October 11, 2015

International Conference Registration Open
10/11/2015, 7:00 am – 7:00 pm, 7th Floor Registration

International Conference Opening Reception
10/11/2015, 5:00 pm – 7:30 pm, Salon 1&2

October 12, 2015

International Conference Registration Open
10/12/2015, 7:00 am – 4:30 pm, 7th Floor Registration

Breakfast
10/12/2015, 7:15 am – 8:15 am, Salon 3

Opening Keynote Address:
Vinton G. Cerf
Vice President and Chief Internet Evangelist, Google
10/12/2015, 8:15 am – 9:45 am, Salon 3

Exhibit Hall Open
10/12/2015, 9:45 am – 4:00 pm, Salon 1&2

Break in Exhibit Hall
9:45 am – 10:00 am, Salon 1&2

Breakout Sessions

Featured Speaker

Embracing and Securing the Internet of Things (IoT)

10/12/2015, 10:00 am - 10:45 am, Room Salon 3

Track: Infrastructure

Smarter, connected products offer an increasing amount of opportunities and capabilities that span across multiple boundaries. The IoT space is the new norm. The use of these smarter, connected products will force businesses to raise a new set of strategic choices related to how Information Security is integrated into these complex IoT ecosystems. Veteran CISO, Demetrios Lazarikos (Laz) will review how IoT has been adopted as the fastest disruptive technology in recent years, the Information Security considerations that come with it, and what can be expected for future integration.

Demetrios Lazarikos: Chief Information Security Officer, vArmour

The Value Proposition for Federated Digital Identity Services

10/12/2015, 10:00 am - 10:45 am, Room Kane/McHenry

Track: Mobile Security

Mobile devices are becoming the defacto method for marketing, retail, payments and social activities. However, as consumers hop from channel to channel, keeping their personal information both accessible and secure is a huge challenge. In this session, SecureKey SVP of Business Development, Stu Vaeth, will showcase the Government of Canada's award-winning implementation of a federated digital identity service and discuss how it is enabling Canadian consumers to simply and securely access government services, with the credential of their choice.

Stu Vaeth: Senior Vice President, Business Development, SecureKey

SELinux Integrity Instrumentation (SII)

10/12/2015, 10:00 am - 10:45 am, Room Lincolnshire 1&2

Track: Infrastructure

As a security reference monitor SELinux configuration integrity is critical. SELinux users battle complexity of the configuration and have few methods to verity its setup. There is a lack of methods to ensure SELinux configuration compliance. This doctorate dissertation research created a set of algorithms to monitor the configuration of SELinux and alert to changes. SII also offers the ability to see relationships between service and SELinux policies based on type/domain. The panel will cover the research and offer a live demo of the framework used during research.

Mike Libassi: Doctorate Student and Adjunct Professor and Sr. Performance Engineer, Colorado Technical University

Pathways to Empowered Security Leadership

10/12/2015, 10:00 am - 10:45 am, Room Northwestern/Ohio State

Track: Business Skills for the Information Security Professional

The evolving security leader can seamlessly blend technical knowledge with business acumen to serve as a trusted partner to the board and the business - but no one starts at the top. During this invaluable panel discussion, top CISOs and information security leaders will share personal stories about when and where their careers began, what pivotal events launched them into leadership, and what has empowered them to grow stronger in the field. Security professionals at any level of experience will benefit from hearing the advice, knowledge and personal challenges these leaders have faced on their pathways to empowered security leadership.

Moderator: Marci McCarthy: President & CEO, T.E.N.

Panelists:

Todd Fitzgerald: Global Director Information Security, Grant Thornton International, Ltd

Larry Lidz: CISO, CNA Insurance

Jeff Reich: CSO, Barricade

Richard Rushing: CISO, Motorola

Silver Bullet for Identifying Hacking and Information Theft in ERP Systems

10/12/2015, 10:00 am - 10:45 am, Room Purdue/Wisconsin

Track: Business Skills for the Information Security Professional

The modern hacker to ERP systems knows the current technologies and is well prepared for them. The only unbreakable method for identifying hacking attempts and information theft is monitoring users activity and identifying suspicious behavior. This session will focus on identifying irregular user activity from different angles, activity in multiple systems environments, static and dynamic controls over user activity and more. Real-life examples about identifying hackers and internal frauds using these methods will be shown.

Moshe Panzer: CEO, Xpandion

Sponsored Session

Malvertising, Drive-by Downloads, and Web Exploits: Stop Them All with Browser Isolation

10/12/2015, 10:00 am - 10:45 am, Room Michigan/Michigan State

Track: Infrastructure

All businesses rely on web applications, but connecting to the Internet introduces the risk of running untrustworthy code from servers outside your organization’s control. Effectively defending against web malware threats requires isolating web content in disposable virtual machines run on hardened appliances in your organization’s demilitarized zone. Isolation effectively shields your endpoints from web-based malware while allowing them to browse the web safely and protect your network.

Ben Strother: Director of Business Development, Spikes Security

Sponsored Session

Harnessing Innovation to Address Emerging Security Challenges

10/12/2015, 10:00 am - 10:45 am, Room Indiana/Iowa

Track: Incident Response

2015 is a year in Cyber Security like we have never seen before. The year is not even completed and we have seen numerous Cyber Attacks showing themselves in the form of Breaches, Denial of Service, Ransomware, and many more. These are just a few of the threats that keep many CISO's up at night. Crime Syndicates, Blackhats, and Amateurs are learning more every day. They say two types of companies exist in the United States: those that have been hacked and those who don't know they have been hacked. You know the Risks, now find out the solutions in this invigorating session made up of a panel of experts.

Moderator: Dr. Michael C. Redmond, PhD

Panelists:

Gautam Aggarwal: Chief Marketing Officer, Bay Dynamics

Sean Blenkhorn: Senior Director of Solutions Engineering, eSentire, Inc.

Jack Daniel: Strategist, Tenable Network Security, Inc.

