ISSA

Information Systems Security Association

Celebrating Cybersecurity • Driving Our Destiny

2014 ISSA International Conference Agenda

October 21, 2014

7:00 am - 5:00 pm: Registration Open
West Registration Area

8:00 am - 5:30 pm: Chapter Leaders Summit*
Nutcracker Ballroom

5:00 pm – 7:00 pm: ISSA International Conference Opening Reception
Fantasia Ballroom

October 22, 2014

7:00 am - 4:30 pm: Registration Open
West Registration Area

9:30 am - 5:00 pm: Exhibit Show Floor Open
Room Fantasia Ballroom

Keynote Address Necessary Skills for Cyber Security Professionals
10/22/14 8:30 am – 9:30 am Room Fantasia Ballroom
Admiral Michael S. Rogers: Commander, U.S. Cyber Command; Director, National Security Agency; Chief, Central Security

The Truth About Securing Networks and Systems

Featured Speaker

10/22/2014 10:20 am - 11:10 am Room Fantasia A&B

Why is it that after spending millions of dollars on various computer security technologies, the hackers still gets through? The ugly truth (that every sophisticated hacker knows) is that contemporary network, computer systems and application programming language contain inherent vulnerabilities that can never be ameliorated by only purchasing more technology and writing more policies. If you want to get ahead of the next exploit then you have to think differently about how to secure systems and data. This presentation discusses why systems are inherently insecure and how your next move should be fundamental network and system architecture changes vice buying more security technology.

Robert Bigman: CISO, Central Intelligence Agency (Retired)

Building the Next Generation of Cyber Defenders: Cross-Training Wounded Warriors to help Protect and Defend the Nation's Information Systems

Community Track

10/22/2014 10:20 am - 11:10 am Room Grand Republic C&D

Today's cyber attacks are continuing to become more technically astute and effective. Gone are the days of simple denial of service attacks targeting websites and other Internet-facing IT systems. Today's attacks are targeting the intellectual property and economic foundations of organizations in every industry, vertical and country. The theft of such information is a common occurrence as critical information systems are infiltrated through Internet connections and vital economic capital, critical technologies, and other forms of national wealth are being plundered. Real-life events demonstrate that those organizations that employ highly technical cyber security professionals in areas such as incident response, network defense, and penetration testing or forensics analysis are in the best position to identify, quarantine and remediate today's cyber threats. The differentiator is not just a device or appliance. There is a critical need for people who are able to use judgment and analysis at a deep technical level that can make the difference. The problem for our nation is this: we don't have enough people with the right mix of technical cyber security skills to adequately protect and defend all the information systems. The need is real. The supply of trained personnel is limited. Something needs to be done. This presentation will discuss an advanced training and assessment program currently in development by the Federal IT Security Institute to arm our wounded warriors with technical skills that supplement their existing dedication, patience, and devotion to duty, thereby strengthening national cyber defenses.

Jim Wiggins: Executive Director, FITSI - Federal IT Security Institute

Pushing the Envelope on Data-Driven Security Awareness

Securing the End Users Track (Sponsored Session)

10/22/2014 10:20 am - 11:10 am Room Fantasia C&D

This session explores established and cutting-edge methods to help you take your social engineering simulation and phishing mitigation programs to the next level. Models, case studies, and "stories from the trenches" will provide real-world examples of how information security teams are effectively driving positive change at the human layer. The presentation will cover the Attacker, Employee, and Training Perspectives and will help you align your human layer security initiatives with the entirety of your risk-based security program.

Mark Chapman: President, Phishline.com

Looking To Build A Secure Enterprise Mobile Application? Here's How!

Application Security Track

10/22/2014 10:20 am - 11:10 am Room Fantasia E&F

Mobile applications need to allow people convenient access, but also enable them to maintain organizational control, security and compliance. Additionally, a great mobile application should properly handle data remnants and harmoniously coexist with BYOD policies. In this session, attendees will learn the successful components for designing and building a mobile application for the enterprise, including features like support for multiple methods of authentication for different devices, and remote wipe capabilities. It will also teach attendees how to navigate through the use of native versus HTML APIs, security protocols and explain how to properly cover test an app for security purposes.

