

2016 State of Ohio Cyber Security Day

8:30 – 9:00 am Registration / Check-in

9:00 – 9:10 am Opening Remarks

Stu Davis – State Chief Information Officer, *State of Ohio*

Bio:



Stu Davis currently serves as the State Chief Information Officer (CIO) and Assistant Director for the Ohio Department of Administrative Services (DAS), Office of Information Technology (OIT). Stu has a varied background in IT leadership and management, including infrastructure, enterprise shared services, and spatial technologies. Prior to his appointment as State CIO, Stu served as the State Chief Operating Officer and deputy director of the Infrastructure Services Division within DAS/OIT.

As the State Chief Information Officer, Stu leads, oversees and directs state agency activities related to information technology development and use. As Assistant Director of DAS, Stu oversees the Office of Information Technology (OIT) which delivers statewide information technology and telecommunication services to state government agencies, boards and commissions as well as manages IT procurement, policy and standards development, lifecycle investment planning and privacy and security management.

Stu serves as Chair of the Multi-Agency Radio Communications System (MARCS) Steering Committee that supports voice and data communications for statewide public safety and emergency management. He also chairs the Ohio Geographically Referenced Information Program (OGRIP) Council that provides geographic information systems (GIS) coordination across the state between all levels of government and chairs the Emergency Services IP Network (ESINet) Steering Committee that focuses on Ohio's Next Generation 911 solution.

Stu is a 16 year member and past president of the National States Geographic Information Council (NSGIC). He is a 4+ year member of the National Association of State Chief Information Officers (NASCIO). Stu has served on various NASCIO committees as well as the executive board. He also served as Secretary/Treasurer, Vice President and currently serves as Past President.

Stu's career spans 35 years focused on state and local government with 12 years of hands on experience in local government, 18 years in state government and 5 years in the private sector consulting to state and local government on IT/GIS initiatives

9:10 – 10:00 am Morning Keynote Speaker

Scott Montgomery – Vice President and Chief Technology Officer, *Intel Corporation*

The Need for Efficiency

Information security and privacy has become an even more complex challenge over the last few years. The intense drive for business or mission to become more mobile, utilize cloud services, generate and retain more and more varied types of data than ever before, to internet-enable every facet of our work and personal lives, from the factory floor to the light bulbs in our homes creates an untenable math problem for practitioners. Although the devices and threats continue to increase, the budget, number of practitioners, their amount of training, and especially the number of hours in the day – remain

static. Something has to give in this bad math equation, and where organizations suffer is in their efficiency, creating business or mission impacts through not only the detection of breaches but also their remediation. This presentation will highlight the precious value of the infosec labor hour, and the need for increasing the organization's efficiency in order to better drive their business or mission.

Bio:



Scott Montgomery is Vice President and Chief Technical Officer for the Intel Security Group at Intel Corporation. Montgomery has dedicated his career to information security and privacy software development, gaining a breadth of expertise that spans from silicon to satellite. He joined the Intel organization in 2011 with the acquisition of McAfee Inc., now a wholly owned subsidiary that operates as the Intel Security Group.

Before assuming his current position in 2015, Montgomery was chief technology officer for McAfee's public sector and America's business units. His efforts helped drive government and cybersecurity requirements into McAfee products and services and guided the company's policy strategy for the public sector, critical infrastructure and threat intelligence.

Earlier in his career, Montgomery spent six years at Secure Computing Corporation (acquired by McAfee in 2008), where he was responsible for worldwide product management and corporate strategy.

10:00 – 10:10 am *Break*

10:10 – 11:00 am

Main Room

Split Session

Robert E. White II – Supervisory Special Agent, *FBI*

Cybersecurity: What you don't know *can* hurt you

Alerts about large-scale cybersecurity breaches happen almost every day. It seems that no organization is immune to hacks, attacks or insider espionage. How can you protect yourself?

