Information Warfare Summit 9 - "Balancing Security"

Speaker	Title	Synopsis	Bio	Time	Location
Alva, Samuel	"Physical and Network Security: Same Principles, Different Agendas"	Physical and Network Security: Same Principles Different Agendas As a Security professional and well versed in both principles in physical and network security I feel there is a huge vulnerability that exist in both these methodologies. We live in a digital age where everything and everyone is connected in some shape or form, some would say we are digital citizens. Currently most or all physical security equipment is some way connected to the LAN, either through hard-lined, wirelessly or Bluetooth. Physical and Network security share the same principles, each protecting our assets with a layered defense. Physical Walls = Firewalls, Access Control = User Name and Password these are just a few of the similarities we share amongst both principles. Unfortunately Physical and Network security personal have different agendas. Physical security are concerned about the physical threat whereas Network security are concerned about the network threat. Criminals foreign and domestic understand both principles which creates vulnerabilities in our overall layered defense. Having studied both principles, you have to understand that if you can't hack your way in, you must social engineer your way in. The briefing will cover vulnerabilities that currently exist and how by combining both principles, you can mitigate, reduce and identify threats quicker thereby creating a safer more secure environment.		3:00 PM	Room D
Beede, Rodney	"Seagate's Amazon AWS Cloud Security"	Case Study: Seagate's Amazon AWS Cloud Security Overview of the architecture developed by Seagate for use in its IT AWS cloud deployments. Coverage includes use of next generation firewalls and cloud network security controls to secure internet and internal traffic. A technical dive into how the security team at Seagate enabled business flexibility for rapid deployment while balancing security requirements by leveraging Amazon cloud security technologies will be explored. The audience will also learn about the security tradeoffs compensating auditing controls, and limitations of AWS in regards to cloud network security and user management. Additionally, a consolidated checklist based on industry whitepapers and cloud security leaders, as used by Seagate, for evaluation of cloud security readiness will be provided.	Rodney Beede works for Seagate Technology as their IT Cloud Security Architect & Engineer. He received his M.S. in Computer Science from the University of Colorado at Boulder in 2012 with a thesis work titled "A Framework for Benevolent Computer Worms." His primary interests in computer security go back to 2001 and today revolve around web and cloud security. He has also authored a chapter of the OpenStack Security Guide over "Object Storage" and was the discoverer of CVE-2013-3627: McAfee Agent v4.6 Denial of Service.	1:00 PM	Room B
Buchanan, Craig	"Are you serious? Security Reality Vs Recommendations"	In this session, we will discuss the different surveillance video technologies available in a vendor neutral way. We will discuss the pros and cons of analog and digital cameras and different methods o recording and archiving video. At the end of the presentation, you should have a good idea of what is currently on the market and how t make an informed decision about what technologies to adopt to get the most out of your security budget.	Craig Buchanan has worked in government at the city, state and federal levels. He also worked in the private sector for over a decade at computer multimedia innovator Creative Labs, Inc. He currently works for the city of Stillwater Oklahoma, where his duties include installing and maintaining the city's ever-growing fleet of security cameras, servers and monitoring devices. In his spare time, he volunteers for the American Red Cross conducting reviews for the fraud prevention team and is a graduate student at Oklahoma State University, where his research focuses on disaster management.	12:30 PM	Room D
Dawkins, Jerald, Dr	"Cyber Security Perspectives"	Looking beyond the latest buzz words and security products and focusing on cyber security's impact across the organization.		3:00 PM	Room C