Mushegh Hakhinian: Chief Security Architect, Intralinks

The Many Facets of a Data Breach: Practical Case Studies for Incident Response, Remediation and Legal Disclosures.

Laws and Regulations Track

10/22/2014 10:20 am - 11:10 am Room Nutcracker 1

This presentation will provide practical examples, case summaries and actionable takeaways designed to assist the attendees with managing the legal, operational and technical issues resulting from a data breach and will include the following topics:

- Developing a data classification protocol to inventory critical network assets

- Network defense strategies to mitigate the theft of intellectual property and sensitive assets

- Current Attacker Tactics, Techniques and Procedures trends used to breach network defenses

- Tactical and Strategic remediation recommendations designed to remove the Attacker's and deny further access to the network

Jason Smolanoff: Vice President, Stroz Friedberg

Automating Threat Intelligence

Infrastructure Track

10/22/2014 11:30 am - 12:20 pm Room Grand Republic C&D

There is a lot of interest being generated in the security community around threat intelligence. Most solutions currently rely on manual consolidation of alerts into summary reports, and those that go beyond are built on proprietary frameworks. Through our presentation, we seek to answer the following questions: What is threat intelligence? How should cyber intelligence be classified and organized? How can organizations maximize automation when collecting, contextualizing, analyzing, and sharing threat intelligence? What is the proper balance to strike between automation and human-driven quality assurance? We will also discuss some of the prominent structured threat intelligence standardization language efforts.

Elvis Hovor: Research Analyst, Accenture Technology Labs
Shimon Modi: Research and Development Associate Manager, Accenture Technology Labs
Stephen Schall: Senior Analyst, Accenture Technology Labs

The Evolving Threat Landscape — Microsoft Security Intelligence Report

Threats and Responses Track (Sponsored Session)

10/22/2014 11:30 am – 12:20 pm Room Fantasia A&B

Threats have changed in dramatic and unexpected ways over the past year as attackers continue to hone and evolve their strategies and tactics, and Internet-connected devices proliferate. Using the latest data from billions of systems around the world, join Greg Lenti for this session where he will provide a unique perspective on the global threat landscape.

After completing this session, you will be able to:

- Understand the latest trends in security threats
- Examine the emerging online threats used by criminals today
- Identify best practices for securing networks, software and customers

Matthew Littleton: Microsoft

Threats & Response: Updates, Forensics, Law Enforcement, eDiscovery

Threats and Responses Track (Sponsored Session)

10/22/2014 11:30 am - 12:20 pm Room Fantasia C&D

Approximately four years ago, Trend Micro's Forward Threat Research (FTR) team began investigating the people behind SpyEye, which eventually helped lead to this historic arrest. The FTR team decided that by pursuing the cybercriminals themselves instead of just their servers, permanent damage could be done to the entire criminal underground. In this presentation, hear the back story of how SyeEye was taken down; understand how the team mapped out the infrastructure used to support the malware, identified weak points in that infrastructure, and pursued important leads, pointing to the identities of individuals behind this virus; and hear the details of how Trend Micro and other vendors worked with law enforcement in order to help them make the arrest. Attendees will learn best practices when partnering with law enforcement and government bodies which continues to prove effective in bringing cybercriminals to justice. Attendees will learn:

- Learn strategies for bringing public and private enterprises to the table to set objectives
- Hear best practices in working with law enforcement and government toward a common goal
- Understand why law enforcement and the security community need to work together to stop cybercrime as neither group, working alone, can protect users as effectively.

Jon Clay: Sr. Global Threat Communications Manager, Trend Micro

Developing a Defensible eDiscovery / Forensics Program for any Organization

Business Skills Track

10/22/2014 11:30 am - 12:20 pm Room Fantasia E&F

eDiscovery and Computer forensic capabilities are crucial in our litigious society. Is your organization prepared to produce data demanded by the court during litigation? Are you in a position to support your Legal Department's efforts to defend your organization? We will discuss options for archiving and retrieving email, accessing and protecting data properly from user's devices, as well as from company systems of record, and the plethora of other locations where data live. From a practitioner's viewpoint, see steps to take to move your organization into a defensible position before opposing counsel makes their requests and challenges your practices.