The first line of defense against cyberattacks is knowing what kind of threats and vulnerabilities exist so that you can develop a plan to mitigate them. Join Special Agent Robert White for a discussion on cybersecurity and fraud prevention.

Special Agent Robert White of the FBI will discuss:

- the tools and methods cyber criminals use to get access to important data
- the damage cyberattacks can inflict on your finances and reputation
- best practices for protecting your organization

Bio:

No Picture
Available

Special Agent Robert E. White II is a native of Woodbridge, Virginia. He has a Bachelor of Science in Computer Science from the United States Naval Academy and Masters of Business Administration from The Ohio State University.

Prior to joining the FBI, Special Agent White served 13 years in the United States Navy as an enlisted sailor, Surface Warfare Officer with Electronic Warfare specialty, Naval Parachutist, Navy Diver and Cryptologist. His personal awards include a Joint Commendation Medal, a Navy Commendation Medal and 5 Navy/Marine Corps Achievement Medals.

Since 2002 SA White has served in the FBI as a Special Agent, Technically Trained Agent and Supervisory Special Agent. In the Cincinnati Division, he investigated and/or supervised national security and criminal computer intrusions, counterintelligence, child exploitation, Internet extortion, and Internet fraud matters. SA White's collateral duties include SWAT Team member and FBI Instructor. He is author of the FBI's National Cyber Emergency Incident Response Plan and a recipient of the FBI Director's Award for Leadership.

-----OR-----

Breakout Room 1

Simon Herring – Information Security Consultant, *Ubersecure*

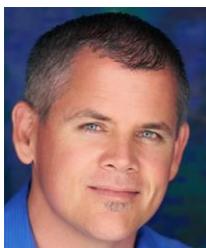
The Overwhelmed Security Professional

Simon Herring is a security expert on a mission, not just to find security holes, but to help people actually do something about them. But today's security professional is spread thin...struggling to stay afloat in a sea of constant demands. Many are stuck in meetings, spinning their wheels with internal business units, and performing mundane tasks that barely scratch the surface of their full potential. With thousands of unread emails, crazy deadlines, and overdue projects, even the best professionals are overwhelmed and looking for change. Consider these direct quotes from some of Simon's clients:

- "I have so much to do and don't know where to begin."
- "I feel stretched in 10 different directions. I'm not focusing on anything."
- "I love security, but I don't love what I do anymore."

The overwhelmed security professional – distracted and exhausted – makes a hacker's job easier. The adversary, after all, has nothing but time to think, plan, and strike. So how do you gain ground against an enemy that has such a critical advantage? In this entertaining, how-to packed presentation, Simon will teach you:

- How overwhelm begins and what it means to information warriors.
- What habits steal your focus, wreck decision making, and actually perpetuate overwhelm.
- His personal process for thriving in chaos, loving what you do, and helping others do the same.

Bio:

Simon Herring is an independent cyber security consultant with nearly 25 years of experience. He equips front-line information warriors at billion dollar companies with common sense tips, tricks, and tactics for doing more with less in a world of increasing threats. Through assessments, workshops, and one-on-one coaching, Simon helps executives, managers, and IT teams discover what's holding them back and how to achieve security success. Simon loves security, but people are his passion. You'll enjoy his stories, deep technical expertise,

and his dream of building better security professionals. You can reach him at simon@ubersecure.com.

-OR-

Breakout Room 2

Steve Holton – Infrastructure Specialist, *State of Ohio*

Chopping Logs: First Steps to Becoming a Forensic Log Guru

The exhilaration of slogging through log files is often one of the first steps in a {security | performance | problem} investigation. Attend this session and learn how to use Microsoft's (free) Log Parsing tools to make finding the relevant needles in the log file needlestack fun (or at least a little bit easier). We'll cover Log Parser commands and Log Parser Studio (gui) features, and investigative techniques that will allow you to home-in on log data relevant to your investigation.

Bio:

No Picture Available

In previous lives, Steve has been a system programmer (IBM Mainframe), software developer (Goal Systems/Legent), freelance consultant, web developer and administrator, and sysadmin. He is currently attempting to assist agencies to stamp out vulnerabilities in all State agency web sites.

