and a cluster of commodity hardware.

**Winning the Battle against Phishing Scams**

**White River Ballroom A**

Harvard C. Townsend, CISO, Kansas State University

Since January 2008, K-State has been plagued by spear phishing scams that attempt to steal users’ e-IDs and passwords. Unfortunately, this has proven to be a particularly effective form of social engineering, with over a thousand K-Staters falling victim to these scams in the past four years. We’ll provide detailed statistics about these scams, the demographics of the victims (it’s not just naive freshmen), and examples that were particularly effective at tricking people. We’ll also detail what we did to dramatically reduce the number of compromised accounts in 2011 after three years of frustration and lost battles.

*Awareness and Training*

**Capture the Flag as a Tool for Training and Teaching**

**White River Ballroom B**

Cornelis Leune, Information Security Officer, Adelphi University

Augmenting classroom-based technical security training with hands-on capture the flag (CTF) environments enables participants to develop
information security skills and to put theoretical knowledge to use in a controlled, purpose-built environment. Learning-by-doing, also known as experiential learning, is proven to be a very effective method to train technically inclined staff members, as concepts are put into practice immediately and consequences are demonstrated clearly. This presentation will provide an overview of using CTF as a teaching tool and show how system administrators and software developers alike have taken an immediate liking to it.

**Governance, Risk, and Compliance**

**There’s Data Lurking in Your Labs!**

**WHITE RIVER BALLROOM D**

Warren Petrofsky, Director of Information Security and UNIX Systems, University of Pennsylvania

Securing the research data spread across your institution is a challenge requiring robust processes of discovery, triage, and diplomacy. Almost inevitably some of your most critical research data will be stored lovingly in a wetlab on an SGI Indy that “must not be patched.” This presentation will describe how the School of Arts and Sciences at UPenn has combined university policy with data “interventions” to entice researchers to move critical data to centralized services. We’ll discuss access control, service agreements, and charge-backs and how to convince faculty without using FUD (fear, uncertainty, and doubt). Attendees will leave with a reproducible model for finding and securing research data.

**Technology Concepts**

**IPv6 Security at Virginia Tech and WPI**

**WHITE RIVER BALLROOM C**

Randy Marchany, CISO, Virginia Tech; Phillip Deneault, Information Security Officer, Worcester Polytechnic Institute

Institutions are hesitant to migrate to IPv6 because of perceived difficulties in supporting clients, servers, and the network infrastructure. IPv6 will force institutions to rethink their strategies and practices supporting services such as NAT and DHCP. Unfortunately, IPv6 traffic is also transparent to campus networking and security staff due to a lack of vendor security products capable of analyzing IPv6 traffic. This talk will discuss two institutions’ IPv6 implementation processes. Virginia Tech has been running a full-production IPv6 network since 2006 and has been an active implementer since 1998, when the project was conceived. WPI has some production IPv6 available on its servers, with a tentative goal of offering IPv6 client support by fall 2012. Using real-world examples, we’ll highlight successes and pitfalls in technology and policy at both institutions. We’ll also feature several solutions to common security problems related to implementation of IPv6 networks and the seamless support of both IPv4 and IPv6.
10:45 a.m.–11:45 a.m. cont.

WHITE RIVER BALLROOM E
Carol Myers, Director College Technology, Paradise Valley Community College

As a security professional, have you been asked to evaluate or provide input on security for cloud computing or mobile technologies when neither is really your area of expertise? Don’t panic! Use the Information Security Guide, sponsored by the EDUCAUSE/Internet2 Higher Education Information Security Council. We’ll discuss practical security considerations for cloud computing and mobile devices. All references are from the Information Security Guide.

11:45 a.m.–1:00 p.m.

Lunch and Roundtable Discussions
SPONSORED BY ORACLE, GOLD PARTNER
WHITE RIVER BALLROOM F

Roundtable Discussions
Career Progression Plan for Security Professionals
Compliance and Governance
Cloud (including NET+ Services, Unsanctioned Clouds, Privacy and Security)
Department of Education
E-Discovery and Forensics
Encryption (Whole Disk, File)
Finding Sensitive Data
Identity and Access Management Program Development
Identity Management
InCommon (Assurance Program, Certificates)
IPv6
Late-Breaking Topics
Metrics
Network Security (including Wireless, NAC, IDS, IPS, etc.)
Oracle Security
Physical Security
Risk-Assessment Strategies
Security and Privacy for Mobile Devices (BYOD, MDM)
Security Awareness
Security for Research
Social Media and Reputation Management (Institutional/Personal)
Web Application Security (including PenTesting)
WEDNESDAY, MAY 16

1:00 p.m.–2:00 p.m.

Concurrent Sessions

Advanced Technology

DNS Sinkholing to Reduce Network Compromises
MEETING ROOM 103/104

Brandon Dixon, Security Engineer, and Matthew Wollenweber, Principal Security Engineer, The George Washington University; Melissa Muth, Senior Information Security Analyst, University of Pennsylvania

Large university networks are often decentralized as a result of organic growth and federation between schools. These environments therefore tend to lack centralized network security controls, which makes mitigating threats difficult. Antivirus software and patching aren’t enough to protect clients from zero-day threats, polymorphic malware, and malicious third-party ads hosted on otherwise legitimate websites. We’ll compare and contrast two different implementations of a DNS sinkhole, which ultimately led to a minimum 70% reduction in compromises at two different universities. Attendees will come away with a firm understanding of two different DNS sinkhole implementations, with quantitative evidence of their effectiveness, and with a model for handling privacy concerns.