Dunkel, Derek	"Vulnerability Management"	Vulnerability Management - My company started a vulnerability management program from scratch, on a shoe string budget, and had an 80% reduction rate within 2 years. In this talk, I'll go through my experience: the highs, the lows, and how any organization can improve their vulnerability metrics. This talk will not be vendor specific but may include screen shots from our vulnerability management product. Any organization can have a robust vulnerability management program, but it cannot be completed by just one department. Many key factors of the risk management life cycle are critical to a successful program. Finally, we'll go through the steps that our group has taken to maintain and improve upon our initial gains. Major points – vulnerability management isn't just a technical problem, it requires time and effort both in IT and with major business units. Vulnerability management isn't sexy but is incredibly valuable to an organization -- we've seen cost reductions, infection rates fall and better performance through our efforts. I also don't want to be anti-vendor, but this isn't an expensive program and it's not a feature set from a vendor that will define your organization's success. My opinion is that vulnerability management is the cheapest and most effective way to protect your endpoints….your efforts won't win any Gartner awards, but they'll keep your organization and its data safe.		3:00 PM	Room B
Earnest, Wes	"Investing in Information Security"	Topic: Investing in Information Security: A Case Study in Community Banking Small businesses, such as community banks, often do not have resources dedicated to information technology, much less resources dedicated to information security. Despite larger financial institutions having more resources to invest in information security, they are also attempting to secure much larger and more complex environments. Community banks, with a smaller footprint of compute systems and networks, require a comparatively smaller investment in order to produce even greater results. This presentation shows how one small community bank improved its information security strategy by focusing the decision making process on solutions that reduce risk in terms of business opportunity, information technology and compliance. Following these basic principles, Smalltown Community Bank transformed its approach to culture and risk assessment into a driver for continuous improvement and competitive advantage.		12:30 PM	Room E
Eckenstein, Ed	"What I've Learned From Identifying 35,000 Phishing Websites - Giving Users a Second Chance"	What I've Learned From Identifying 35,000 Phishing Websites. Giving Users a Second Chance. A scammer's task is not only to get their victim to click a link in an email but also to maintain the illusion their phishing site is legitimate. We train our users to identify phishing emails and not to click on links in anything that looks suspicious. Sometimes they miss the warning signs and click tainted links anyway. Then they're staring at a fraudulent site. At that moment, there's a second chance for them to spot a fake site if they know what to look for. You can find plenty of advice online on how to spot a phishing emails. However, there's not as much good information on spotting phishing web sites. In this session, we'll look at real-world examples drawn from over 35,000 phishing sites I reviewed as a participant in a community-based phishing clearinghouse. We'll examine: • Some obvious and not so obvious phish spotting clues. • Tricks scammers use to keep the victim from realizing they're being phished. • How phishing URLs are manipulated to appear legitimate. • The problem with those pesky account verification questions	Ed Eckenstein is the founder and principal consultant of Smartly Secured, LLC. He has expertise in both cybersecurity and training. He holds Security+ and SSCP certifications and has an M.A. degree in Information and Learning Technologies from the University of Colorado Denver. Ed serves as a board member of the Oklahoma Infragard chapter. He is an adjunct instructor at Francis Tuttle Technology Center in Oklahoma City where he teaches personal computer security awareness	1:00 PM	Room A
Estes, Grayson	"Hacking with UAVs"	Hacking with UAVs - when Pentesting tools become Airborne. In this talk I will discuss many current pentesting tools, I, automation tactics, and open source projects that when attached to a UAV could be very lethal to a network or organization		2:00 PM	Room C

Farrow, Donovan	"Incident Response (find the hacker) - Foundation of Digital Forensics"	Everyone these days wants to be a hacker" and find all the latest attacks in order to subvert the everyday IDS/IPS or Anti-Virus. So what about the Blue Team? What can we do in order to track down these malicious attacks without relying the blinking lights of an alerting system. What bread crumbs are left behind by these hackers? Where can we find them and what can we do to bring them to justice?		12:30 PM	Room A