Kevin Sapp: Vice President, Strategy, Pulse Secure

Featured Speaker

Information Security Needs a Reboot

10/12/2015, 11:00 am - 11:45 am, Room Salon 3

Track: Business Skills for the Information Security Professional

Breaches are increasing in both size and frequency but most Information Security team's means and methods remain unchanged. As financial and reputational losses continue to mount, Boards are demanding that the same rigor and discipline used in measuring their financial and business risks be applied to how cyber risk is evaluated. To achieve this, the existing Information Security paradigm must be broken. The profession's continued focus on tools and technology to protect complex organizations isn't and won't work. While a core function of an Information Security team will always be cyber response, the profession must pivot away from acting as the sole team that protects the enterprise to the team that evaluates risk and directs coordinated action from across the enterprise. This talk will discuss the changing role of the Information Security team and its leadership and introduce a formalized methodology to measure and communicate cyber risk. Attendees will come away with over 300 metrics, KPIs and KRIs to use in their organization and a framework to measure their gaps and successes. Once implemented, you'll be able to confidently answer the five key questions that Board level executives are asking:

- How do I know when the security program is working?
- Is my security program aligned to the organization's desired risk profile?
- Can I report to the Board our current risk posture and quantify potential impact of threats to the business?
- Is my organization more or less secure than last year?
- Am I spending the right amount of money?

Arlan McMillan: CISO – IT Security, Risk, and Compliance, United Airlines

Breakout Sessions

Cisco Annual Security Report

10/12/2015, 11:00 am - 11:45 am, Room Kane/McHenry

Track: Mobile Security

Discussion of the results of a study that Cisco does every year. 1700 customers in 9 different countries where followed and studied. The 2015 Cisco Annual Security Report is a look into the Attackers and the practices of the Defenders. This is an industry product agnostic presentation, no vendors products are discussed. If you want to take a look at the report check it out free here: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html?keycode=000657685

James Natoli: Systems Engineering Manager, Cisco Systems Inc.

Understanding & Defending Against Data Breaches, as part of a Custom Software Development Process

10/12/2015, 11:00 am - 11:45 am, Room Indiana/Iowa

Track: Application Security

Security incidents that lead to data breaches have been happening a lot, from the latest Anthem Blue Cross breach, to Target, to Home Depot, to breaches including the MongoHQ incident that lead to the BufferApp compromise. Waiting until a software project is complete and bolting security on through the use of security software or network security countermeasures is not effective enough. To have a chance to build a secure system, a team requires the active support of developers and for the organization to adopt a written information security policy that influences business model decisions and the requirements gathering process.

Frank S. Rietta, MSIS: Senior Developer, Rietta Inc.

Mainframe Security: A Practical Overview

10/12/2015, 11:00 am - 11:45 am, Room Lincolnshire 1&2

Track: Infrastructure

Whether you started on mainframes, still working with them, or have never seen a mainframe, this is a practical view into the security capabilities of todays z/OS systems. Mainframes started out in the glass house, and host much of the enterprises critical sensitive data, but they are not in the glass house anymore. They are just a node on a TCP/IP network and looks like any other server. But is it being protected like the other servers on the network? This is a survey of the ways z/OS mainframes are being protected today, and will include some demonstrations to illustrate some of the common security capabilities.

Joe Sturonas: Chief Technology Officer, PKWARE, Inc.

Patient Portal Security: Ensuring Security & Enhancing Patient Privacy

10/12/2015, 11:00 am - 11:45 am, Room Northwestern/Ohio State

Track: Laws and Regulations

The US national health IT strategy is calling for the deployment of patient portals and expanded patient engagement. This session is will introduce some application, network, and security operation best practices to ensure a secure and privacy preserving patient portal. The session will close with a discussion on Identity and access management recommendations for establishing a robust and secure patient enrollment process.

George Bailey: Senior Security Advisor, Purdue Healthcare Advisors

Making the Business Case for Information Security

10/12/2015, 11:00 am - 11:45 am, Room Purdue/Wisconsin

Track: Business Skills for the Information Security Professional

Often ill-equipped with outdated defenses, education is a prime target for cybercriminals. In fact, a recent cybersecurity threat report names Education as the sixth most targeted industry in the world. Between budget restraints, security policies, and often a misperception about the risk, higher ed security professionals and business executives undoubtedly face a significant challenge. Please join California State University CISO, William Perry, to learn how the California university system is protecting its most sensitive information against today's advanced cyber crime. Mr. Perry will share his security roadmap as it relates to several key elements of developing an effective strategy and business case.

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

Sponsored Session

The Fight Against Phishing: Defining Metrics That Matter

10/12/2015, 11:00 am - 11:45 am, Room Michigan/Michigan State

Track: Securing the End Users

Phishing and social engineering attacks are at the heart of most significant data breaches. Threats targeting the human layer continue to evolve beyond the obvious. In this session, explore how a risk-based approach applied at the human layer improves organizational resilience and user level resistance to these threats.

Mark Chapman: President and CEO, Phishline

CISO Panel Luncheon

10/12/2015, 12:00 pm – 1:30 pm, Salon 3

Seasoned CISOs and C-Level security professionals share their thoughts and insights on how to advance the culture of security in your company from the corner office and beyond.

Moderator: Tim Stanley: Risk Management Consultant, Cummins Inc.

Panelists:

Mary Ann Davidson: Chief Security Officer, Oracle Corporation

Joe Filer: Vice President, Chief Information Security Officer, Harland Clarke Holdings Corp.

Tim Rains: Chief Security Advisor, Microsoft Worldwide Cybersecurity Business Unit.

Dane Sanderson: Global Security Director, Trek Bicycle Corporation

Tim Virtue: Chief Information Security Officer, Texas.gov

Breakout Sessions

ISSA Women in Security SIG Presentation: TAP Into Your Potential

10/12/2015, 1:45 pm – 2:30 pm, Room O'Hare

Track: Business Skills for the Information Security Professional

"TAP into your potential" helps you create an effective roadmap that identifies your #1 goal, an action plan and a sustainable program to make your #1 goal a reality. You will understand the success factors that got you at your current level of mastery. You will then work on identifying your top 10 goals and prioritize your topmost goal. Subsequently, you will create an action plan for your topmost goal. Finally, you will create a program plan, complete with risk analysis/mitigation plans/back up action plans. The TAP workshop will train you to generate immense success in every endeavor.