Two Approaches to Security Tools Using Flowlogs, IDS, Port Scans, Darknets, Honeypots, Passive DNS, and Much More
WHITE RIVER BALLROOM B

Justin C. Klein Keane, Senior Information Security Specialist, University of Pennsylvania; Brian Allen, Network Security Analyst, and Patrick Crowley, Associate Professor of Computer Science, Washington University in St. Louis

Come see two approaches to security tools that incorporate flowlogs, IDS, port scans, darknets, honeypots, passive DNS, and much more, plus see many real-world examples of incidents they detected. Washington University has developed PNA (passive network appliance), a network monitoring and security tool that provides a superior understanding of an enterprise network’s Internet traffic behavior, particularly in the presence of encrypted services. The University of Pennsylvania School of Arts and Sciences developed HECTOR (Hector Entity Coordination and Tracking Operational Repository), a security intelligence repository based on open-source technologies that provides data for information security decision making.

Awareness and Training

Phishing Ourselves to Raise Awareness
WHITE RIVER BALLROOM A

Derek Spransy, Senior Information Security Specialist, Emory University

Emory University and Healthcare changed phishing awareness approaches in 2010 from using traditional e-mail and web-based awareness messages to employing a third-party service to send phishing e-mails to everyone on campus.
We’ve tracked the results of these efforts both over time and between a number of different demographic variables. We’ll discuss notable trends and what level of value we feel we obtained from this approach. We’ll also cover the technical and nontechnical challenges we encountered and how we addressed them.

**Governance, Risk, and Compliance**

**Ensuring Electronic Data Records Integrity through a Simple Audit Process**

WHITE RIVER BALLROOM D

Theresa Semmens, Chief IT Security Officer, North Dakota State University

To incorporate efficiencies, reduce paper records, and provide a central repository for data records, institutions are implementing an electronic data records process to convert paper records into electronic format. This “green” implementation requires that institutions ensure the CIA (confidentiality, integrity, and availability) of the documents. This presentation will describe a simple audit process for testing the compliance of electronic records as they relate to CIA. Attendees will identify needs and use a template to help them develop their audit scope. The results of their completed audit will identify potential issues and implementation recommendations for departments, if needed.

**Technology Concepts**

**Campus-Wide Vulnerability Scanning**

WHITE RIVER BALLROOM C

Edward Carter, Senior Security Analyst, and Thomas Conley, Senior Security Analyst, Ohio University; Kelley J. Bogart, Senior Information Security Analyst, and Gil Salazar, Senior Information Security Analyst, The University of Arizona

Scanning a campus network for vulnerabilities and managing the results can be a tedious task. Even a moderately sized network produces too much information to process manually or without a logical management system. We’ll discuss two approaches to addressing this issue. Ohio University takes a centrally managed approach and looks at each device as it comes on the network. Scanning is initiated automatically using Nessus and custom-built scripts. At the University of Arizona, scanning is done by departmental IT personnel, with the project managed by the Information Security office. The focus is on servers and applications and involves scheduled scans, training, and remediation consultations. Both methods present challenges that must be overcome. Come discuss these and other issues concerning campus-wide vulnerability scanning.

**Enhancing Desktop Security in a Time of New and Evolving Threats**

WHITE RIVER BALLROOM E

Brian Doherty, Director of Desktop Computing and Network Services, SAS Computing, University of Pennsylvania
Given new and evolving threats such as rogue security software, “drive by” attacks, and exploitation of vulnerabilities in third-party applications, it may be beneficial to supplement existing desktop security techniques with newer approaches. Application whitelisting is one such technique that, while not commonly used in higher ed settings, can greatly enhance desktop security. This presentation will focus on methods to better protect administrative desktops from such new threats using an application whitelisting technique, combined with other techniques that have been in use for a longer period of time. We’ll review the substantial benefits this approach can provide.

2:00 p.m.–2:45 p.m.

Refreshment Break and Corporate Displays

**WHITE RIVER BALLROOM FOYER**

**Corporate Displays**

**Audible Magic Corporation**

As an industry leader in patented “fingerprinting” technology, Audible Magic’s CopySense products provide copyright-sensitive identification that accurately detects copyrighted material. The device is easy to install, easy to run, and easy to manage. It can also be customized to deliver the messages and sanctions that support your policies on unauthorized network downloads.

**Cherwell Software**

Noted by Forrester as an emerging leader, Cherwell Service Management software provides help desk professionals with out-of-the-box ITSM processes, a self-service portal, real-time metrics/dashboards, mobile access, and social media integration—all at competitive pricing. Get up-and-running in just weeks with incident, service catalog, problem, change, and service-level management.

**CloudLock**

CloudLock’s data security suite gives organizations the enterprise-class visibility and control they need for their data in the cloud. Its flagship product, CloudLock for Google Apps, lets companies implement secure collaboration and enforce acceptable use policies. The largest Google Apps customers in the world trust CloudLock to secure their data.

**Cloudpath Networks**

Cloudpath Networks connects users effortlessly to WPA2 wireless and 802.1X wired networks. Let us show you how universities large and small use XpressConnect to enable industry-standard wireless security with minimal support overhead and ensure a great end-user experience.

**Corero Network Security**

Corero Network Security is a leading global provider of distributed denial of service (DDoS) attack defense and network intrusion prevention systems (IPS) solutions that enable enterprise organizations to protect their critical online assets against risks associated with network-borne cyberthreats. Our
solutions have been deployed at educational institutions throughout the United States and abroad.

**Damballa: Advanced Cyberthreat Protection**

Damballa is the leader in advanced cyberthreat protection, pinpointing active breaches in networks from advanced malware, APTs, botnet agents, and zero-day threats that have bypassed traditional and virtual defense layers. Damballa spots threats entering a network or trying to communicate out of a network and confirms the risks.

**Fischer International Identity**

Fischer International provides cloud-based and on-premise identity management solutions for today’s business climate: low cost, no risk, rapid time-to-value, no capital expenses, and interoperability at its core to quickly and inexpensively extend security, user access control, business efficiency, and regulatory compliance benefits to all parts of your enterprise.