J. Michael Butler: Information Security Consultant, Black Knight Financial Services

Mobile Application Penetration Testing: Windows Phone 8

Laws and Regulations Track

10/22/2014 11:30 am - 12:20 pm Room Nutcracker 1

Believe it or not, Windows Phone 8 (WP8) is gaining popularity, which means we are the ones late on the bandwagon. There is some sporadic research and documentation on how to find and exploit vulnerabilities on WP8 but nothing concrete or centralized. This presentation will bring all that research as well as experience testing WP8 mobile apps together and provide a proven methodology for testing WP8 apps. The presentation will quickly introduce the audience to WP8 as an understanding of the platform is required to test an app that runs on it. We will then jump to how to test your favorite mobile app, find vulnerabilities, and exploit them. I will outline and demo step by step methods so the audience member can begin finding vulnerabilities as soon as they leave the presentation, no physical device required!

Jorge Orchilles: Vice President - Vulnerability Assessment Manager, Citi

The Biggest Risk You Face May be Yourself – Addressing Insider Risks

Securing the End User Track

10/22/2014 11:30 am - 12:20 pm Room Nutcracker 2

Although most of our resources and attention is focused on defending information and systems from external threats, many of the worst incidents involve those we work with. How do recent incidents inform how we should monitor and control risks from users, service providers and system administrators? This panel will look to legal and regulatory requirements and discuss possible ways to address insider risks.

James T. Shreve: Attorney, BuckleySandler LLP

Dr. Christopher Pierson: EVP, Chief Security Officer & Chief Compliance Officer, Viewpost

ISSA Awards Lunch

10/22/2014 12:20 pm – 2:10 pm: Room Fantasia Ballroom

Accounting for Humans Panel Discussion

10/22/2014 2:10 pm - 3pm Room Fantasia A&B

Moderator:

Samantha Manke: Executive Vice President, Secure Mentem

Panelists:

Amy Baker: Vice President of Marketing, Wombat Security

Robert Ivey: Chief Technology Officer, GCA Technology Services

Josh Larsen: CEO, Blackfin Security

Security is for Suckers

Laws and Regulations Track

10/22/2014 2:10 pm - 3pm Room Nutcracker 1

Description: In this session, Castle will discuss how cyber attacks have continued to evolve and what led to the Target breach. Attendees will learn how these past attacks are driving criminals in a new direction that will eventually result in a complete and total failure of the social security identification system. During this session, attendees will learn how vulnerable businesses are to the future of cyber attacks. In addition, Castle will discuss what organizations can and should be doing to prepare for future attacks, including how employees contribute to avoid being the next cyber breach news story.

Ryan Castle: Director of Product Management, TraceSecurity

Defense Wins Championships - Practices for Developing Effective Cyber Defense Professionals

Business Skills Track

10/22/2014 2:10 pm - 3pm Room Fantasia E&F

Offensive security classes and instruction, often referenced as Ethical Hacking or Penetration Testing, are popular both for current professionals as well as for students at both the college and university levels. While this may be successful in teaching how to attack systems it is less common to see effective teaching of intrusion detection and response techniques. Another challenge is conveying these concepts and practical techniques as attractive and interesting as those utilized by the "red team". This session will discuss how industry and academia can overcome these challenges and develop effective Cyber Defense professionals to meet the industry need.

Brad Wilkerson: Assistant Professor, Information Assurance, Eastern Michigan University

How to Fight an APT attack - Identifying and Responding to a visit from China

Infrastructure Track

10/22/2014 2:10 pm - 3pm Room Grand Republic C&D

This presentation is an actual case study of an advanced attack that originated from China and breached a client’s network. We will do a step-by-step review how the original malware was discovered, the different types of malware used, how we identified the extent of the breach, how the remediation was planned and how the malware was removed. We will discuss what went right and mistakes that were made during the process. We will also discuss the open source and commercial tools used during the detection and remediation process.