Jyothi Charyulu: Senior Principal Application Architect, SABRE INC

Featured Speaker

It's Not a Cyberwar, It's a Lifestyle

10/12/2015, 1:45 pm - 2:30 pm, Room Salon 3

Track: Infrastructure

How much does security cost? Probably too much. The key to success in protection, defense and offense in the non-kinetic world is having the right people do the right thing. With the proliferation of attacks, breaches, disclosures and malware one could make the case that we are at war continuously. Rather, we need to view this as normal and adapt accordingly. Walking down the street does not engage you into a war on crime just as being online does not place you into cyberwar. The discussion during this session will point out opportunities to improve security by not training and hiring more security professionals. Contrary opinions are welcome.

Jeff Reich: Chief Security Officer, Barricade

Preparing for the Big One

10/12/2015, 1:45 pm - 2:30 pm, Room Lincolnshire 1&2

Track: Incident Response

The Board Room cannot wait for the Big One. From the Securities and Exchange Commission to the American Bar Association to the White House, regulatory and oversight bodies are foreshadowing the liability event. CxO, Board Members, shareholders, and Insurance companies are going to feel the punch as negligence suits become the norm. Preparing for a major privacy data breach requires a Board level approach to coordination across General Council, CISO, finance, HR, IT operations, and partners. The session will focus on a 5 step process for developing an effective Executive Cybersecurity Program that demonstrates due diligence.

David Phillips: Managing Director, Cybersecurity Consulting, Berkeley Research Group

Cybersecurity Due Dilligence of a Vendor: Legal Requirements and Beyond

10/12/2015, 1:45 pm - 2:30 pm, Room Northwestern/Ohio State

Track: Laws and Regulations

The objective of this panel discussion is to review the legal requirements that form the foundation of an entity's compliant cybersecurity vendor due diligence model, understand why exceeding the legal requirements can cause legal liability, appreciate the value of certain vendor contract terms including insurance requirements, and discuss challenges with static versus ongoing due diligence activities. The conversation will look at these issues in all industries, but will include particular focus on highly regulated industries, including healthcare.

Marilyn Hanzal: Associate General Counsel, University of Chicago Medical Center

Rich Skinner: Executive Advisor, S3 Venture Group

Why Traditional Perimeter Security Approaches Leave your APIs Exposed to Threats

10/12/2015, 1:45 pm – 2:30 pm, Room Indiana/Iowa

Track: Application Security

More and more enterprises today are doing business by opening up their data and applications through APIs. Though forward-thinking and strategic, exposing APIs also increases the surface area for potential attack by hackers. To benefit from APIs while staying secure, enterprises and security architects need to continue to develop a deep understanding about API security and how it differs from traditional web application security or mobile application security.

Sachin Agarwal: Vice President, Product Marketing and Strategy, Akana

Striking the Right Balance Between Security and User Enablement in Cloud Platforms

10/12/2015, 1:45 pm – 2:30 pm, Room Purdue/Wisconsin

Track: Securing the End Users

With the consumerization of IT, employees are self-selecting and enabling third-party apps independently, blurring the lines between sanctioned and unsanctioned IT. The security concerns are understandable, however, many of these apps offer compelling productivity and efficiency-enhancing benefits. When companies deny access to certain applications, they get between their employees and how they want to work. In organizations where this is the case, it is clear that companies and policies are not keeping pace with technology adoption and are failing their workers. This session will reveal how organizations can strike the right balance between security and user enablement in cloud platforms.

Ron Zalkind: CTO and Co Founder, CloudLock

"Architecting" Your InfoSecurity/Cybersecurity Organization, Teams, and Careers

10/12/2015, 1:45 pm – 2:30 pm, Room Kane/McHenry

Track: Business Skills for the Information Security Professional

The role Information technology as an engine of enterprise innovation and competitiveness has caught many IT leaders and professionals unprepared. That's because for years they've been slow to address persistent human capital problems ranging from IT skill deficits, hiring/retention issues and pay inequalities to murky promotion paths and ineffective professional development programs. With information security and cybersecurity threats stunning the industry on a regular basis, the pressure to fix longstanding 'people problems' associated with securing the enterprise is enormous.

Coming to the rescue: applying traditional architecture principles to infosec/cybersecurity human capital and workforce management. Known as 'people architecture', it is now the most dominant strategy for executing mission-critical IT-business initiatives effectively and predictably. In this session industry analyst David Foote will define the pillars of infosec/cybersecurity people architecture, describe people architecture components, and reveal who's doing it and how they're doing it.

David Foote: Co-Founder, Chief Analyst and Chief Research Officer, Foote Partners LLC

Sponsored Session

The New Security Stack – 2015–2020

10/12/2015, 1:45 pm – 2:30 pm, Room Michigan/Michigan State

Track: Incident Response

What does it mean when we say 'the perimeter is dead?' We know that we now live in a world with myriad devices with wi-fi and cellular connections, employees working outside the office, and applications and data moving to the cloud. It's a brand new IT landscape, with a boundless surface to protect from entirely new threats, in a world filled with more sophisticated attackers. What are we going to do? What should the new security stack look like? Let's talk about how to re-establish the benefits of a secure network perimeter in a world where one no longer exists. Join this session and learn how to: - Extend threat protection from your existing security stack, beyond the traditional network perimeter - Leverage how the Internet already works to enforce always-on security and gain global visibility into emerging threats - Watch as attacks are staged by observing changes in the Internet's infrastructure.

James Brown: Product Manager, OpenDNS

Break in Exhibit Hall

2:30 pm – 3:00 pm, Salon 1&2

Breakout Sessions

The Permissions Gap

10/12/2015, 3:00 pm - 3:45 pm, Room Indiana/Iowa

Track: Infrastructure

In this presentation, Lee Mangold will discuss how excessive permissions in operating system and application architectures have been the primary contributing factor in the majority of data breaches. Lee will show how best practices are not filling this "permissions gap" and offers actionable discovery and remediation techniques.