11: 00 – 11:10 am *Break*

11:10 – Noon

Main Room Aaron Ansari –, Central Ohio *OWASP Board Member*

OWASP Top Fundamental – Application Security

Recently, there has been a new addition to the OWASP Mobile Top Ten. OWASP debuted the 2014 list and briefly highlighted examples of threats in the new M10 category. In Aaron's talk, Aaron will discuss some of the new categories in much more depth. He educates the audience about the prevalence of binary risks and highlights the mobile app risks that relate to this new category and how to leverage particular OWASP Projects for the solution. By the end of this talk, you will have a solid understanding of the new components in the OWASP Top 10 and how to begin thinking about solutions to this category.

Bio:



As an Account Executive at GuidePoint, Aaron brings practical knowledge which allows him to deliver tailored, seamless integration for any company - large or small. Aaron has overall responsibility for the accelerating growth in the North Central US & Canada and focuses on key verticals to expand their products and services to new markets & businesses.

At BMW Financial Services, Aaron facilitated security program management. Aaron oversaw development and application of IS application security policies, standards, and guidelines. He managed application compliance across the BMW & also served as a subject expert ensuring key vendors and partners maintained BMW's practices.

Aaron built his risk management portfolio with prior roles at JPMC, Cardinal Health and Huntington. At Chase, he led management of multiple security groups which included risk management of the deposits platform, BC&DR planning and long-term risk planning & internal auditing. At Cardinal, he oversaw the installation & management of intrusion detection devices globally, also conducting HIPAA audits.

Aaron received his MBA from Franklin & his BS in Comp Sci from OSU. He gives back and uses his experience as an Instructor at Franklin, teaching Info Sec. Aaron also has an active family life & spends much time with his 2 kids & wife. They reside in Dublin and are involved in their church as well as volunteering for their kids' school. For more information on the OWASP Foundation, the local Columbus chapter or for membership go to: <https://www.owasp.org/index.php/Columbus>.

Noon – 1:10 pm *Lunch Break*

New this year: The main room will be available for networking during lunch.

Bring your lunch, grab something from the food truck (available on-site) or run out and get something and bring it back! The State of Ohio OISP senior staff will be having their lunch in the main room and would love to have you sit down with them for a Q & A and/or networking during your lunch break. All the OISP staff members will have on a Blue name badge so you are able to recognize them. All attendees are welcome to use this time for networking with each other as well!

1:10 – 2:00 pm Afternoon Keynote Speaker

Brent Huston – Security Evangelist and CEO, *MicroSolved, Inc.*

When Cars Don't Crash Anymore – A look at the near term collision of tech, machine learning, AI & your life.

Just over the horizon of perception is a set of changes that will make the industrial revolution and the Internet seem small in comparison. A near term collision of technology, artificial intelligence and human lives seems inevitable. Beginning with the supposition of what happens when cars don't crash anymore, this talk attempts to get the audience thinking about the coming changes and their impacts on our organizations, our economy, way of life and personal choices. From careers to privacy, and from national security to globalization, everything you know today is about to change and this talk strives to help get you thinking about where these changes lead and how you can prepare and participate.

Bio:



Brent Huston is the Security Evangelist and CEO of MicroSolved, Inc. He spends a LOT of time breaking things, including the tools/techniques and actors of crime. When he is not focusing his energies on chaos & entropy, he sets his mind to the order side of the universe where he helps organizations create better security processes, policies and technologies. He is a well-recognized author, surfer, inventor, sailor, trickster, entrepreneur and international speaker. He has spent the last 20+ years dedicated to information security on a global scale. He likes honeypots, obscure vulnerabilities, a touch of code & a wealth of data. He also does a lot of things that start with the letter "s". You can learn more about his professional background here: <http://www.linkedin.com/in/lbhuston> & follow him on Twitter (@lbhuston).