**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 flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem onset and resolution. Enterprises worldwide rely on Lancope to make better network decisions and avoid costly outages and downtime.

**PhishMe**

PhishMe.com provides organizations with the ability to train their employees and customers about the risks of spear phishing. With over one and a half million individuals trained, PhishMe has proven that its trainings can reduce the threat of employees and customers falling victim to phishing attacks by up to 80 percent.

**Proofpoint**

Proofpoint is a pioneering security-as-a-service provider that focuses on cloud-based solutions for threat protection, compliance, archiving and governance, and secure communications. Organizations around the world depend on Proofpoint’s expertise, patented technologies, and on-demand delivery system to protect against phishing, malware, and spam; safeguard privacy; encrypt sensitive information; and archive and govern messages and critical enterprise information. More information is available at [proofpoint.com](http://proofpoint.com).
WEDNESDAY, MAY 16

Qualys, Bronze Partner
Qualys is a pioneer and leading provider of information security and compliance cloud solutions with over 5,500 customers in 85 countries, including 51 of the Forbes Global 100. The QualysGuard Cloud Platform and integrated suite of applications helps businesses simplify security operations and lower costs, delivering critical security intelligence on demand.

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 the premier software solution for higher education, helping institutions save, make, and manage money better throughout the campus enterprise.

Trusteer
Trusteer is a leading provider of endpoint cybercrime prevention solutions that protect organizations from financial fraud and data breaches. Hundreds of organizations and millions of end users rely on Trusteer to protect their computers and mobile devices from online threats that are invisible to legacy security solutions. Trusteer’s Cybercrime Prevention Architecture combines multilayer security software with real-time threat intelligence to achieve sustainable protection against malware and phishing attacks.

Trustwave
Trustwave is a leader in information security and compliance management solutions. We tailor our higher education business unit’s products and services to meet the unique needs of over 400 colleges and universities. Learn how we can help your institution address its web, network, application, and data-security needs.

2:45 p.m.–3:45 p.m.
Corporate and Campus Solutions

Automated, Rapid Response to Botnets and Advanced Malware Infections in a University Environment
WHITE RIVER BALLROOM D
Tammy L. Clark, CISO, Georgia State University; Brian Taylor, Director of Systems Engineering, Damballa

Evasive threats such as advanced persistent threats, next-generation malware, and botnets have altered the modern security landscape. Adding to the complexity and risks are environments that allow personal devices onto research, student, and faculty networks. In this session, see how Georgia State University automates the detection of bot infections inside the network by using Damballa Failsafe to rapidly pinpoint malware activity and criminal bot command-and-control communications. By streamlining response processes, GSU is able to rapidly remove infected users from their network and offload first-level remediation to data center operations, freeing up the security team for other initiatives.
2:45 p.m.–3:45 p.m. cont.

**Cybercrime Threats: How Criminals Bypass Security Measures to Steal Your Sensitive Data, Money, and Reputation**

**MEETING ROOM 103/104**

**Michelle Dilanian,** Account Executive, Higher Education, Trusteer

Data breaches and credential/PII theft incidents are becoming more prevalent, and recent red flag rules require heightened data security procedures. Meanwhile, BYOD, social media proliferation, and a growing reliance on cloud and SaaS applications only increase the chance that your users’ devices will be compromised. Cybercriminals have created malicious software specifically designed to bypass your existing security controls and network and application protection measures by infecting end-user devices directly. This malware evades standard antivirus and antimalware solutions. We’ll describe these cybercrime techniques, review lessons learned from recent incidents, and present possible solutions.

**Do We Stand a Chance in the War against Spear Phishers?**

**WHITE RIVER BALLROOM B**

**Aaron Higbee,** Chief Technology Officer, PhishMe; **Brad Sanford,** CISO, Emory University

Targeted phishing attacks have become the number-one attack vector to break into organizations. Lax technical security control, a social media–friendly generation, and sensitive research data make higher educational institutions and universities a juicy target. Merely throwing technology at the problem hasn’t gotten us very far. What can we do to mitigate this trend? We’ll discuss setting up an antiphishing education program that relies on mock phishing exercises as the means of propagating educational materials to those found susceptible.

**Network Security That Works for IT and Users**

**WHITE RIVER BALLROOM C**

**Tim Evans,** Vice President, Impulse Point; **Eric Weakland,** Director, Information Security, American University

The traditional approach to network security is to institute top-down policy measures that are then imposed on users with a patchwork of systems to maintain compliance. This approach is inherently flawed because it fails to make the user an active participant in creating and maintaining a secure computing environment. American University will discuss how the implementation of Impulse Point’s network access control solution balanced IT staff and users’ need for convenient access. Impulse Point will also present the user-centric elements of its NAC solution.

**Real-Life Use Cases for Vulnerability Management and Best Practices**

**WHITE RIVER BALLROOM A**

**Mike Chapple,** Senior Director, Enterprise Support Services, University of Notre Dame; **Maurice Hampton,** Technical Account Manager, Qualys; **Tom Siu,** Chief Information Security Officer, Case Western Reserve University
In this session, we will present trends and leading practices for vulnerability management in higher education. University IT security professionals will discuss the unique challenges for vulnerability management in academic and research-centric environments. They’ll also describe how they were able to leverage a cloud service from Qualys to cost-effectively and easily deploy and manage identification and remediation of vulnerabilities to protect their data and IT assets.

Securing Hyperconnected Networks: Tales from the Frontlines of BYOD
WHITE RIVER BALLROOM E
David Buckwald, Director of Systems Engineering, SonicWALL

With the explosion of laptops, smartphones, and tablets and the online resources they access, IT security challenges can seem overwhelming. New tools and strategies are needed that manage the applications on the network and enforce policies in the background, protecting an institution’s assets and resources while fostering an environment of increased openness. Learn from the experience of five different universities and colleges, presented by the director of systems engineering for one of the industry’s leading network security providers, SonicWALL.