Lee V. Mangold: Managing Security Engineer, GuidePoint Security

InfoSec in the Hot Seat: How to Accomplish Breach Response Readiness

10/12/2015, 3:00 pm - 3:45 pm, Room Lincolnshire 1&2

Track: Incident Response

In many organizations, executive management has off-loaded preparedness for data breach response to the CISO. But the subset of security incidents that are significant data breaches will require coordinated execution of 10 interrelated activity channels: Security, Legal, Forensic, Law Enforcement, Regulatory, Insurance Coverage, Public Relations, Stakeholders, Notifications, and Personnel Management. IT Security response preparedness is necessary, but not sufficient. Many of these activities may be beyond the CISO's reach, creating a dangerous mismatch of authority vs. accountability. This session will explore how CISOs can help their organizations move beyond incident preparedness to effective breach response readiness.

Peter Sloan: Partner, Husch Blackwell LLP

Rob Rudloff: Partner, RubinBrown LLP

Preventing, Insuring and Surviving Fund Transfer Fraud

10/12/2015, 3:00 pm - 3:45 pm, Room Northwestern/Ohio State

Track: Laws and Regulations

It usually isn't sexy from a technical perspective, but more and more businesses are feeling the effects of fund transfer fraud. Whether it is a spear phishing attack, social engineering, or malware specifically tailored to obtain online banking credentials, hundreds of thousands of dollars are at risk to these attacks. If your business is not prepared for and properly insured against these items, you could be left holding the bag. Overseas organized crime is using increasingly sophisticated methods to gain temporary control of commercial accounts and to initiate fraudulent wire transfers. Over the past year, new fraud techniques have proven increasingly effective and US companies are becoming victim to these attacks at an alarming rate.

Nick Merker, CISSP, CIPT: Attorney, Ice Miller LLP

Nick Reuhs: Attorney, Ice Miller LLP

Stephen Reynolds, CIPP/US: Partner, Ice Miller LLP

Diversified IT: Why the Security Workforce Needs Qualified Women...and Men

10/12/2015, 3:00 pm - 3:45 pm, Room Kane/McHenry

Track: Business Skills for the Information Security Professional

There's long been a need for more diverse slate of candidates in information technology but lately the need is growing much stronger for simply finding qualified security professionals - men and women alike - to enter the workforce and grow long and rewarding careers in cyber security. A recent 2015 Frost & Sullivan report said that the global workforce shortage of security professionals will reach 1.5 million within five years and the need for a wider skill set and strong communications skills has never been greater. So how do we build the next generation of cyber warriors and also ensure that more females get interested at an early age in joining the workforce? This presentation will discuss first-hand lessons learned from Tammy Moskites, Venafi's CIO/CISO, who has enjoyed a 30-year career span in IT and security. Tammy will discuss the challenges of entering the workforce as a woman and how she's built and grown her career over the years. She'll also discuss how she's built and mentored great teams and where she sees the need for skills to evolve as the threatscape has changed.

Tammy Moskites: CIO and CISO, Venafi

Security & the Internet of Things

10/12/2015, 3:00 pm - 3:45 pm, Room Purdue/Wisconsin

Track: Securing the End Users

Wearables. Smart homes. Connected cars. As technology becomes more pervasive, attackers are growing more sophisticated, cyberespionage is becoming a real-world concern, and breaches are skyrocketing. For security professionals, the challenge of contending with shadow IT while still finding the time to stay abreast of external threats can feel like a “perfect storm” designed to derail security programs. In this talk, Nick Percoco will: 1. Address how the Internet of Things impacts security, 2. Forecast where the industry will go in 5, 10, and 15 years, 3. Provide a roadmap for how organizations can position their security program for success amidst an uncertain future.

Nich Percoco: Vice President, Strategic Services, Rapid7

Sponsored Session

House of Lies

10/12/2015, 3:00 pm - 3:45 pm, Room Michigan/Michigan State

Track: Incident Response

Social engineering tactics from attackers are not new, and have been used for decades. Social engineering attacks have had some of the most devastating consequences in the most recent data breaches. Their scope goes beyond phishing links and fake profiles. Modern social engineering tactics have been used to stage complex modern attacks. This talk will look case studies for modern data breaches, and in-depth look at the social engineering tactics that were, and examine how complex attacks were launched and bypassed traditional cyber security defensive devices. Lastly, we will conclude examining what these organizations could have done to mitigate these attacks and how they could have protected themselves. We will look at policies, procedures, and next-generation security devices that nay help combat this risk.

Aamir Lakhani: Senior Security Strategist, Fortinet

Sponsor Prize Drawings

10/12/2015, 3:45 pm – 4:00 pm, Salon 1&2

Cyber Defense Center

Bomgar

10/12/2015, 4:00 pm – 5:00pm, Room Indiana/Iowa

CLOSE THE DOOR TO CYBER-ATTACKS WITH SECURE VENDOR ACCESS

This session will feature:

•LIVE! Cyber Attack & Defense. Watch a cyber-attack unfold live to show you how your vendors can unwittingly leave the door open to your network and understand how to prevent these by managing, controlling and auditing all vendor access

•Best practice recommendations on how to secure vendor access to your organization. Hear top tips to protect your company and customer data, infrastructure and assets from cyber-attacks by securing vendor access while improving productivity.

Microsoft

10/12/2015, 4:00 pm – 5:00pm, Room Lincolnshire 1&2

Exploitation Trends: From Potential Risk to Actual Risk. Microsoft researchers have studied some of the exploits discovered over the past several years and the vulnerabilities they targeted. Understanding which vulnerabilities get exploited, who exploits them, the timing of exploitation, and the root causes, all help security professionals more accurately assess risk. Development practices that help minimize vulnerabilities will be discussed.

