# 2017 North American International Cyber Summit
## Hosted by Michigan Governor Rick Snyder
### October 29-30, 2017
### COBO Center - Detroit, MI
### *Twitter Hashtag: #MICyberSummit*
### As of October 19, 2017

**Monday, October 30, 2017 - COBO Center, Detroit, MI**

| Start Time | Presentation |
|---|---|
| 7:30 AM | **Registration and Continental Breakfast & Visit with Sponsors** |
| 8:00 AM | **High School Cyber Challenge**<br>Teams of high school students from around the state will compete against each other in a unique cyber competition. These students have completed Round 1 of the competition and have scored high enough to be invited to go head-to-head in a fast-paced cyber challenge. Students will complete the challenge from 8:00 am until 12:00 pm with the top 3 teams receiving awards. |
| 8:30 AM | **Presentation of the Colors by the Michigan State Police Color Guard and Performance of the National Anthem by OneAchord** |
| 8:35 AM | **Welcome & Event Kick Off**<br>**Speaker:**<br>*David L. DeVries*, DTMB Director and State of Michigan Chief Information Officer |
| 8:40 AM | **City of Detroit/Local Welcome**<br>**Speaker:** *Warren Evans*, Wayne County Executive |
| 8:45 AM | **Keynote Speaker:**<br>*Michigan Governor Rick Snyder* |

| | |
|---|---|
| 9:05 AM | **Title:** Michigan's Tomorrow, Today<br>**Description:** Digitization, automation, and cybersecurity are rapidly changing the world. Every city, state, country and business faces a challenge like never before to establish and maintain a competitive edge in this digital world – and first movers will pave the way. During this 20-minute keynote, Alison Gleeson will paint a vision for how Michigan will lead in the United States, driven by mobility, manufacturing, citizen-centric government, training and education, and smart cities.<br>**Speaker:** *Alison Gleeson* , SVP, Americas, Cisco |
| 9:25 AM | **Title:** The State of Cyber in the National Guard<br>**Description:** Cyberspace is an integral component of the United States' national security, and offers opportunities for economic prosperity and individual liberties. Threats within the cyber domain transcend all sectors of a technologically-dependent society, providing threat actors a vast array of effects to leverage upon leadership and citizens. The National Guard is preparing for these threats that range from nation state-actors to non-affiliated individual criminal activities and seeks to improve readiness resiliency against these elusive 21st century threats.<br>**Speaker:** *General Joseph L. Lengyel* , Chief National Guard Bureau, Department of Defense, National Guard Bureau |
| 9:45 AM | **Diamond/Platinum Ted Talk Session:** Security Awareness: What Does it Mean to You and Your Organization?<br>**Description**: In today's cyber threat landscape, it's not a matter of if but when a cyber-attack will occur. Every day, businesses and governments seek to maximize their preparedness through security education and ways to change, or improve, behaviors of employees, citizens and customers. This need, coupled with increased mobility, cloud solutions and Internet of Things, requires security professionals to identify and manage the increasing impact employee behavior has on security and risk management effectiveness. Our Platinum and Diamond Level Sponsors will impart valuable information on how their organizations are reducing cyber risk through awareness and training.<br>**Moderator:** *Rajiv Das,* Chief Security Officer and Deputy Director, State of Michigan Department of Technology, Management and Budget (DTMB)<br>**Speaker:** *Michael R. Singer,* AVP-Technology Security, AT&T<br>**Speaker**: *James L. Turgal, Jr.,* Managing Director, Cyber Risk Services, Deloitte & Touche LLP<br>**Speaker**: *Keith Wojcieszek* , Associate Managing Director, Cyber Security and Investigations, North America, Kroll<br>**Speaker**: *Ron Zalkind* , Cisco, Founder & CTO of Cloudlock |
| 10:30 AM | **Networking Break, Visit with Sponsors and Transition to Breakout Sessions** |
| 11:00 AM | **Breakout Sessions -** Attendees may choose one session to attend during each of the breakout sessions. |

**Title**: Security Analytics and Orchestration

**Description**: According to Ponemon Institute data, the typical security team can only respond to 1 out of every 25 critical alerts that their 70-100 security tools generate. That makes prioritizing those alerts extremely critical. In order to do that successfully, security teams need to translate insight into action. They need to enrich the incident data with as much context as possible, enabling responders to make the right calls when choosing which incidents to work on.

This is why Security Analytics and Orchestration systems are critical in creating an efficient and effective immune system for your organization.