Lowder, Jim	"Finding Balanced Security using NIST RMF"	Finding Balanced Security Using the NIST Risk Management Framework -The NIST Risk Management Framework (RMF) offers a comprehensive, multi-dimensional potential for balancing cost and risk considerations in achieving a cost effective, efficient and secure implementation of information systems and critical infrastructure protection, especially for federal government customers, for whom it is often mandatory. This presentation will explore tips, tools and insights for utilizing sound requirements definition, performance parameter prioritization, and architectural trade-offs in the RMF process to achieve an integrated, comprehensive and balanced system security authorization plan.		1:00 PM	Room D
McCrary, Barbara	"Developing Security Policy"	Developing Security Policy -Every organization, regardless of size, should consider having documented security policies, but many do not. Every organization has a position or policy on security, but it may not be written down anywhere. Policy can form the foundation of your entire approach to security, but you must consider the corporate culture and work to achieve harmony as you work to improve documentation. You may not have a policy for every situation that could arise, but aim for creating broad policies that you can enforce now.		12:30 PM	Room B
Meding, Paul	"Ransomware: It's not your grandmom's family photos anymore, it's your company's database"	We will be discussing the history and recent evolutions of ransomware as it has pivoted from casual end users to corporate environments. We will then discuss strategies to identify, Respond, and defend our networks, our users, and our data.	Net Witness Sales Engineer, RSA Security	1:00 PM	Room E
Olivares, Dan	"Are you Cloud Secure?"	The use of cloud solutions within an organization is no longer an option, but a necessity for go-to-market speed, agility, scale and cost-savings. However, the access and ease of implementing cloud services exposes your organization and leaves you with all the risks of securing your company's assets. All too often, the risk of cloud usage is not completely understood by the business. While the cloud promises scale and speed to propel your business, it also introduces threats and complexities you must consider. Do you really know where or how much cloud is being utilized by your company? To make the most of your move to cloud and protect your business, you must understand the associated risks and build an appropriate plan for your organization. Optiv helps organizations define, architect and operate cloud security at scale, so you can grow your organization with confidence. Today, there are more cloud applications in use than ever, but there are also more security solutions to consider. During our session, we will help provide you with an introduction to planning for Cloud Security that can help you navigate the options in protecting your cloud-enabled business.	Dan Olivares Director of Cloud Security Programs	11:00 AM	Room ABCDE
Optiv Pentest Panel	"Life of a Pentester"	Pentesting Panel - with Tim Elrod, Lars Coenhour, and Kyle Grote. What really goes on in the life of a penetration tester? Come meet with our Pentesting Panel of experts to see!		1:00 PM	Room C
Pyle, Matthew	"Friendly Phishing"	Friendly Phishing, discussing our experience with building a phishing training campaign that the end users actually like, and appreciate.		2:00 PM	Room A

Ross, David	"Cyber Attacks: A Warning - The Need to Understand the Dangers of Organized Cyber Criminals"		Since May of 2000, David Ross has grown TriCorps Security, a corporate security firm, into a nationally-recognized corporation, headquartered in Oklahoma City, with 750 employees in eleven states, while also building other companies in different industries. David graduated high schoo in Durant, Oklahoma, and enlisted in the United States Army. the military he returned home and earned a Bachelor's Degre in Criminal Justice from Southeastern Oklahoma State University. After graduating from college he joined the Oklahoma Highway Patrol as a state trooper, rising to the rank of Major. During his career with the Highway Patrol, Davi commanded the Governor's Security Detail, protecting severa of Oklahoma's governors and first families. He also commanded the Investigations Division and State's Tactical Team.	9:00 AM	Room ABCDE
Schweizer, Scott	"Security in the Digital Age - Cyber Crime Inhibiting Economic Growth"	As the Americas Distribution lead for Security Architecture, Scott is responsible for design development and implementation of distributor and partner program's within Cisco's #1 IT leading Security Solutions Portfolio. With the World going Digital, the Industrialization of Hackers and Cybercrime on the rise, Security Synergy around People, Processes, and Technology is "top of mind" for Scott at Cisco. In 2016, he delivered over 20 main stage presentations to partners and customers on "Security in the Digital Age". Scott is a 20+ year veteran in IT Channels and his family resides in Southern California.	– Americas SBDM, Security Architecture, Cisco	2:00 PM	Room D