Spikes Security

10/12/2015, 4:00 pm – 5:00pm, Room Northwestern/Ohio State

All businesses are now reliant on web applications. But how can you protect your organization from web malware when browsers are connected directly to the Internet and can run untrusted code from servers outside your control? This interactive session will cover how isolation technology can prevent browser-borne malware from entering your corporate network and infecting endpoint devices. You're invited to learn the basics of isolation technology:

- How it's implemented outside your network
- How it prevents users from connecting directly to the Internet
- How it's different from detection-based technology

Venafi

10/12/2015, 4:00 pm – 5:00pm, Room Michigan/Michigan State

Evolving Public Key Infrastructure: Critical updates needed to keep up with our changing world Several industry trends are forcing organizations to take a strong look at their PKI. Factors such as the need to encrypt more data, the expanding network perimeter, the viewpoint that digital keys should be rotated more frequently and unplanned events such as Heart Bleed all put significant pressure on an organization to modernize their PKI environment to keep pace with change. This one hour workshop will walk through the history of PKI, why it is long overdue for a comprehensive upgrade and the factors that are driving this sea change within our industry. Topics such as automated lifecycle management, security controls and policy considerations, centralization strategies and enterprise adoption will be addressed. Participants will take away a broader awareness of the challenges they face as well as actionable strategies that can be used for subsequent planning steps within their own organization

Chicago Welcome Reception: Party in the Sky
10/12/2015, 6:00 pm – 9:00 pm
360° Chicago
875 N Michigan Avenue, 94th Floor
Work hard, play hard. Party with the stars in the sky and the stars of cybersecurity in the 360 Chicago Observatory. This premier networking event is sponsored by 360° Diamond Sponsor BOMGAR. Take advantage of ISSA's private use of 360° Chicago's 30-degree, all-glass, tilt-out stations for a new angle on Chicago and the Magnificent Mile!

October 13, 2015

International Conference Registration Open
10/13/2015, 7:00 am – 12:00 pm, 7th Floor Registration

Women in Security Breakfast: Networking For Success
10/13/2015, 7:30 am – 8:30 am, Room Kane/McHenry
Join us for a WIS SIG breakfast filled with cybersecurity fun-facts, networking opportunities, and plenty of ways to earn some great SWAG. Interact with peers and women luminaries in the field whom are working to bring information, opportunity, and success to each of you. Celebrate with and recognize those leaders whom have made the past five years of WIS SIG possible.
Breakfast
10/13/2015, 8:00 am – 9:00 am, Salon 3

Keynote Address:
Dan Geer
CISO, In-Q-Tel
10/13/2015, 9:00 am – 10:00 am, Salon 3

Exhibit Hall Open
10/13/2015, 10:00 am – 2:00 pm, Salon 1&2

Break in Exhibit Hall
10:00 am – 10:15 am, Salon 1&2

Breakout Sessions

Featured Speaker
The Cyber Threatscape & the Need for Public/Private Partnership
10/13/2015, 10:15 am – 11:00 am, Room Salon 3
AD Trainor will identify the five main cybersecurity threats and provide current examples of the threat and how the FBI is working with the private sector to identify, pursue, and defeat these threats.
AD James C. Trainor, Jr.: Assistant Director, Cyber Division, FBI

ISSA Women in Security SIG Presentation: Looking to 2020 -- Are we too late?

10/13/2015, 10:15 am – 11:00 am, Room O'Hare

Track: Incident Response

Everyday, we work to protect our companies, organizations, government from the information security threats around us. Our focus is on controls, educating our associates, determining how best to fund our efforts, engaging our senior leadership, and keeping our organizations' names off Krebs Online. That said, we somehow are missing the big picture related to where we, as a nation, are in terms of protecting ourselves. The public sector and private sector are starting to work together, but there are so many constraints that even this leaves much to be desired. In this presentation, the presenter applies the often used Capability Maturity Model to our nation to see how secure we are as a nation and then presents ideas for how to think strategically in order to move our nation forward over the next several years. Her current assessment is that we are somewhere in the "ad hoc to repeatable" phase and that to effectively address global information security threats over the coming years, our nation will need to define a multi-tier integrated approach. This approach will be discussed during the session.

Jill Rhodes: Vice President and Chief Information Security Officer, Trustmark Companies

The Future of Mobile App Security

10/13/2015, 10:15 am – 11:00 am, Room Kane/McHenry

Track: Mobile Security

Do you know what your mobile app is doing? Are you relying on app markets to protect you? Today's mobile apps are riddled with defects that hackers can exploit. Vincent Sritapan, a Cyber Security Division Program Manager at the Department of Homeland Security S&T, will discuss ongoing research for securing mobile technology. He will present a current projects in mobile app archiving that can continuously inventories apps from mobile app markets like iTunes, Google Play, Windows Phone Store, and includes over 83 global app marketplaces. He will discuss the future of mobile app security and where R&D is taking us.

Vincent Sritapan: Program Manager for Mobile Security R&D, Department of Homeland Security, S&T – Cyber Security Division

Practical Application Security for the Real World

10/13/2015, 10:15 am – 11:00 am, Room Indiana/Iowa

Track: Application Security

Web applications are undoubtedly our future for interacting with businesses and data. Companies trust their data and reputations with applications, which most times provide internet accessible avenues inside the firewall. This presentation will demonstrate web based attacks through live demos and touch upon mitigation strategies. Tools for application testing will be discussed and tested against our vulnerable application. Further, we will discuss the effort needed to fix these vulnerabilities; as a security professional, you will be able to give the proper fixes and understand the level of effort needed by developers.

Andrew Leeth: Product Security Engineer, Salesforce

N-Gram Analysis in Suspect Author Identification of Anonymous Email

10/13/2015, 10:15 am – 11:00 am, Room Lincolnshire 1&2

Track: Incident Response

In late 2010, a Fortune 100 company's executives were being threatened via anonymous email. Multiple anonymous remailers prevented standard IP tracing techniques. eVestigations Inc. developed a system and protocol utilizing current linguistic techniques to successfully identify the perpetrator. Empirical authorship analysis has a long history, primarily as it relates to literary works of unknown or disputed authors. One such technique known as N-Gram Analysis has shown promise in identifying the most likely author of known texts when presented with candidate authors having predefined text samples of undisputed authorship.