John Henderson: Security Analyst, Pondurance

Ron Pelletier: Partner, Pondurance

Jeff Foresman: Partner, Pondurance

Security in the Era of the Digital Polis

2:10 - 3:00 pm, Fantasia C&D

Whereas the analog polis clearly defines between public and private life, the Digital Polis merges public and private, personal and professional. Join us as we explore security processes aligned with the digital polis, including the intelligence cycle, information hierarchy, and their implications in organizations large and small; as well as novel models of access such as authorization-in-depth.

Christopher Adelman, Chief Security Ambassador, Eleven Paths, and Dir. Market Development - Security, Telefonica N. America

How To Make A Security Awareness Program… FAIL!

Featured Speaker
10/22/2014 3:40 pm - 4:30 pm Room Fantasia A&B
Are you ready for a wake-up call? How about two?

1. Security Awareness Programs are a valuable part of every company's security strategy.

2. Security Awareness Programs are abysmal failures and a waste of resources.

Which is it? After 30+ years in the information security business, Winn Schwartau has been involved in scores of controversial debates and held more than the occasional unpopular idea. In this exciting, provocative and interactive session, Winn will again move you from your comfort zone, and show you How to Make Security Awareness Program Fail. Epically. Fall flat on its face and become an abysmal failure while still wasting valuable resources.

- Since readability is not important, and graphics and multi-media use up valuable bandwidth, all awareness should be done in small font text.
- Make it unintelligible by hiring an English Major to run your security awareness messaging.
- Your CISO took a film class in college. Use his expertise.
- Never, ever, use casual language as it might improve communications.
- Humor has no place in the workplace.

And that is only the beginning. Learn other ways organizations can totally screw the pooch while trying to get:

- Users to behave with at least a modicum of common sense?
- Executives to follow the rules? Any rules at all?
- Geeks to stop making "totally secure, hidden back doors" to make maintenance easier?

No, Security Awareness Programs are not perfect and will NOT solve everything. But learning how to make one Fail is critical to understanding how to make one successful. So, what's on the other end of Schwartau's security awareness spectrum?
Hope. And a creative landscape of ideas, hints, techniques, tricks and tips he has used and seen used over the last 30 years – that work. That's don't suck.Stay tuned and do not miss his irreverent, but 'spot-on' analysis of security awareness – and how to design an affordable and effective program that addresses the real issue: the successful cohabitation of man and machine.
It can be done.
Winn Schwartau: Security, Privacy, Infowar, and Cyber-Terrorism Expert

Badges, Bombers and Barbarians: 7 New Tactics for Arming Corporate Citizens

Securing the End User Track

10/22/2014 3:40 pm - 4:30 pm Room Nutcracker 1

While some security pundits evangelize the failures of security awareness training and corporate budgets wasted on human security, the rest of us persevere, knowing that awareness is but one part of the security equation. And while glorious triumph may be unrealistic, success is achievable to those that are calculated, rhythmic and committed. But youâ€™re not going to get there with your grandfather’s awareness kit. Join us for a frank conversation on what’s working, what’s not, and 7 new tactics to make your awareness program more effective.

Reg Harnish: Chief Security Strategist, GreyCastle Security

Computer Forensics and Incident Response in the Cloud

Threats and Responses Track

10/22/2014 3:40 pm - 4:30 pm Room Grand Republic C&D

As most security professionals know, effective incident response plans include physical access to servers, and the ability to scan logs and pull data from deep packet forensic devices. When this happens in the cloud, the incident takes place on your cloud server where there is no physical access or forensic devices in place to track it and much less visibility into network activity. However, by partnering with a cloud provider security practitioners can often gain far more access to the data and expertise they need to assist their security team with the investigation of the breach than they expect. This session offers a blueprint of capabilities cloud providers should have in place to help conduct computer forensics and obtain actionable intelligence including mining logs, cloning the server and reverse engineering the malware. The session will cover practical steps to establishing contact with a cloud provider, developing a working relationship and maintaining realistic expectations before incidents occur, allowing the audience to act when time is of the essence. In addition, this session will offer examples of real-life investigations performed by cloud provider incident response teams, giving the audience a perspective on ways in which cloud providers deploy forensic resources and what capabilities they plan to develop in the future.