The presentation will provide insight and dialogue around available orchestration and analytics technologies along with strengths and challenges of leading approaches.

**Speaker**: *Rebecca Harvey* , Information Security Specialist, Data Strategy

---

**Title**: Cognitive Cybersecurity: Concepts and Practices

**Description**: The evolving landscape of cybersecurity threats is outpacing humans' ability to properly harness and process data, especially in critical infrastructure environments. This session will discuss how cognitive computing and machine learning can be applied to impact the discovery, understanding and mitigation of these threats, including across IT/OT environments.

**Speaker**:

*Bob Kalka* , Vice President - Technical Professionals, Strategic Client Initiatives, and Field Enablement, IBM

---

**Title**: Security: The Economics of IT Security - Optimizing Security Decisions

**Description**: Spending "whatever it takes" to "stay off the front page of the Wall Street Journal" is an emotional response to an operational problem. It is also unsustainable. The ambiguities associated with risk and loss create large problems for enterprises and fosters bad decisions full of cognitive bias. This session shows how to understand the concepts of technology risk management to make better decisions about IT security. It will also assist IT and LOB executives in understanding the concepts and frameworks of risk so they can make better decisions.

**Speaker**:

*Pete Lindstrom* , Research Vice President for Security Strategies, IDC

| | |
|---|---|
| | **Title**: Improving Healthcare Security and Patient Safety with U.M.B.R.E.L.L.A.<br><br>**Description**: We examine the challenges surrounding patient identification, interoperability, exchange of health records, and complexities in providing a robust security system capable of protecting patient identifiable information and present new solution regarding the identification of patients and medical personnel using a touchless form of biometrics and demonstrating its capabilities in a large-scale healthcare architecture. We call our solution U.M.B.R.E.L.L.A. or Unique Medical Biometric Recognition Enforcement of Legitimate and Large-scale Authentication. Our goal for U.M.B.R.E.L.L.A is to assist in reducing the complexities associated with user misidentification in healthcare and enhance the interoperability and security mechanisms affiliated with health data exchange, resulting in lowering healthcare costs, improving patient safety, and enhancing population health management and transition of care.<br><br>**Speaker**:<br>Dr. *Guy Hembroff* , *PhD* , Associate Professor of Medical Iformatics and Director of ICC Cybersecurity Center, Michigan Technological University |
| | **Title**: Challenges and Trends: Addressing Security Vulnerabilities in the Internet of Things<br><br>**Description**: Presentation of an overview of findings related to what is being captured, stored, and distributed by active and passive data collection with Internet of Things (IoT) devices including home appliances and personal assistants such as the Amazon Echo and smartphones. In addition to the privacy issues we will describe the challenges of cyber defense in the Internet of Things environment and how security practices and incident response are not scalable or effective in their present forms.<br><br>**Speaker**:<br>*Greg Gogolin, PhD* , Professor, Ferris State University |
| | **Title:** Cyber Range - Annual International Invitation Cyber Competition<br><br>**Description**:  The International Cyber Exercise is a multi-team event that challenges the offensive and defensive cybersecurity skills of its participants. This year, teams from fourteen states and fourteen countries will face off in Alphaville, the virtual training environment created by the Michigan Cyber Range. Using open source tools and their own skills, teams will compete to control as many of Alphaville's network assets as possible. This event requires a high degree of group skill, as they will have to protect the devices they control while attacking other teams. The team controlling the most devices at the end of the day is declared the winner. |
| 11:55 AM | **Luncheon and Presentation of the High School Cyber Challenge Awards by Governor Rick Snyder** |