Paul Herrmann, CISSP, EnCE, CISA, CPP: President, eVestigations Inc.

Embedded Like a Tick - Cyber Intelligence

10/13/2015, 10:15 am – 11:00 am, Room Northwestern/Ohio State

Track: Laws and Regulations

Most intelligence collection in IT shops and in particular are driven exclusively by technology and technical information. This provides only a fraction of the necessary data, information and potential actionable intelligence needed. Creating online personas helps round out the collection efforts and serves to establish a beach head in target communities of interest. Know your adversary as they know you gathering information about their intent before execution of that intent.

Jeff Bardin: Chief Intel Officer, Treadstone 71

Data Classification – Discovery and Response Prioritization

10/13/2015, 10:15 am – 11:00 am, Room Purdue/Wisconsin

Track: Securing the End Users

ata Classification and Secure handling is something companies desire to do. It is hard work and requires a cohesive approach. This presentation will demonstrate how a company can attach the topic. It shares the methodology for how sensitive data sets can be identified, risk qualified and quantified. Through use of this model measurements can be made on risk and progress towards remediating the risk issues a company faces. Lastly, through measurement and reporting senior management can be made aware of data risks and progress towards improving the secure handling of sensitive data.

Tim Plona: Business Solution Architect, Freeport-McMoRan

Breakout Sessions

Sponsored Session

Build an Adaptive Awareness Program Based on NIST's Cybersecurity Framework

10/13/2015, 11:15 am – 12:00 pm, Room Michican/Michigan State

Track: Securing the End Users

NIST's Cybersecurity Framework describes a Tier 4: Adaptive program as one that uses "a process of continuous improvement incorporating advanced cybersecurity technologies and practices … to respond to evolving and sophisticated threats in a timely manner." The question is, how do you bring this kind of sophistication to your Security Awareness program? In this presentation, we'll discuss the range of options you have to plan, measure, train, analyze, and continually adapt your program to shifting risks. You'll come away armed with options for raising the bar on your end user awareness efforts.

Tom Pendergast: Director of Awareness Solutions, Instructional Design Manager, MediaPro

Steven Conrad: Managing Director, MediaPro

Applied Privacy Engineering: User-Controlled, User-Monetized Mobile Advertising

10/13/2015, 11:15 am – 12:00 pm, Room Kane/McHenry

Track: Mobile Security

Observation: primitive data objects cannot protect or govern self. CYVA Research has designed a self-protecting, self-governing mobile object, a Self-Determining Digital Persona that enforces privacy and empowers the right of persons to be secure in their human-digital existence. These technologies are being built in accordance with our guiding architecture principles: human-digital dignity and human-digital integrity. We all should respect human-digital dignity and the right of informational self-determination, the right of people to control their personal information wherever they exist. Human-digital integrity: never separate a person's data from their policies, and the capability for them to enforce governance over the use of their human-digital identity wherever they exist.

Kevin O'Neil: CISSP, CYVA Research Corporation

Medical Device Safety and Security (MeDSS): Assessing and Managing Product Security Risk

10/13/2015, 11:15 am – 12:00 pm, Room Indiana/Iowa

Track: Application Security

The US Food and Drug Administration (FDA) have recently signaled a significant shift in a paradigm that is relevant for many stakeholders in the networked medical device arena by pointing out that as medical devices are increasingly interconnected via the Internet, hospital networks, other medical devices, smartphones, electronic health records and 3rd party cloud solutions there is an increased risk of cyber security attacks. Such an attack could affect how a medical device operates and ultimately endanger human health or worse, human life. In fact, networked medical devices are part of the Internet of Things (IoT). This session will explore the cyber security risks related to networked medical devices including the types of vulnerabilities currently observed in both "wired" and "wireless" medical devices in hospitals and large health systems. This session will also highlight Deloitte's framework to addressing the evolving recommended practices and standards for assessing, designing, testing, and manufacturing more secure networked medical devices.

John Lu: Principal, Cyber Risk Services, Life Sciences and Healthcare industry, Deloitte & Touche LLP

Muhammad Kashif: Manager, Cyber Risk Services, Life Sciences and Healthcare industry, Deloitte & Touche LLP

Taking Control of 'Control': Addressing Cybersecurity in Industrial Control Systems

10/13/2015, 11:15 am – 12:00 pm, Room Lincolnshire 1&2

Track: Infrastructure

Industrial Control Systems (ICS) have become something of a third rail in cybersecurity circles. Managing everything from light dimmers to elevators to the electricity we all rely upon, ICS automates many aspects of our everyday physical environments, but its historically insecure architecture represents growing and significant security risk that is difficult to manage using traditional security approaches. Even worse, it has become a nearly irresistible target for those seeking to wreak havoc by jumping the gap from information disruption to real world destruction. This presentation highlights how the failures to secure ICS are presenting real threats to everyday business operations. More importantly, however, this presentation attempts to present a series of ideas for real change to combat these threats, ideas that can be used by security professionals in their respective environments to start fixing the more immediate problems, mitigate the current and near future risks, and provide leadership to effect change into the future.

Daniel Ziesmer: ISSO, Bechtel Corporation

Stake Your Reputation on your Cyber Security Incident Response Program CSIRT

10/13/2015, 11:15 am – 12:00 pm, Room Northwestern/Ohio State

Track: Incident Response

Learn Best Practices for CSIRT Programs, Plans, Playbooks and Testing, Cyber Security Incident Response Program is a must for any organization using the Internet. It must be robust yet flexible. Unfortunately in spite of all of the Cyber Events, many companies are taking a long time to respond. Teams must be trained and have written procedures. Time is critical in responding to an incident. Every incident costs the organization, money and reputation.

Dr. Michael C. Redmond: CEO and Lead Consultant, Redmond Worldwide

How to be a highly effective CISO - Top 10 Performance Success Factors!