4:00 p.m.–5:30 p.m.
Concurrent Sessions

Advanced Technology

Are You Ready? A Planning Tool for Managing Sensitive Data Incidents
WHITE RIVER BALLROOM A
Kimberly A. Milford, University Information Policy Officer, Indiana University; Shirley C. Payne, Assistant Vice President for Information Security, Policy & Records, University of Virginia

Universities have had to deal with many different types of incidents involving the exposure of sensitive and legally protected information. When an incident occurs, those involved usually have limited experience with such occurrences. They look for guidance to manage the appropriate response, including incident identification, assessment, eradication, recovery, notification, and follow-up. The EDUCAUSE HEISC Governance, Risk, and Compliance Working Group has developed a framework and checklist for universities, schools, and departments to easily come up to speed and manage such incidents effectively and efficiently. We’ll walk through the resources available in the sensitive data exposure incident checklist.

Tools and Methods for Managing Snort Sensors in Distributed Environments
MEETING ROOM 103/104
Edward Carter, Senior Security Analyst, and Scott Pack, Information Security Analyst, Ohio University; Larry Parker, Information Security Specialist, University at Albany, SUNY
4:00 p.m.–5:30 p.m. cont.

Intrusion Detection Systems are a valuable component of a security monitoring program; however, they can be expensive to operate, both in terms of equipment/licensing costs and person hours. By making use of commodity hardware and open-source products, Ohio University has greatly simplified the management while minimizing the associated costs. University at Albany-SUNY will discuss tools and methods by which one can manage the large number of Snort signatures and ensuing deluge of alerts.

**Awareness and Training**

**Securing the Human on Your Campus: How to Successfully Deploy Your Security Awareness Program**

**WHITE RIVER BALLROOM E**

**Doug Markiewicz**, Assistant Director of Information Security, Carnegie Mellon University; **Daniel deBeaubien**, Director, Information Technology Services and Security, Michigan Technological University; **Randy Marchany**, CISO, Virginia Tech

*Moderated by: John Fitzgerald*, Managing Director, The SANS Technology Institute

Security awareness must be a critical part of any university’s information security program. Institutions of higher education are the gateway for important research. They hold personal records of future leaders of our country, and they are a critical part of the innovation critical infrastructure. They are a target that’s under attack on a daily basis. Many of these attackers today target the human, bypassing most security controls and using techniques such as social engineering to get what they want. Awareness, not just of technology, is now a key factor in a university’s ability to reduce risk, protect its reputation, improve governance, and, in many cases, ensure compliance.

**Governance, Risk, and Compliance**

**Governance, Risk, and Compliance Systems in Higher Education**

**WHITE RIVER BALLROOM D**

**Cheryl Washington**, CISO, California State University, Office of the Chancellor; **Merri Beth Lavagnino**, Chief Privacy Officer and Compliance Coordinator, Indiana University; **Jennifer A. Stewart**, Privacy Coordinator, The Pennsylvania State University

*Moderated by: Sarah D. Morrow*, Chief Privacy Officer, The Pennsylvania State University

GRC (governance, risk, and compliance) systems are integrated applications that help automate the policy development and dissemination process; the tracking of requirements of law, regulations, standards, and frameworks such as ISO and NIST; the risk assessment and mitigation process; and many other similar functions. Such systems are new to higher education but have been used in industry for years for both IT GRC and enterprise-wide GRC purposes. Join us as we explain how these systems can
be used in higher education. We’ll also share the stories of three universities that are actively seeking and implementing GRC systems.

*Technology Concepts*

**Tools, Techniques, and Practices: Lightning Round**

**WHITE RIVER BALLROOM B**

George Mathew, Chief Technology Officer, Goodwin College, Drexel University; Adam Arrowood, Research Scientist I, and Jason Belford, Information Security Operations Manager, Georgia Institute of Technology; Kevin R. Keough, Senior Information Systems Auditor, Indiana University; Justin Azoff, Security & Network Analyst, University at Albany, SUNY

Discover the tools, techniques, and practices that are already working in higher education and how you can adapt these at your institutions.

*Fighting Backlinks: Identifying and Mitigating Unauthorized Ads on your Webserver* — Georgia Tech

*InCommon Silver Compliance Validation Developed by the Big 10 IT Auditors* — Indiana University

*Netflow-Indexer: Indexing Your Existing Netflow Data for Lightning Fast Searches* — University at Albany-SUNY

*Security Issues Related to Smart Phone Applications* — Drexel University

**Gaming the System: A Business Continuity Tabletop Exercise Simulation**

**WHITE RIVER BALLROOM C**

Christine Brisson, Senior IT Project Leader, University of Pennsylvania

You’ve worked hard to develop a business continuity plan. Great, but will it work? Find out by testing it with a tabletop exercise (TTX). Although it’s extremely useful, a TTX is also difficult to plan and therefore not used as frequently as it should be. In this session, we’ll treat a TTX as a game that everyone gets to play. Attendees will play the roles of participants in a TTX based on an actual exercise used at the University of Pennsylvania. By participating in a “real” tabletop, attendees will leave with the tools needed to plan their own TTXs.

5:30 p.m.–6:30 p.m.

**Joint Reception**

**SPONSORED BY OPENDNS**

**WHITE RIVER BALLROOMS G-J**

One of the most valuable aspects of this conference is the opportunity to connect face-to-face with fellow Security Professionals and Enterprise IT Leadership Conference 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.
WEDNESDAY, MAY 16

6:30 p.m.–7:00 p.m.
PGP Key Signing
MEETING ROOM 103/104
Brian Epstein, Computer Manager, Network and Security, Institute for Advanced Study; Ken Connelly, Associate Director, Security and Systems, University of Northern Iowa
Additional information is available on this at ren-isac.net/events/spc_2012_keysigning. Questions about this event should be directed to the presenters.