| | |
|---|---|
| 1:00 PM | **Keynote Presentation -** Public Private Partnerships in Cybersecurity<br>**Description**: In his keynote address, the U.S. Deputy Attorney General will describe the cybersecurity threat that confronts our nation and explain how law enforcement, with the cooperation of private industry, can help. He will also address some of the challenges that law enforcement faces in this area. Finally, he will touch upon ways that private industry can work with law enforcement to protect itself, and to help deter and disrupt cyber criminals.<br>**Speaker:** *Rod J. Rosenstein* , United States Deputy Attorney General, United States Department of Justice |
| 1:20 PM | **Title:** Critical Success Factors for Today's Information Security Programs<br>**Description:** Organizations are rapidly adopting cloud, cognitive and block chain technology to improve their organizations competitive advantage. While these technologies are transformative in nature, they also introduce significant changes and possible risks to information security programs. This presentation will discuss the impact of these technologies on infosec programs and what needs to be considered in order to be successful with these technologies.<br>**Speaker:** *David A. Cass* , IBM Global Partner Cloud Security Services &<br>Chief Information Security Officer Cloud & SaaS Operations |
| 1:40 PM | **Title:** The State of Aviation Cybersecurity: Critical Infrastructure's Need for Public Assistance<br>**Description:** Commercial aviation is classified by the US Government as Critical Infrastructure under the Transportation Systems sector. This session will take a look at the current state of cybersecurity in the Airline industry, focusing on where we are and where we need to go. It will also touch upon public/private sector partnerships and how both sides can benefit from working together on cybersecurity initiatives.<br>**Speaker:** *Julie Porro* , Chief Information Security Officer (CISO), JetBlue |
| 2:00 PM | **Federal Panel Discussion:** Cyber Threat Information Sharing<br>**Description:** The topic of the federal panel discussion will focus on cybersecurity threat intelligence sharing. This panel will bring together federal officials and policy makers to identify ways in which cybersecurity threat intelligence sharing may be enhanced to promote improved cybersecurity preparedness. Cybersecurity threat intelligence sharing has been, and continues to be, a significant topic of conversation at the gubernatorial, state and federal levels.<br>**Moderator:** *Timothy Blute* , Program Director, National Governors Association (NGA)<br>**Panelist(s):**<br>*Jason Bilnoski* , Supervisory Special Agent (SSA), Federal Bureau of Investigation (FBI) Detroit Division<br>*Guy M. Walsh* , Brigadier General (Ret), Strategic Initiatives, United States Cyber Command<br>*Bradford Willke* , Chief, CSA Field Operations, Office of Cybersecurity & Communications, Department of Homeland Security |
| 2:30 PM | **Featured Presentation:** Future Threats and Challenges in the Cyber Space<br>Join Rami Efrati in expert in cyber technology strategic methods in discussing current issues in cybersecurity.<br>**Speaker:** *Rami Efrati* , Former Head, Civilian Department of Cyber Bureau and Associate, ICT, IDC, Herzliya Israel |
| 2:45 PM | **Networking Break, Visit with Sponsors and Transition to Breakout Sessions** |

| 3:10 PM | **Breakout Sessions** - Attendees may choose one session to attend during each of the breakout sessions. |
|---|---|
| | **Title**: Strategic Challenges in Implementing Integrated Cyber Defenses<br>**Description**: According to Symantec's 2017 Internet Security Threat Report, although many CIOs believe they only have 30-40 cloud aps operating in their environments in reality they often have over 1,000.  How then can organizations protect themselves in the face of such "shadow clouds" and other hidden threats?  This session will explore these and other challenges facing organizations in implementing an integrated cyber defense program.<br>**Speaker**:<br>*Thomas MacLellan* , Director, Government Affairs & Policy, Symantec Corporation |
| | **Title**: Combatting Cyber Crime: Changes to the Cybersecurity Program are Needed to Address the New Normal<br>**Description**: Cyber Crime is on the rise and the associated costs are skyrocketing. Accenture and Ponemon Institute collaborated to identify the real costs organizations incur as a direct relation to cyber crime annually.  We'll share our findings from this newly published research – which includes some quite provocative insights.  From those insights, we'll also explore new perspectives – programmatic and associated technology – to address the "New Normal" of combatting advanced cyber adversaries.<br>**Speaker**:<br>*Kevin Richards* , Managing Director, Accenture |
| | **Title**: Invasion of the Zero Days<br>**Description**: With Cyber Security there's zero day vulnerabilities popping up all the time. Now to add to it, there are zero day vulnerabilities all around us. Criminals are always coming up with new and creative methods to hack into every day devices. We on the other side have to do our best to prevent and recover from these events.<br>**Speaker**:<br>*Luke Thelen* , Incident Response Specialist, Michigan State Police |
| | **Title**: Cybersecurity as a Growth Advantage, Empowering Digital Transformation<br>**Description**: Cybersecurity can be an enabler that supports innovation and helps organizations move forward with their digital transformations. This session will cover how to present Cybersecurity as a critical link to digitalization, thus providing the foundation for the business strategy.<br>**Speaker**:<br>*Guillermo Guerra* , Vice-President & CISO, Jackson National Life |