Scott, Vincent H.	"Total Security"	Total Security: Balancing Investments as you increase security maturity - PwC provides auditing, tax, and consulting services, including Cyber Security risk, security maturity, technology implementation, incident response, and forensics services to a broad range of clients globally. When balancing security it is very challenging for organizations to decide where to invest, when to invest, how to invest in security with an exploding list of compliance requirements, governing body investigations from the FCC to the SEC, and a constantly shifting attack landscape. It is important to balance those investments as you drive up the maturity continuum to provide 360 degree defense. With a 100 ft wall in one section of you defenses, and a gently sloping path with a sign that says "Hackers enter here" in another, which path is the adversary more likely to take? So creating a holistic security program that balances the different areas of security (Identity and Access, network security, app dev etc) along with the different regulatory and legal requirements is critical to the success of a security program. PwC will offer insight on these challenges, and make recommendations on how organizations can create programs which provide for effective ways to reduce real risk, and are sustainable in a volatile cyber security environment.		4:00 PM	Room A
Simpson, Bob	"Critical Security Controls Change Everything"	Critical Security Controls Change Everything. It starts with an overview of the CSC, how they are different than other frameworks, and how they are applicable to organizations of various sizes. The presentation can stop there, and that would fit into a 25 minute slot. Then, though, I do a deeper analysis of one specific control and talk about automation and management reporting. That takes another 20 minutes or so, so the whole thing would fit in the 50 minute slot.	Bob Simpson is the creator of GhostSentry, an access control and compliance firewall and CIO for Finley & Cook, PLLC, a private accounting firm where he has served for 9 years. Before that, Bob was Security Architect for the Oklahoma Department of Human Services. Mr. Simpson holds the CISSP, GCIH, GCIA, and GPEN, as well as MCSE and CCNA Security certifications. He is a member of the SANS Advisory board and InfraGard.	2:00 PM	Room E
Spaid, John	"Public Wi-Fi Security"	Public Wi-Fi Security - Demo Current Wi-Fi attacks and show detection/countermeasures. Hide yo' routers! Hide yo' hotspots! Cuz dey be reaver'n errbody up in herr!	John Spaid has been breaking breakable things for the past 3 years, and has yet to find a thing that can't be broken. He will review typical public WiFi setups, their risks, and how you or anyone with a little time & money can snoop, spoof, and crack WiFis for fun and profit... in your WiFi lab only, obviously.	4:00 PM	Room C

Sweaney, Nathan	"Hunting SysAdmins"	Hunting SysAdmins: As a penetration tester my job is to demonstrate the business risk of vulnerabilities, which often means gaining access to sensitive data or systems. But attacking your data isn't always a straight route. Most organizations have invested heavily in protecting their most sensitive assets. Often the easiest way to compromise a system is to first target the system administrators. During this talk I'll outline a number of ways that attackers focus on finding and attacking administrators within an organization. I'll explore how sysadmin systems can be exploited to pivot onto more sensitive systems. And then I'll outline specific steps defenders can take to better shore up these targets. This talk will provide attackers with new ideas and tactics, defenders with mitigation techniques, and management with a better understanding of indirect threats to sensitive systems.	Nathan Sweaney is a Senior Security Consultant with Secure Ideas. He has over 10 years of experience in the Information Security field with a wide range of involvement in network operations, systems administration, and application security. Nathan has worked with both very large and very small businesses to provide practical risk assessments that are useful at both technical and executive levels. Prior to joining Secure Ideas, most of his career was in the point-of-sale industry helping retail, hospitality, grocers, and restaurateurs apply strong information security controls in unique and demanding situations. He holds a B.S. in Computer Science and the GPEN, GWAPT, and GAWN certifications.	4:00 PM	Room B