Stephen Coty: Director, Threat Research, Alert Logic

Death to Passwords - Changing the Nature of Online Authentication

Mobile Security Track

10/22/2014 3:40 pm - 4:30 pm Room Fantasia E&F

Historically, strong two factor hardware authentication has been too costly and complicated to scale to all businesses and the mass markets. To address this problem, a significant number of large scale online services and financial institutions have joined the FIDO Alliance open standards organization. The presentation will provide a brief history of FIDO standards and discuss how a FIDO enabled device, which has been successfully proven with thousands of users, enables one single and secure device to access any number of online, network or mobile services - with no drivers or client software needed.

John Haggard: Chief Business Officer, Yubico, Inc.

How to Hack a Bank - ISSA Financial SIG Presentation

SIG Meeting

10/22/2014 3:40 pm - 4:30 pm Room Nutcracker 2

This talk will show the top three vectors a team uses to successfully breach banking networks 63% of the time and gain domain administrator access. We will walk through each vector and show examples or technical demonstrations. The talk will focus heavily on showing an attack from the attacker's perspective. Be prepared to see some new methodologies for finding and attacking common vulnerabilities. Attendees will see successful attacks from the attacker's perspective, learn new penetration testing techniques, and better understand how to fight back.

Tom Schauer: CEO and Client Experience Officer, Trusted Advisory Group

Andy Robbins: Trusted Advisory Group

ISSA 30th Anniversary Dinner and Ceremony and Capture the Flag Event

10/22/2014 6:00 pm – 10:00 pm

Fantasia Ballroom

October 23, 2014

7:00 am - 4:30 pm: Registration Open
West Registration Area

ISSA Women in Security SIG Breakfast: Driving Our Destiny – Paying Homage to the Queen!

SIG Meeting
10/23/2014 7:30 am - 8:30 am Room Nutcracker 2
Join us for a networking breakfast highlighting 'Women's Voices' as we celebrate our roles within cybersecurity by sharing stories from the field. Learn how women are taking on greater leadership roles as cybersecurity becomes more and more integral to all levels of government, education, private enterprise, and nonprofit organizations. Network with women cybersecurity leaders from all around the world at this informative, enlivening, humorous, and tasty session.

Keynote Address Security Researcher, Security Besmircher: Security for Organizations in a world of bug bounties and random security researchers

10/23/14 8:30 am – 9:30 am Room Fantasia Ballroom
Kevin Johnson: CEO, Secure Ideas
From Weev to Microsoft's Bug Bounty, organizations have to understand how their organization deals with security in a world that appears to have gone mad. We used to know that an "attack" coming from the outside world was malicious. Now we have to determine if its just another "security researcher" and if we want to actually invite these people to test our systems.
In this talk, Kevin Johnson of Secure Ideas will explore the ideas behind bug bounties and security research. He will discuss ways that your organization can adjust and how to determine if this makes sense to you.

The Confluence of Data Security Challenges

Threats and Responses Track (Sponsored Session)
10/23/2014 10:20 am - 11:10 am Room Fantasia C&D
Sophisticated cybercrimes and advanced persistent threats are occurring at an incredible rate. Aided by new attack techniques, increased financial support and the ease of exploiting social connections, attackers are having more success than ever before. Traditional security solutions are no longer sufficient to defend against these escalating threats.