2:00 – 2:10 pm *Break*

2:10 – 3:00 pm

Main Room

Split Session

Bob Smock – Vice President, *Gartner Consulting*

Improving Security by Benchmarking your Security Maturity, Risk Exposure and Program Spend

Insights and trends show how and where security and risk leaders should focus security-specific initiatives and investments by measuring and correlating the perspectives of existing protection capabilities, the cost of achieving those protection capabilities, and how much risk remains to be managed using the current approach. View the impact of this measurement and correlation across the various domains of the enterprise security architecture, see how existing approaches compare to industry peer groups and industry leading practices, and identify opportunities for improving the return on investment for deploying appropriate protection capabilities, improving security maturity, and lowering risk exposure.

Bio:



Based in Houston, Texas, Bob Smock is an experienced consultant with more than 30 years of IT experience with a background in software and infrastructure development and operations, IT architecture engineering and design, and senior/executive-level IT management. His background also includes more than 25 years in IT and information security and mission-critical risk management. He has provided leadership and expertise for numerous successful IT and security projects across a wide spectrum of industries including government, aerospace, defense, financial services, health care, education, insurance, manufacturing, and service providers.

Bob currently leads the Gartner Public Sector Security and Risk Management team, with projects stretching across the nation for State and Local government entities as well as Federal. He has conducted or led more than 1000 security program evaluations in numerous commercial and public sector industry verticals. This includes several hundred security strategy assessments conducted for public sector entities over the past five years, which involved the development of organization-specific strategic security architectures and improvement deployment roadmaps.

Bob has extensive experience in IT security architecture strategy and security program development and management, including executive management experience. Specific security process experience includes security policy and governance, computer and data protection, identity management including multi-factor authentication, risk analysis and threat assessment, business continuity and disaster recovery, incident response and forensic investigation, training and awareness, intrusion detection and monitoring, IT audit and change management with assurance, PKI and encryption, and secure application development. Bob is familiar with numerous security standards including NIST, (including FISMA, PIV, and HSPD-12), ISO-27001, Cobit, and ITIL security management.

Prior to joining Gartner/Burton Group in 2008, Mr. Smock spent 17 years as the CISO and Director of IT Security with contractor management responsibilities for providing the protection of NASA's ground-based IT resources that supported space operations at several NASA manned spaceflight centers. Before that, Mr. Smock provided program management and technical leadership as director of Rockwell International Information Security Consulting, and was the director of R&D for a private engineering and software development firm.

Mr. Smock is a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), a certified Project Management Professional (PMP), and is a graduate of the Federal Law Enforcement Training Center (FLETC). He has numerous professional organization affiliations and is also a college-level educator, writer, and public speaker. He holds an approved U.S. Government National Agency Check with

Inquiries (NACI) background investigation and (formerly) a SECRET clearance. Mr. Smock also holds a Bachelor of Science degree in Computer Science and Engineering Technology from Texas A&M University.

-----OR-----

Breakout Room 1

Steve Holton – Infrastructure Specialist, *State of Ohio*

Chopping Logs: First Steps to Becoming a Forensic Log Guru

The exhilaration of slogging through log files is often one of the first steps in a {security | performance | problem} investigation. Attend this session and learn how to use Microsoft's (free) Log Parsing tools to make finding the relevant needles in the log file needlestack fun (or at least a little bit easier). We'll cover Log Parser commands and Log Parser Studio (gui) features, and investigative techniques that will allow you to home-in on log data relevant to your investigation.

Bio:

No Picture Available

In previous lives, Steve has been a system programmer (IBM Mainframe), software developer (Goal Systems/Legent), freelance consultant, web developer and administrator, and sysadmin. He is currently attempting to assist agencies to stamp out vulnerabilities in all State agency web sites.