Teel, Lisa & Aaron Baillio	"Roadmap to Balancing Security and Academic Freedoms"	Roadmap to Balancing Security & Academic Freedom @ the University of Oklahoma Corporations and governments work to closely regulate and restrict devices, users and online traffic in an effort to protect intellectual property, strategy and other sensitive data. However, that doesn't make as much sense in an academic environment which draws on the intellectual inputs from faculty, students and other members all over the globe. At the same time, higher educational institutions must protect personal information and intellectual property while preventing computing resources from being compromised or leveraged to attack other targets. The University of Oklahoma viewed the landscape and has developed a path that walks the line between Security and Academic Freedom. We've organized several new committees that address risk, disaster recovery and information security with members from all different levels. This presentation highlights where we were as an institution, where we needed to be from a risk and compliance perspective, and what we are doing to achieve that goal.		3:00 PM	Room E
Thompson, Andy	"Advanced Targeted Attacks using Powershell Empire"	See the world from the eyes of a hacker. This talk will demonstrate the phases of a targeted attack, from initial breach to the end-game attack. I will demonstrate password dumping, pass the hash, and golden ticket attacks to demonstrate the ability of the PowerShell Empire post-exploitation framework. I will also discuss how to prevent and protect your organization from such attacks. (Also has a Ransomware talk)		10:00 AM	Room ABCDE
Tribble, Eryn	"Resilience and Data Security"	Resilience and Data Security New trends in resilience are making data security more uncertain than ever. What are the bottom line business needs to continue to gain business value and strength during times of false security? Major Points: * Trends in resilience (Diversity, Globalization, Accountability. Automation) increase market pressure, expectation and demand result in increased damage during failure. * New reaches for higher highs and lower lows require greater foundational certainty to navigate sustainably. * Need to account for the cost of innovation and creativity: building failure into the process. Audience ROI: * Awareness of tension, need for ability to negotiate to find common ground and creative solutions, opportunities for greater agility from aligned expectations creates new points on which to leverage critical gains. * Resources to assist in developing alignment, trust and strength for resilience requirements.	You have found something completely different in our next speaker: Resilience expert Eryn Tribble has several levels of advanced certification and degrees in business, continuity and psychology. This unique lens allows a innovative perspective to information warfare that's built of more than just "ones and zeros". Her experience in building empirical corporate strength offers a unique advantage to planning around the organization's greatest and most colorful asset: the human component. Eryn is the owner DCS Planning, a midwest consulting specializing in strategically addressing risk to operations. DCS works with businesses which are competitive, savvy and want to protect their HIGH-dollar value creation. Eryn is known for "spicing it up" on the board of the University of Oklahoma's Resilience Development Institute and "keeping it real" as an overactive member of the national Association of Continuity Professionals. And of course she has worked in conjunction with many national powerhouses such as the Department of Homeland Security and the Federal Emergency Management Agency (FEMA).	2:00 PM	Room B

Watson, Michael	"Crack the Code: Defeat the Advanced Adversary"	The presentation will give a Good understanding of emerging security approaches that will be helpful to incorporate into your organization's security strategy. Key perspectives - right mindset for the challenges that CIOs face today: Think Strategically About Security, Safely Enable the Business, "Safe Enablement", Apply Innovative Thinking to Security Challenges	Michael Watson has 16 years of experience as a Network and Security engineer across multiple industries.	12:30 PM	Room C
Yates, Chris	"What would you do if you had firewalls EVERYWHERE? - Practical Advice on What to Do with the Zero Trust Network Security Architecture"	Is your perimeter secure, but you struggle with how to implement network security controls WITHIN your network? Many organizations approach this problem by creating zones where they place risky applications and systems, but they still have a significant amount of internal systems that have NO preventative or detective controls around them except for the Internet/DMZ perimeter. When all it takes is one user clicking on a phishing email to infect a workstation, it is imperative that we take a new approach that allows us to have better control of our internal networks. The Zero Trust Network Security Architecture provides a framework to solve this problem. I will describe the model, and provide some real world examples of vendors who provide solutions that help make the model a practical reality.		3:00 PM	Room ABCDE