Advanced threats have become one of the IT security industry's most discussed topics. Today, organized criminal or State-sponsored elements pursue specific targets via well-orchestrated, patient, long-running attacks, often using highly customized malware and tactics. This session explores the activities of the criminal underground. Understanding the scope of the problem will assist in defining the roles of information systems governance, security, audit and assurance for ISSA professionals.
Brian Marshall: VP Research and Development, Vanguard

Architecture Of Global Surveillance

Laws and Regulations Track

10/23/2014 10:20 am - 11:10 am Room Nutcracker 1

Snowden, Anonymous, NSA, FBI, GCHQ, Boeing, China, Cisco, ATT, Verizon, Google, Facebook, GM, Ford, Apple, Amazon, Your doctor, Spouse, Grocer, iphone, android, your child's school. What do they have in common? Each and everyone is a spy. Individuals, corporations and governments have built the modern surveillance state. Executive over reach, insufficient planning, systemic flaws, and blind faith in institutions has led to a global panopticon. Our jobs, social interactions and technology have made it extremely easy to become a spy...or a peeping tom. It's much harder not to look, than to look. App stores, vendors, governments have transmogrified society into the Truman Show. This presentation delves into how we got here, what lessons we have learned, what lessons we have yet to learn, and where we're headed. Based on 10 years of research, this presentation will delve into history, technology, the Bill Of Rights, EU Privacy Charter, George Orwell and others to discuss the origin and architecture of the modern surveillance state and what we can do about it. What's the difference between the US & China? US & Russia? Come and find out.

Raj Goel, CISSP: Author, Speaker, TV Guru, Cyber Civil Rights Activist, Brainlink International, Inc.

Beyond Sandboxing

Application Security Track

10/23/2014 10:20 am - 11:10 am Room Fantasia E&F

Trends in mobility, peer to peer protocols, and virtualization are dissolving our defense perimeter. Without a well-defined perimeter we cannot inspect all inbound content through a sandbox, thus causing gaping security holes. We show how advanced correlation techniques can exploit the intersection of Intrusion Detection and Flow Analysis to result in effective heuristics that uniquely detect compromised assets. Like sand-boxing, these heuristics require virtually 0 prior knowledge of the threats but can find and shut down compromised machines. We will provide some case studies on the effectiveness of such heuristics across a great variety of Enterprises.

Livio Ricciulli: President and Chief Scientist, MetaFlows, Inc.

Continuous Authentication Protects From Physical Attacks on Mobile Terminals

Mobile Security Track

10/23/2014 10:20 am - 11:10 am Room Grand Republic C&D

The current standard method for validating a user’s identity for authentication on a mobile information system requires humans to manage long complex passwords, a smart card or a one-time password. Moreover, as long as the session remains active, typical systems incorporate no mechanisms to verify that the user originally authenticated is the user still in control of the keyboard. Continuous Authentication monitors the user to ensure that the user does not leave proximity of the mobile data terminal, and locks data in real-time. The added benefit is that the user needs to authenticate only once as long as he/she stays in proximity of the mobile data terminal.

Ben Ayed: CTO, Secure Access Technologies

Dr. Scott Jenkins: CEO, Directive Health

ISSA Security Education and Awareness SIG Presentation

SIG Meeting

10/23/2014 10:20 am - 11:10 am Room Nutcracker 2

The SEAG has been successful during this last year and is growing in participants as well as improved content. For 2015 and beyond what can SEAG provide that will help in developing and/or maintaining an Information Security, Education, Training, Awareness Program. How can this be done with minimal staff and dollars while being a requirement for almost every audit? These and other questions hopefully can be answered during this brief interactive discussion. Lead by Kelley P. Archer, CISSR, Facilitator of MN-ISSA SEAG, MN-ISSA Executive Advisor, Distinguished Fellow, ISSA Ethics Committee member and Adjunct Instructor with over 24 years of experience specializing in creating and implementing INFOSEC Awareness Programs.

Kelley Archer: Director Information Security, AIMIA Inc.