6:30 p.m.–8:30 p.m.
Dinner on Your Own

8:30 p.m.–10:00 p.m.
Birds-of-a-Feather Sessions
WHITE RIVER BALLROOM F
We invite you to join colleagues for birds-of-a-feather discussion sessions, where you can network with those who share similar interests or responsibilities and discuss topics of particular interest to you. These sessions are designed to encourage you to exchange experiences and insights with colleagues. You can also establish a new topic by notifying us in advance (security-council@educause.edu) or signing up on the sign near the registration desk.
Topics include: Open Source Identity Management for Higher Education initiative, OSIdM4HE
### THURSDAY’S SCHEDULE AT A GLANCE

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6:00 a.m.–6:45 a.m.</strong></td>
<td>Fun Run&lt;br&gt;<strong>HOTEL LOBBY</strong></td>
</tr>
<tr>
<td><strong>7:00 a.m.–8:15 a.m.</strong></td>
<td>Breakfast&lt;br&gt;2013 Program Committee Breakfast&lt;br&gt;by invitation only 注意：只有受邀人士可以参加。</td>
</tr>
<tr>
<td><strong>7:15 a.m.–5:00 p.m.</strong></td>
<td>Registration Desk Open&lt;br&gt;<strong>WHITE RIVER BALLROOM FOYER</strong></td>
</tr>
<tr>
<td><strong>7:15 a.m.–8:15 a.m.</strong></td>
<td>Breakfast&lt;br&gt;<strong>SPONSORED BY MODULO SECURITY</strong>&lt;br&gt;<strong>WHITE RIVER BALLROOM F</strong></td>
</tr>
<tr>
<td><strong>8:15 a.m.–9:30 a.m.</strong></td>
<td>General Session&lt;br&gt;<strong>Ensuring Effective Communications for Information Security on Campus</strong>&lt;br&gt;<strong>SPONSORED BY GFI SOFTWARE</strong>&lt;br&gt;<strong>WHITE RIVER BALLROOM E</strong></td>
</tr>
<tr>
<td><strong>9:30 a.m.–9:45 a.m.</strong></td>
<td>Refreshment Break&lt;br&gt;<strong>WHITE RIVER BALLROOM FOYER</strong></td>
</tr>
<tr>
<td><strong>9:45 a.m.–10:45 a.m.</strong></td>
<td>Concurrent Sessions&lt;br&gt;<strong>Advanced Technology</strong>&lt;br&gt;Data Governance: Essential for Strategy, Policy, and Operations&lt;br&gt;<strong>MEETING ROOM 103/104</strong></td>
</tr>
<tr>
<td><strong>10:45 a.m.–11:00 a.m.</strong></td>
<td>Refreshment Break&lt;br&gt;<strong>WHITE RIVER BALLROOM FOYER</strong></td>
</tr>
<tr>
<td><strong>11:00 a.m.–12:00 noon</strong></td>
<td>Concurrent Sessions&lt;br&gt;<strong>Advanced Technology</strong>&lt;br&gt;On the Edges of Policy Questions, Student Privacy, and Student Learning&lt;br&gt;<strong>MEETING ROOM 103/104</strong></td>
</tr>
<tr>
<td><strong>10:45 a.m.–11:00 a.m.</strong></td>
<td>Security Metrics: Telling the Right Story&lt;br&gt;<strong>WHITE RIVER BALLROOM B</strong></td>
</tr>
<tr>
<td><strong>11:00 a.m.–12:00 noon</strong></td>
<td>Awareness and Training&lt;br&gt;Building an Information and IT Compliance Program&lt;br&gt;<strong>WHITE RIVER BALLROOM A</strong></td>
</tr>
</tbody>
</table>

### Highlight Sessions

- **Leading the Way to PCI Compliance: It’s All About Planning and Collaboration**<br>**WHITE RIVER BALLROOM A**
- **Governance, Risk, and Compliance**<br>Identity and Access Management: The Intersection with Privacy and Security at Penn State<br>**WHITE RIVER BALLROOM D**
- **Technology Concepts**<br>Security on the Cheap: Creating a Cost-Effective Information Security Program<br>**WHITE RIVER BALLROOM C**
- **Virtualization beyond Servers: Delivering a New Desktop and Application Deployment Strategy**<br>**WHITE RIVER BALLROOM B**
Governance, Risk, and Compliance

InSight: Helping Management Make Informed IT and Information Security Management Decisions
WHITE RIVER BALLROOM D

Technology Concepts

Lions and Tigers and Mobile Devices: Removing the Fear Factor from Securing Smart Devices
WHITE RIVER BALLROOM E

Security in the Global Network University
WHITE RIVER BALLROOM C

12:00 noon–1:00 p.m.
Lunch for Postconference Seminar Participants
WHITE RIVER BALLROOM F

12:00 noon–10:00 p.m.

SEM01Z

REN-ISAC Member Meeting
(REN-ISAC members only)
WHITE RIVER BALLROOM I/J

1:00 p.m.–4:30 p.m.

Postconference Seminars

Seminar 02Z
Engage! Creating a Meaningful Security Awareness Program
WHITE RIVER BALLROOM H

Seminar 03Z
Developing an Approach to Mobile Security: A Workshop
WHITE RIVER BALLROOM G
THURSDAY, MAY 17

6:00 a.m.–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.

7:00 a.m.–8:15 a.m.

Breakfast
2013 Program Committee Breakfast
(by invitation only)
MEETING ROOM 101/102

7:15 a.m.–5:00 p.m.

Registration Desk Open
WHITE RIVER BALLROOM FOYER

7:15 a.m.–8:15 a.m.