3:00 – 3:10 pm *Break*

3:10 – 4:00 pm **Split Session**

Main Room

Matt Curtin – CISSP and Founder, *Interhack*

Protecting Assets Under Global Threat

This is not a game and this is not an abstraction. The Internet has brought the entire world closer together. As a consequence we find that the information infrastructure that we use locally is exposed to global thread. How can we build systems that will work effectively while being targeted by hostile actors worldwide? Building systems and operations that are resistant to attack requires much more and firewalls and encryption. It requires good policy we will discuss how to make policy procedures and technology work together to protect our information and infrastructure.

Bio:



Matt is a computer expert, leading Interhack's Cyber security team. Through projects and managed services, Interhack helps organizations to prepare for, respond to, and recover from high-impact incidents like data breaches, trade secret misappropriation, and business litigation. Matt has appeared as an expert witness in civil, criminal, administrative, and military **adjudication**. Matt is also a Sr. Lecturer in the Department of Computer Science and Engineering at The Ohio State University, where he began teaching in 1999. He is the author of:

- Developing Trust: Online Privacy and Security
- Brute Force: Cracking the Data Encryption Standard

-----OR-----

Breakout Room 1

Brent Huston – Security Evangelist and CEO, **MicroSolved, Inc.**

From Phishing to Ransomware – Following the Flow of Critical Security failures

It only takes a single click - just one mistake - and the bad guys win the day. Follow the speaker on a walk through some of the fascinating ways that attackers select, target and exploit their victims using bleeding edge techniques. More than an awareness lesson, this talk features examples of real world attacks, the consequences of making simple mistakes and the aftermath of what follows. Join us for an up to the moment discussion of watering holes, coercion, accidents, ransom and crime. If you already know not to click on that link, you only know a small part of the story. Go beyond the headlines to the technical discussions and board rooms of those who have learned the hard way...

Bio:



Brent Huston is the Security Evangelist and CEO of MicroSolved, Inc. He spends a LOT of time breaking things, including the tools/techniques and actors of crime. When he is not focusing his energies on chaos & entropy, he sets his mind to the order side of the universe where he helps organizations create better security processes, policies and technologies. He is a well-recognized author, surfer, inventor, sailor, trickster, entrepreneur and international speaker. He has spent the last 20+ years dedicated to information security on a global scale. He likes honeypots, obscure vulnerabilities, a touch of code & a wealth of data. He also does a lot of things that start with the letter “s”. You can learn more about his professional background here: <http://www.linkedin.com/in/lbhuston> & follow him on Twitter (@lbhuston).

4:00 – 4:10 pm Break

4:10 – 4:30 pm Closing Remarks



Russ Forsythe – State Chief Information Security Officer, **State of Ohio**
and
Daren Arnold – State Chief Privacy Officer, **State of Ohio**

Russ Forsythe currently serves as the Chief Information Security Officer (CISO) for the State of Ohio. Prior to this role he served as the Deputy Chief Information Security Officer and Enterprise Vulnerability Manager for the Office of Information Technology (OIT). Russ has served the State for 27 years and has a diverse IT security background, including operational security, vulnerability management solutions, network management solutions, forensic and incident response. As the CISO he leads the enterprise security team. Their goal is to provide governance and operational security controls for Ohio’s cabinet level agencies, boards and commissions. With the ever increasing demands placed on security teams it’s becoming more important that we work together to share knowledge and lessons learned. If you have questions or information to share please feel free to contact Russ or any of the OISP team

Daren Arnold is the Chief Privacy Officer for the State of Ohio. In that role since 2008, Daren assists more than 80 state agencies and their data privacy leads with evaluating privacy risks and adopting privacy protection processes designed to mitigate those risks. Daren joined the State of Ohio in 1996 and has provided analysis and advice on matters of information technology policy and law for the Ohio Office of Information Technology. Prior to working for Ohio, he was the lead researcher for NASCIO, the National Association of State Chief Information Officers. He is an attorney, a graduate of the University of Kentucky, and a certified information privacy professional (CIPP-US).



OhioDAS
SERVICE · SUPPORT · SOLUTIONS
DEPARTMENT OF ADMINISTRATIVE SERVICES