| | |
|---|---|
| | **Title**: When it Rains, It Pours: How Data Breaches Can Get You Sued, and What to Do About It<br>**Description**: This presentation examines the risk of civil liability stemming from data breaches and cyber-attacks. Companies themselves are not the only ones at risk of lawsuits - officers and directors are facing personal liability for not having done enough to oversee cybersecurity. We will demonstrate the potential risks and help businesses understand the types of practices courts have deemed negligent as well as shedding light on the standards companies must meet to avoid liability and help insulate their operations from financial exposure.<br>**Speakers**:<br>*Katherine L. Pullen* , Associate, Warner Norcross & Judd<br>*Brian D. Wassom* , Partner and Chair, Privacy and Cybersecurity Litigation Group, Warner Norcross Judd LLP |
| | **Title:** Cyber Range - Annual International Invitation Cyber Competition<br>**Description**:  The International Cyber Exercise is a multi-team event that challenges the offensive and defensive cybersecurity skills of its participants. This year, teams from fourteen states and fourteen countries will face off in Alphaville, the virtual training environment created by the Michigan Cyber Range. Using open source tools and their own skills, teams will compete to control as many of Alphaville's network assets as possible. This event requires a high degree of group skill, as they will have to protect the devices they control while attacking other teams. The team controlling the most devices at the end of the day is declared the winner. |
| 3:55 PM | **Networking Break and Visit with Sponsors** |
| 4:05 PM | **Breakout Sessions -** Attendees may choose one session to attend during each of the breakout sessions. |
| | **Title**: Werewolves and Silver Bullets, Vampires and Holy Water, Hackers and Encryption<br>**Description**: Encryption, as with any security tactic, quickly becomes complex and diffuse without a unifying strategy. The question of how it protects the organization's mission must be answered. And what about threats and criminal activities? This session details how to identify and document the business processes, convert threat intelligence into actionable threat models, and strategically deploy encryption.<br>**Speaker**:<br>*J. Wolfgang Goerlich* , VP, Strategic Security Programs,  CBI |

| | |
|---|---|
| | **Title**: Third Party Risk Management 2.0: Continuous Monitoring Exposes Blind Spots<br><br>**Description**: Third-party risk is an important cybersecurity dimension that needs to play a bigger role in supply chain and cybersecurity decisions. This session will cover the impact of third-party cybersecurity risks, how third-party risk management systems work, how continuous monitoring works and what type of information it provides, how analytics work to provide better breach response, and how future of combining third-party management with existing IT and operational technology security solutions.<br><br>**Speaker**:<br>Juliet Okafor, JD, VP of Global Business Development, Fortress Information Security |
| | **Title**: The Human Factor in Cyber Security: Insider Threats<br><br>**Description**: This presentation will include an overview of a cyber breach caused by an insider and how an insider threat program that includes a strong employee communication platform could have prevented the incident. We will also discuss how to engage your Board of Directors to secure their active support for your Insider Threat program.<br><br>**Speakers**:<br>*Scott LaVictor* , CEO, Arbor Insight<br>*Thys DeBruyn* , Owner and President, Advance Resources and Consulting<br>*Jay R. Taylor* , CEO, EagleNext Advisors |
| | **Title**: Cyber Intrusion and Data Breaches of State, Local, Tribal and Territorial (SLTT) Government Entities<br><br>**Description**: Due to an increase in cyberattacks targeting law enforcement, NW3C began compiling a dataset of all reported cases involving state, local, tribal and territorial (SLTT) government entities. The presentation describes the variety of types of data breaches and examines the vulnerability of SLTT law enforcement compared to the rest of the government sector. It also covers the monetary and non-monetary costs associated with failing to properly safeguard computer information systems, infrastructures and computer networks.<br>The presentation will:<br>• Raise awareness of the threats facing law enforcement and government entities involving data breaches and cyber intrusions<br>• Provide information on the variety of types and causes of harmful data breaches<br>• Identify prevention methodologies to put in place to avoid becoming a victim<br>• Explain how NW3C can help agencies prepare and take proactive approach to prevent possible cyber intrusion and the resources available.<br><br>**Speaker**:<br>*Glen B. Gainer, III* , President and CEO, National White Collar Crime Center (NW3C) |

| | |
|---|---|
| | **Title:** Cyber Range - Annual International Invitation Cyber Competition<br><br>**Description**:  The International Cyber Exercise is a multi-team event that challenges the offensive and defensive cybersecurity skills of its participants. This year, teams from fourteen states and fourteen countries will face off in Alphaville, the virtual training environment created by the Michigan Cyber Range. Using open source tools and their own skills, teams will compete to control as many of Alphaville's network assets as possible. This event requires a high degree of group skill, as they will have to protect the devices they control while attacking other teams. The team controlling the most devices at the end of the day is declared the winner. |
| 4:50 PM | **Adjournment** |