10/13/2015, 11:15 am – 12:00 pm, Room Purdue/Wisconsin

Track: Business Skills for the Information Security Professional

Join Brian Schultz, who has served as an advisor to many CISOs, for a CISO panel discussion to explore the Top 10 Performance Success Factors of highly effective CISOs. Topics will include: identifying your adversaries, mark your enterprise crown jewels, optimize security posture based on ROI, performance beyond compliance, meaningful benchmarking in your industry, dealing with inappropriate reporting structures, effective C-Suite and board room communications, recruiting and retaining exceptional talent, building and maintaining a collaborative CISO mentor network and contribute industry thought leadership.

Brian Schultz, CISSP, ISSMP, ISSAP, CISM, CISA: Technical Director, Cyber Architecture and Advisory Services, Battelle

Bob Bigman: President, 2BSecure

Dave Cullinane: Co-founder, TruSTAR

Cyber Security Liability Insurance: Need It or Leave It

10/13/2015, 11:15 am – 12:00 pm, Room O'Hare

Track: Laws and Regulations

This session will feature three speakers' perspectives on a new type of insurance, cyber-insurance. It will cover what cyber-insurance is, how organizations are using it and how it can be used in an organization's IT security/ risk program including how it plays a role in a sound data governance model. Attendees will also learn what they need to know in evaluating different cyber-insurance options, whether it makes sense for your their company, and how to present your their information security program to the cyber-insurance market.

Moderator: Andrea Hoy: President, ISSA

Panelists:

Ronald Raether: Partner, Troutman Sanders

Brian Thornton: President, ProWriters

Sponsored Session

Intelligent Risk in a House Without Walls

10/13/2015, 11:15 am – 12:00 pm, Room Michigan/Michigan State

Track: Threats & Responses

Modern corporate security professionals inhabit a house without walls; one that must remain secure as the penalties for failure grow steeper by the day. In a corporation comprised of complicated supply chains, global partnerships, and a revolving door of personnel and sales professionals requesting greater insight and connectivity for their customers, where does your company end and the market begin? Roll up your sleeves and participate in a lively discussion as we conquer fears, bucket uncertainty, and replace doubt with risk remediation. Symantec's risk assessment champion, Ryan DuPre, will discuss an evolving approach to assess and mitigate strategic and tactical risk in this global environment of unknown vulnerabilities, shifting geopolitics and highly resourced threats. Learn a methodology for ranking critical threats, communicating meaningful guidance to the Board of Directors, and fixing vulnerabilities with limited resources. Leveraging over a decade and a half of defense and intelligence experience, Ryan will provide a framework for risk assessment and remediation.

Ryan DuPre: Symantec

Awards Luncheon

10/13/2015, 12:00 pm – 1:30 pm, Salon 3

ISSA annually recognizes outstanding information security professionals, their companies, and chapters that are at the top of their respective games. Help us honor some of the best and brightest security leaders in the industry at our awards recognition luncheon and ceremony.

Sponsor Prize Drawings

10/13/2015, 1:30 pm – 1:45 pm, Salon 1&2

Breakout Sessions

Featured Speaker

2015 Verizon Data Breach Investigation Report

10/13/2015, 1:45 pm - 2:30 pm, Room Salon 3

Track: Incident Response

The 2015 Data Breach Investigations Report (DBIR) is out, and marks the eighth consecutive year that Verizon has published this highly regarded report. The 2015 DBIR provides a detailed analysis of almost 80,000 incidents, including 2,122 confirmed data breaches. The key findings in the report are:

- The methods of attack are becoming increasingly sophisticated - often involving a combination of phishing, hacking, or malware.
- We found that in the last year, 23% of recipients opened phishing messages and 11% clicked on attachments.
- Nine patterns still cover the vast majority of incidents (96%) of the breaches in this year's dataset.
- We found that company size has no effect on the cost of a breach.

Dave Ostertag: Global Investigations Manager, Risk Team, Verizon

Security or Convenience? Enabling a Collaborative Work Environment

10/13/2015, 1:45 pm - 2:30 pm, Room Kane/McHenry

Track: Application Security

We live in a highly connected world and we have become dependent upon the convenience of email, the cloud and other collaboration tools, but in this effort to increase productivity, security has been compromised. However, organizations do not need to choose between security and convenience. In this presentation, Dr. Guy Bunker will explore the full scope of vulnerabilities presented by email and collaboration tools, as well as new information bourn threats, critical information hidden in metadata and document revision history, and Advanced Persistent Threats (APTs) within active content. Dr. Bunker will share how to enable a collaboration without compromising security.

Guy Bunker: Senior Vice President of Products, Clearswift

Let's Hack a House

10/13/2015, 1:45 pm - 2:30 pm, Room Lincolnshire 1&2

Track: Infrastructure

When we bring cameras, automation controllers and other “Internet of Things” devices into lives, what risks do they bring with them? You may see a camera, but an adversary sees a feature-rich platform to attack your network infrastructure. In this session we'll provide an introduction to device hacking with no engineering background required.

Tony Gambacorta: Vice President, Operations, Synack

Current Trends and Our Methods for Defense

10/13/2015, 1:45 pm - 2:30 pm, Room Northwestern/Ohio State

Track: Laws and Regulations

In the past several years a growing list of computer breaches have scarred numerous US entities from financial industries, health care providers, and the entertainment industry. Adam Keown will provide direct experience about the impact of these breaches from his time in the FBI and more recently as a private consultant at TEKsystems. He will discuss attackers methods of attack, defensive measures for reducing risk, and briefly look into a crystal ball.