Breakfast
SPONSORED BY MODULO SECURITY
WHITE RIVER BALLROOM F

8:15 a.m.–9:30 a.m.

General Session
Ensuring Effective Communications for Information Security on Campus
SPONSORED BY GFI SOFTWARE
WHITE RIVER BALLROOM E
Jane Drews, CISO, The University of Iowa; Levester Johnson, Vice President for Student Affairs, Butler University; Roger V. Bruszewski, Vice President, Finance & Administration, Millersville University of Pennsylvania; Michele Norin, CIO, The University of Arizona
Moderated by: Brian D. Voss, Vice President & CIO, University of Maryland
A panel of C-level executives from institutions of higher education will share their perspectives on the importance of information security on campus, including how to ensure strategic investments and effectively communicate policies to various campus groups to protect institutional cyber assets. This session will focus on how the institutions use a risk-based approach to information security governance.
9:30 a.m.–9:45 a.m.
Refreshment Break
WHITE RIVER BALLROOM FOYER

9:45 a.m.–10:45 a.m.
Concurrent Sessions

**Advanced Technology**

**Data Governance: Essential for Strategy, Policy, and Operations**
MEETING ROOM 103/104
Shirley C. Payne, Assistant Vice President for Information Security, Policy & Records, University of Virginia

Whether your data resides in a campus data center, is held by a third party in a hosted system, or is distributed in the cloud, you’ll be confronted with situations that require strategic and effective decision making regarding your information assets. Data governance is intended to address data quality, data management, data policies, privacy and security, business process management, and risk management surrounding the handling of data. This presentation will describe what effective data governance looks like and provide guidance for building a data governance program.

**Information Security: A “State of the Union” Review**
WHITE RIVER BALLROOM E
David Escalante, Director of Computer Policy & Security, Boston College; Brian Smith Sweeney, Project Lead, New York University; Phillip Deneault, Information Security Officer, Worcester Polytechnic Institute

Last year the HEISC posed the question to various security working groups, “What has improved in security in higher education in the past decade?” This session will begin by reviewing their answers, which are essentially a list of accomplishments, then move on to cover the presenters’ viewpoints regarding the most serious challenges for security practitioners and campus leaders today, or, put another way, what we think our accomplishments need to be in the next 10 years to be secure.

**Awareness and Training**

**Leading the Way to PCI Compliance: It’s All About Planning and Collaboration**
WHITE RIVER BALLROOM A
Tammy L. Clark, CISO, Georgia State University; Kelley J. Bogart, Senior Information Security Analyst, The University of Arizona

So, you were nominated to conduct a PCI (payment card industry) compliance review. PCI is more than a rigorous examination of technical controls—it’s just as much about evaluating the various ways people...
process, transmit, and store credit card information. The hardest part is getting started. We’ll discuss important considerations in conducting PCI compliance reviews on your campus and how to develop and implement an effective PCI compliance program that will allow merchants to do business in an efficient and cost-effective manner.

**Governance, Risk, and Compliance**

**Identity and Access Management: The Intersection with Privacy and Security at Penn State**

**WHITE RIVER BALLROOM D**

Kathleen R. Kimball, Senior Director, ITS Security Operations and Services, Sarah D. Morrow, Chief Privacy Officer, and P. Renee Shuey, IAM Lead Manager, The Pennsylvania State University

Often identity and access management discussions do not include sufficient dialogue with the heads of security or privacy. In reality, IAM is an integral security architectural component and helps preserve privacy by implementing consistent enterprise authentication and authorization mechanisms; there are codependencies. Introduction of improved IAM will also likely require modified practices in both the security and privacy areas. In this session, Penn State’s leaders in security, privacy, and IAM will discuss the measures put in place to overcome the communication gaps and the tangible technical and policy benefits for all concerned.

**Technology Concepts**

**Security on the Cheap: Creating a Cost-Effective Information Security Program**

**WHITE RIVER BALLROOM C**

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

Security as presented by vendors boils down to buying the right box or software. We’ll take the point of view that effective security can be created using homegrown and open-source solutions in combination with policies and out-of-the-box thinking. Learn how we built our security program at Columbia University from scratch in a very complicated and decentralized environment. We’ll address both institutions that are looking to build their security program and those with fully functioning programs that are seeking to reduce cost or improve results.

**Virtualization beyond Servers: Delivering a New Desktop and Application Deployment Strategy**

**WHITE RIVER BALLROOM B**

Duane J. Schau, Director-Leveraged Support, Indiana University Bloomington

This presentation will highlight a new model for delivering desktops and applications as a service from the perspective of several leading academic institutions. This new approach is fundamentally changing the way desktops are currently constructed, delivered, and managed. Decoupling the user
THURSDAY, MAY 17

9:45 a.m.–10:45 a.m. cont.

persona from the local OS and application layers lessens the need for local desktop support and gives technical staff located in schools and departments more capacity to innovate. Whether desktops are delivered through server-based computing, hosted on virtual desktops or PCs, or provided in combination, the user experience remains consistent and predictable.

10:45 a.m.–11:00 a.m.
Refreshment Break
WHITE RIVER BALLROOM FOYER

11:00 a.m.–12:00 noon
Concurrent Sessions

**Advanced Technology**

**On the Edges of Policy Questions, Student Privacy, and Student Learning**
MEETING ROOM 103/104

*Brandt Redd,* Senior Technology Officer, Bill & Melinda Gates Foundation; *John Blegen,* Chief Technologist and PM–Common Education Data Standards, SHEEO

We all participate regularly in discussions of policy data, student learning data, and data privacy, yet it’s difficult to bring the three domains together without conflict, as different priorities, technologies, and ideological stances are associated with each. In our roles as IT managers and security professionals, these three subject areas compete for our attention. We’ll highlight the importance of each and suggest a series of ground rules for engaging in constructive conversation to seek essential solutions that push beyond a single domain approach to problem solving.