Why Enterprise Cyber Security Isn't Working -- and a New Approach

Threats and Responses Track (Sponsored Session)

10/23/2014 11:30 am - 12:20 pm Room Fantasia A&B

Despite billions spent on cyber security, enterprise breaches costing millions are occurring on a daily basis. Why? SIEMs utilize inherently untrustworthy data while other widely used perimeter defenses are simply too rigid – think Maginot Line. Now, imagine if an analyst could see, in real-time, a truthful account of their entire network: they would detect and respond to intrusions immediately, as they occur, eliminating catastrophic loss. Join us to discover how the Department of Defense achieved network visibility and awareness to dramatically increase their security team’s effectiveness with a solution that is now available for private enterprises.

Peter B. LaMontagne: CEO, Novetta

2014 Year of the Mega Breach – Fight Back with a Layered Defense

Threats and Responses Track (Sponsored Session)

10/23/2014 11:30 am - 12:20 pm Room Fantasia C&D

From Spam to Heartbleed and everything in between – protecting your business is well past just antivirus. Whether you are a large or small business there are bad guys looking to exploit any vulnerability they can find in your systems. Today smart business protection calls for a layered defense strategy. The stats are scary:

- Eight of the breaches in 2013 exposed more than 10 million identities each
- 1 in 566 websites have malware
- Ransomware attacks grew 500% in 2013

Join Us To Learn How To:

- Stop threats before they even make it to your network
- Leverage the wisdom of the crowd and only accept files and websites based on reputation
- Monitor in real-time file behavior and block suspicious activity

Katheryne Pelak: Sr. Product Marketing Manager, Symantec

"Get Plumb Maddog Mean." What Josey Wales Taught about Responding to Attacks

Threats and Responses Track

10/23/2014 11:30 am - 12:20 pm Room Grand Republic C&D

In our current threat environment it is not a matter of "if" but "when", we'll be attacked. Adopting the mindset of the attacker and knowing your enemy can give you that "edge" that helped Josey Wales stay alive.

Joseph Patrick Schorr: Strategic Security Architect, HP

How to Get from Security Analyst to CISO: Developing Your Career Path Strategy

Business Skills Track

10/23/2014 11:30 am - 12:20 pm Room Fantasia E&F

So you want to be a CISO. Do you know how to get there? What path you should follow? While there is no single path or easy way, Tim Virtue, CISO with Texas NICUSA, will offer some strategies on managing your security career objectives. He will share the good, the bad and the sometimes ugly aspects of his own journey as well as specific career strategies and roadmaps. Although the focus will be on current and traditional approaches to the CISO role, he will discuss some forward looking, “up and coming” skill sets.

Tim Virtue: Chief Information Security Officer, Texas.Gov

The Human Firewall: Maintaining Your Guise As A Social Engineer

Securing the End User Track

10/23/2014 11:30 am - 12:20 pm Room Nutcracker 1

As Penetration Testers, we are often employed to perform social engineering, phishing and red team engagements. During these engagements, it is important to be able to improvise and withdraw from potential exposure with grace and poise when our efforts fail. We must maintain our guise. In understanding this, we also increase our own and the client's ability to sense the motives of those attempting to exploit the human firewall.

Tim Roberts: Security Consultant, Solutionary (NTT Data)
Brent White: Security Consultant, Solutionary (NTT Data)

Lunch and CISO Panel Discussion

10/23/2014 12:20 pm – 2:10 pm: Room Fantasia Ballroom

Moderator:
Pete Lindstrom: Research Director, SPIRE Security
Panelists:
Bob Bragdon: CSO Magazine
Mary Ann Davidson: Chief Security Officer, Oracle
Brian Engle: Chief Information Security Officer, State of Texas
Sharon Finney: Chief Information Security Officer, Adventist Health System
Wayne Proctor: Director of Information Security & IT Risk Management, UPS

Threat Update Panel Discussion

10/23/2014 2:10 pm - 3pm Room Fantasia A&B

Moderator:
Garrett Felix: ISO and HIPAA Privacy Officer, MediFit
Panelists:
Paul Alvarez: Principal, Threat Intelligence, FireEye Labs
Michael F. Angelo: Chief Security Architect, NetIQ
Dodi Glenn: Senior Director, Security Intelligence and Research Labs
Cris Thomas: Strategist, Tenable Network Security
Lucas Zaichkowsky: Enterprise Defense Architect, AccessData

How to Protect Your Company's Valuable Trade Secrets

Laws and Regulations Track

10/23/2014 2:10 pm - 3pm Room Nutcracker 1

Today US companies loose close to $300 B annually in trade secret theft. Information technology is involved with many of these breaches. In this session we will analyze trade secret laws; recent trade secret theft cases; good security practices to protect your organization's intellectual property and trade secrets.