Adam Keown: Security Consultant / Solutions Architect, TEKsytems

Computer Security for SMB/Gov’t

10/13/2015, 1:45 pm - 2:30 pm, Room Purdue/Wisconsin

Track: Securing the End Users

What makes an effective information security program for a small organization? This educational presentation is intended to promote:

- Awareness of the importance of need for IT security
- Understanding of IT security vulnerabilities and corrective measures

Marv Stein: Sr. Security Consultant, TDAmeritrade

Sponsored Session

Preventing the Inevitable - Safeguarding Critical Assets in the Age of the Mega-Breach

10/13/2015, 1:45 pm - 2:30 pm, Room Michigan/Michigan State

Track: Business Skills for the Information Security Professional

Data security is top-of-mind for organizations, from board members to front-line employees, and their customers. Organizations are on guard, and rightly so – 2014 was an unprecedented year. Are data breaches now ubiquitous, a virtual certainty? Join InteliSecure's President and CEO, Robert Eggebrecht, as he discusses how to build a Critical Asset Protection Program (CAPP) that prevents data loss and protects critical assets.

Highlights include:

- Prioritizing your organization's crown jewels based on revenue, income, reputation and core operational impact
- Aligning your security risk and the corresponding plan
- Recognizing and responding to external and internal threats

Robert Eggebrecht: Co-Founder, President, and Chief Executive Officer, InteliSecure

Sponsored Session

Information Security Beyond Tools and Toys: How Do We Advance the Culture Side of It?

10/13/2015, 1:45 pm - 2:30 pm, Room Indiana/Iowa

Track: Securing the End Users

Companies spend a big chunk of the IT budget in security tool's testing, deployment and maintenance. Mature companies realized (early on) the importance of processes and methodologies around these tools. What companies and the industry as a whole is still struggling with is advancing the institutional culture i.e. the attitude of employees, clients, suppliers and partners. This session will share some organizational initiatives (global) to overcome the flat learning curve. Together will explore:

- How initiatives were designed
- Rolled out
- Who paid for those?
- How the effectiveness of these programs are measured?

Moderator: Sali Osman: Chairperson, Mentor-Protégé Committee, International Consortium of Minority Cybersecurity Professionals

Panelists:

Stephen Cobb: Sr. Security Researcher: ESET North America

Tyler Cohen Wood: Cyber Security Advisor, Inspired eLearning

Jamison Utter: Senior Consulting Engineer, Security, Infoblox

Breakout Sessions

ISSA Cybersecurity Career Lifecyle Program Sessions

10/13/2015, 3:00 pm – 3:45 pm

Pre-Professional: Lincolnshire 1&2
Entry Level: Indiana/Iowa
Mid Career: Northwestern/Ohio State
Senior Level: Kane/McHenry
Security Leader: Purdue/Wisconsin

Sponsored Session

Securing our Future: Lessons From the Human Immune System

10/13/2015, 3:00 pm – 3:45 pm, Room Michigan/Michigan State

Track: Incident Response

All signs point to a future world of more complex, harder to detect cyber threats. Our adversaries are exploiting what seems to be our strengths. Intel predicts the next big hacker marketplace to be in the sale of digital certificates ¬ already selling for more than $1000 each on Russian marketplaces. Gartner expects 50% of network attacks to use encrypted SSL/TLS in less than 2 years. What's to do? The human immune system has evolved to defend and destroy complex and oftentimes overwhelming attacks. What can we learn from it? How can we create a future that's more resistant as we use more software, more clouds, more apps, and more connected devices.

Jeff Hudson: CEO, Venafi

Cyber Defense Center

Bomgar

10/13/2015, 4:00 pm – 5:00pm, Room Indiana/Iowa

CLOSE THE DOOR TO CYBER-ATTACKS WITH SECURE VENDOR ACCESS

This session will feature:

- LIVE! Cyber Attack & Defense. Watch a cyber-attack unfold live to show you how your vendors can unwittingly leave the door open to your network and understand how to prevent these by managing, controlling and auditing all vendor access
- Best practice recommendations on how to secure vendor access to your organization. Hear top tips to protect your company and customer data, infrastructure and assets from cyber-attacks by securing vendor access while improving productivity.

Microsoft

10/13/2015, 4:00 pm – 5:00pm, Room Lincolnshire 1&2

Moving to the cloud in a compliance-driven world. As cloud adoption skyrockets, you might find it complex to deploy innovative services while simultaneously trying to meet demanding compliance requirements. This is because many IT regulations and standards were not designed for the cloud, and frequently fail to address its unique qualities. In this session you will learn what it takes to deploy a Microsoft Azure cloud solution that addresses the requirements of regulatory standards such as ISO 27001 / 27018, FedRAMP, PCI, and HIPAA. The presentation will look at a shared responsibility model where deploying good security principals can facilitate a successful adoption of a cloud service, while meeting your compliance regulatory requirements. What you will learn:

- How Azure can help you meet global compliance requirements such as ISO 27001 / 27018, FedRAMP, PCI, and HIPAA
- How security controls such as at-rest data encryption, key management, virtual machine protection, logging and monitoring, anti-malware services, identity management, and access controls, can help protect your solution and advance your compliance posture.

Spikes Security

10/13/2015, 4:00 pm – 5:00pm, Room Northwestern/Ohio State

All businesses are now reliant on web applications. But how can you protect your organization from web malware when browsers are connected directly to the Internet and can run untrusted code from servers outside your control? This interactive session will cover how isolation technology can prevent browser-borne malware from entering your corporate network and infecting endpoint devices. You're invited to learn the basics of isolation technology:

- How it's implemented outside your network
- How it prevents users from connecting directly to the Internet
- How it's different from detection-based technology

Venafi

10/13/2015, 4:00 pm – 5:00pm, Room Michigan/Michigan State

Evolving Public Key Infrastructure: Critical updates needed to keep up with our changing world Several industry trends are forcing organizations to take a strong look at their PKI. Factors such as the need to encrypt more data, the expanding network perimeter, the viewpoint that digital keys should be rotated more frequently and unplanned events such as Heart Bleed all put significant pressure on an organization to modernize their PKI environment to keep pace with change. This one hour workshop will walk through the history of PKI, why it is long overdue for a comprehensive upgrade and the factors that are driving this sea change within our industry. Topics such as automated lifecycle management, security controls and policy considerations, centralization strategies and enterprise adoption will be addressed. Participants will take away a broader awareness of the challenges they face as well as actionable strategies that can be used for subsequent planning steps within their own organization