**Security Metrics: Telling the Right Story**
WHITE RIVER BALLROOM B

*Wyman Miles,* Director of IT Security, Cornell University

All too often security metrics are used to demonstrate work output or justify security office budget or staffing when they can be used to effectively support a message. This session will describe different use cases for metrics: the story you want to tell, data sources and methods of analysis, errors to avoid, presentation and use in security awareness, and long-term tracking.

**Awareness and Training**

**Building an Information and IT Compliance Program**
WHITE RIVER BALLROOM A

*Thomas R. Davis,* Chief Security Officer, and *Merri Beth Lavagnino,* Chief Privacy Officer and Compliance Coordinator, Indiana University; *Michael J. Chapple,* Senior Director, Enterprise Support Services, University of Notre Dame
In higher education, we’ve seen an unprecedented increase in laws and regulations that govern everything from the way we handle student data to how we process credit card information. At first we addressed compliance regulation by regulation, but this inefficient model resulted in conflicts between the guidance issued by various areas and was also confusing for employees, who must comply with multiple regulations. In this session, representatives from two universities will provide an overview of the major compliance issues facing higher education and describe an approach to building and maintaining an effective compliance program.

**Governance, Risk, and Compliance**

**InSight: Helping Management Make Informed IT and Information Security Management Decisions**

**WHITE RIVER BALLROOM D**

Randy Todd, Office of Information Security, and Steve Werby, Information Security Officer, University of Texas at San Antonio

UTSA’s InSight management tool is a web application that was implemented to help managers and executives make informed decisions concerning the management of their IT resources and information security risk. InSight collects information from multiple sources and presents it through an easy-to-use dashboard. We’ll cover our business need and the design, development, and implementation of the system as well as management, usage, successes, lessons learned, and future plans.

**Technology Concepts**

**Lions and Tigers and Mobile Devices: Removing the Fear Factor from Securing Smart Devices**

**WHITE RIVER BALLROOM E**

Lori McElroy, Information Security Officer, Texas State University–San Marcos; Shirley Erp, Information Security Architect, University of Texas System

The dramatic increase of smart devices across campus has presented security professionals with some interesting opportunities and challenges. Two Texas state institutions will review where they are in this process and share experiences such as building mobile device security awareness into the training program and managing technology implementation options. This session will offer ideas, security awareness content, an implementation checklist, and sample policy statements for those campuses just embarking on developing and implementing a smart device security strategy.

**Security in the Global Network University**

**WHITE RIVER BALLROOM C**

Brian Smith Sweeney, Project Lead, New York University

In recent years NYU has undergone a major strategic and philosophical shift from a classic university with a study abroad program to a highly distributed
11:00 a.m.–12:00 noon cont.

and interconnected global network university. This transition has had a direct and positive impact on our approach to IT security. This presentation will address a common set of challenges for establishing a global security program and our approach so far to meeting those challenges. This talk will address not only technology issues but also organizational considerations, policy and compliance land mines, and procedural rethinking.

12:00 noon–1:00 p.m.

Lunch for Postconference Seminar Participants
(lunch ticket required)
WHITE RIVER BALLROOM F

12:00 noon–10:00 p.m.

SEM01Z

REN-ISAC Member Meeting
(REN-ISAC members only)
WHITE RIVER BALLROOM I/J
Doug Pearson, Technical Director, REN-ISAC, Indiana University Bloomington; Ken Connelly, Associate Director, Security and Systems, University of Northern Iowa

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. This meeting is open only to REN-ISAC members. Lunch and dinner will be provided.

1:00 p.m.–4:30 p.m.

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

Seminar 02Z

Engage! Creating a Meaningful Security Awareness Program
WHITE RIVER BALLROOM H
Cherry L. Delaney, Coordinator, Security Awareness and Outreach, Purdue University; Ben Woelk, Information Security Policy and Awareness Analyst, Rochester Institute of Technology

This session will help attendees identify available resources and tools and determine the steps needed to create an engaging security awareness program. We’ll share how to integrate social media, video, and other resources in an effort to reach a variety of audiences. We’ll also discuss how to leverage
security incidents to create opportunities for engagement with your community. We’ll conclude the session by helping you plan a series of targeted activities for a high-profile event such as the National Cyber Security Awareness Month (October).

Seminar 03Z

**Developing an Approach to Mobile Security: A Workshop**

**WHITE RIVER BALLROOM G**

**Joseph Butler**, Principle Systems Analyst, and **Tom Zeller**, Senior Technology Analyst, Indiana University Bloomington

The presenters will lead the group in a simulation of a mobility security task force process. Working in small groups, participants will be presented with a series of questions, scenarios, policy issues, and technological enforcement mechanisms to analyze and then determine recommendations. Technical background information will be provided on various tools as input to the discussion.
EDUCAUSE is grateful to the following corporations for their participation in the Security Professionals Conference 2012.

Need more information? Contact these companies.

323link
Don Cottam, CEO
doncottam@323link.com, 615-310-3969
www.323link.com
**Product Categories:** Accessibility; Content Capture; Content Management System

Aegis Identity Software
Janet Yarbrough, Director of Business Development
janet.yarbrough@aegisidentity.com, 303-589-5435
www.aegisidentity.com
**Product Categories:** Access Control; Identity and Access Management; Single Sign-On (SSO)

Audible Magic Corporation
Todd Gedryn, Sales Representative
t_gedryn@audiblemagic.com, 408-399-6405
www.audiblemagic.com
**Product Categories:** Intrusion Detection and Prevention; Network Security and Applications; Security Policies

Caption Colorado
John Irwin, Senior Vice President Sales and Marketing
johni@captioncolorado.com, 303-468-4093
www.captioncolorado.com
**Product Categories:** Accessibility; Learning Management Systems; Media Production, Preservation, and Storage