Frederick Scholl: Visiting Professor of Information Security, Lipscomb University
André (A.J.) Bahou: Managing Partner, Bahou Law Firm, PLLC

Insider Insights: Seven Observations on the Evolving CISO Leader

Business Skills Track

10/23/2014 2:10 pm - 3pm Room Fantasia E&F

When Information Security first appeared on organizational charts, IT technicians found themselves in an unexpected career, in an undefined field, with training that did not include leadership, business alignment, risk assessment, communication or team-building. Today, CISOs play a pivotal role in providing corporate leadership on information security issues, defining security standards and policies, assuring customers of data security and validating controls to regulators. From a unique industry-insider vantage point, Marci McCarthy has witnessed the profession’s transformation and the evolution from unknown "spook" working in the back office to a go-to person and leadership for Boards, management teams and other stake holders.

Marci McCarthy: CEO and President, T.E.N.

Why Teaching Information Security In College Is Important

Community Track

10/23/2014 2:10 pm - 3pm Room Grand Republic C&D

This talk will give a brief introduction and unique perspective in to the world of teaching information security to graduate students. Students range from a variety of levels among some whom are in infosec to many that are not in infosec. Come to this session to learn the ins and outs of why teaching information security is beneficial for all: you and others. What are the challenges? How is it done? Many examples of teaching content will be shown as well as recommended best practices. Bring your Q&A and feedback to this open session!

Roy Wattanasin: ISO, MITM

ISSA Women in Security SIG: Women's Voices – Celebrating Cybersecurity – Lightening Talks

SIG Meeting

10/23/2014 2:10 pm - 3pm Room Nutcracker 2

Join us for a fast-paced and exciting event featuring multiple esteemed speakers sharing thought-provoking wisdom as they continue to drive their destiny as cybersecurity practitioners sky high. They highlight major challenges and triumphs in technology and as strong women leaders. We encourage you to attend and gain valuable insights into the future directions and diversity of the wide realms of cybersecurity.

David and Goliath: Protecting yourself from state sponsored hackers

Infrastructure Track

10/23/2014 3:40 pm - 4:30 pm Room Fantasia E&F

Forgot the politics, state sponsored attacks and espionage are and will continue to be conducted around the world. Organizations across nearly all verticals are caught in the crossfire or actively targeted. Find out who the threats are, how they operate, and what you can do to help protect your network and data.

Chris Camejo: Director, Assessment Services, NTT Com Security

Syrian Electronic Army: Their Methods and Your Responses

Threats and Responses Track

10/23/2014 3:40 pm - 4:30 pm Room Grand Republic C&D

Having helped parties respond to Syrian Electronic Army (SEA) attacks, our organization learned about who they are, their capabilities, and their common methods. They extensively research and then exploit their target while maintaining backdoors primarily to deface their target to draw attention to their cause. This presentation will cover the SEA attack strategies, responding to attacks and finding potential backdoors left behind. It will also cover how to use awareness and technology to mitigate and repel SEA attacks.

Samantha Manke: Chief Scientist, Secure Mentem

The Future of Information Security Awareness

Securing the End User Track

10/23/2014 3:40 pm - 4:30 pm Room Nutcracker 1

In the last year the effectiveness of information security awareness has been the subject of vigorous debate. In this panel, leading experts will discuss the causes for dissatisfaction with historical awareness techniques and how awareness has evolved in the last decade. Topics such as metrics, surrogate outcomes and the latest research will all be discussed.

Kelley Archer: Director Information Security, AIMIA Inc.
Aaron Cohen: Managing Partner, Blackfin Security
Ira Winkler: President, Information Systems Security Association