Cherwell Software
Gail Noren, Account Executive
gail.noren@cherwell.com, 517-285-1657
www.cherwell.com
**Product Category:** Identity and Access Management
CloudLock
Tsahy Shapsa, Co-Founder
support@cloudlock.com, 781-996-4332
www.cloudlock.com
*Product Categories:* Cloud Security; Security Risk Assessment and Analysis; Vulnerability Scanning

Cloudpath Networks
Curtis Reid, Sales
curtis.reid@cloudpath.net, 303-647-1495
www.cloudpath.net
*Product Categories:* Authentication; Mobile Security; Network Security and Applications

Corero Network Security
Carlos Munoz, Regional Sales Manager
carlos.munoz@corero.com, 978-212-1500
www.corero.com
*Product Categories:* Data Security; Intrusion Detection and Prevention; Network Security and Applications

Damballa
Fred Go, Director
sales@damballa.com, 404-961-7400
www.damballa.com
*Product Categories:* Data Security; Intrusion Detection and Prevention; Network Security and Applications

*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

Fischer International Identity
Gary O’Neill, Sales Director
gjo@fischerinternational.com, 678-366-0426
www.fischerinternational.com
*Product Categories:* Identity and Access Management; Information Security Governance; Single Sign-On (SSO)
CORPORATE DIRECTORY

GFI Software
Account Representative
vipresales@gfi.com, 888-688-8457
www.gfi.com
Product Categories: Cloud Security; Firewalls; Identity Theft

Identity Finder
Chris Arold, VP of Sales
sales@identityfinder.com, 888-244-3790
www.identityfinder.com
Product Categories: Data Security; Identity Theft; Privacy

Impulse Point
Genevieve Olds, Regional Sales Manager
golds@impulse.com, 803-422-6173
www.impulse.com
Product Categories: Access Control; Identity and Access Management; Security Policies

Jenzabar, Platinum Partner
Liz DeSmit, Manager of EX Product Marketing
liz.desmit@jenzabar.net, 617-492-9099
www.jenzabar.com
Product Categories: Content Management Systems; ERP; Learning Management Systems

Lancope
David Rudd, Territory Account Manager
drudd@lancope.com, 770-225-3139
www.lancope.com
Product Categories: Intrusion Detection and Prevention; Network Security and Applications; Security Risk Assessment and Analysis

Modulo Security
Doug Payton, Manager, Market Development
doug.payton@modulo.com, 678-335-1160
www.modulo.com
Product Categories: Information Security Governance; PCI DSS; Security Risk Assessment and Analysis
CORPORATE DIRECTORY

OpenDNS
Erin Symons, Communications Manager
erin@opendns.com, 415-344-3197
www.opendns.com
**Product Categories:** Cloud Security; Mobile Security; Network Security and Applications

Oracle, **Gold Partner**
Dan Rupinski, Technology Sales Representative
dan.rupinski@oracle.com, 650-291-0852
www.oracle.com
**Product Categories:** Data Security; Identity and Access Management

PhishMe
Vanessa Bush, Marketing & Events Manager
vanessa@phishme.com, 703-652-0717 x1004
www.phishme.com
**Product Categories:** Security Risk Assessment and Analysis; Security Training; Vulnerability Scanning

Proofpoint
Ed Stacy, Education Account Manager
estacy@proofpoint.com, 408-338-6855
www.proofpoint.com
**Product Categories:** Encryption; Information Security Governance; Privacy

Qualys, **Bronze Partner**
David French, Regional Vice President
dfrench@qualys.com, 650-801-6100
www.qualys.com
**Product Categories:** Network Vulnerability Assessment; PCI DSS; Vulnerability Scanning

SonicWALL
Sales, U.S. Sales
sales@sonicwall.com, 888-557-664
www.sonicwall.com
**Product Categories:** Firewalls; Intrusion Detection and Prevention; Network Security and Applications
CORPORATE DIRECTORY

Stonesoft
Mark Boltz, Director, Federal and Mid-Atlantic
mark.boltz@stonesoft.com, 571-246-2233
www.stonesoft.com

**Product Categories:** Firewalls; Identity and Access Management; Intrusion Detection and Prevention

Symplified
Lauren Twele, Online Marketing Manager
ltwele@symplified.com, 303-318-4154
www.symplified.com

**Product Categories:** Access Control; Cloud Security; Identity and Access Management

**TouchNet Information Systems, Bronze Partner**
John Murphy, Vice President
john.murphy@touchnet.com, 913-599-6699
www.touchnet.com

**Product Categories:** Data and Media Sanitization; PCI DSS

Trusteer
Michelle Dilanian, Account Executive–Higher Education
michelle.dilanian@trusteer.com, 857-263-7234
www.trusteer.com

**Product Categories:** Data Security; Network Security and Applications; Security Architecture

Trustwave
Nemo Stankovic, Higher Education Account Executive
nstankovic@trustwave.com, 312-470-8615
www.trustwave.com/education.php

**Product Categories:** Network Security and Applications; Security Advisory and Consulting; Security Management
[TOUGH QUESTION #18]

WHO MAKES THE HIGHEST PERFORMANCE LOW LATENCY NEXT-GEN FIREWALL?

SonicWALL’s advanced security platform consolidates Next-Gen Firewall app control, gateway protection, and SSL inspection for enterprises along with WAN acceleration for distributed offices. SonicWALL’s low latency platform scans every packet of every protocol, securing the network, controlling Web 2.0 apps, and optimizing bandwidth. Learn how our SuperMassive™ E10000 and the rest of our network security line-up puts secure network optimization within reach at sonicwall.com/optimize

SONICWALL SECURES THE ENTERPRISE.

© 2012 SonicWALL, Inc. SonicWALL and the SonicWALL logo are registered trademarks of SonicWALL, Inc.