Second Annual Cybersecurity Summit

May 24, 2018

Francis Marion Hotel
387 King Street
Charleston, SC 29403

8:30 a.m. – 9:00 a.m. **Registration and Breakfast Networking**

9:00 a.m.–9:30 a.m. **Welcoming Remarks**
Christopher D. Roberti, Senior Vice President, Cyber, Intelligence, and Security Division, U.S. Chamber of Commerce (M.C.)
The Honorable John Tecklenburg, Mayor, City of Charleston

9:30 a.m.–10:00 a.m. **Morning Keynote: Role of the FBI in Cybersecurity**
Howard Marshall, Deputy Assistant Director, Cyber Division, FBI

This isn't your typical law enforcement briefing. Howard Marshall puts the business threat in plain language to enlighten you regardless of your level of technical proficiency. Marshall has become a sought-after speaker for his briefings that provide key insights based on case studies and analysis of current and emerging cyber threats to U.S. companies. His presentation will demonstrate why every business, big or small, needs a plan and ongoing vigilance, and he provides the resources to get started.

10:00 a.m.–10:45 a.m. **Panel Discussion: Small Business Cybersecurity**
Moderator: David Furr, Of Counsel, Gray, Layton, Kersh, Solomon, Furr & Smith, P.A.

- **Steve Flowers**, President, Dragoon Security
- **Brian Heffner**, Security Engineer, Check Point Software Technologies
- **Charles Johnson**, Chief Executive Officer, EDTS Cyber, LLC
- **Pete Seeber**, CEO and Co-Founder, Rocus Networks

Small doesn't necessarily mean secure. More and more, small and midsize businesses are targeted for cyberattacks because they typically lack the resources to adequately defend themselves. Cybersecurity is no longer an IT problem; it's an organizational problem. Solutions are often both challenging and expensive and exceed the budgets of smaller organizations. So how do businesses find a balance between cost and security? What resources exist for businesses to enhance cybersecurity? This panel will provide an overview of existing frameworks and advice on finding affordable solutions to cybersecurity challenges.

10:45 a.m.-11:15 a.m. **Advanced Threat Landscape**
David Durko, CEO and Chief Compliance Officer, Security Validation, LLC and SecValMSP, LLC
Sponsored by Intellectual Capitol

David Durko, who has a deep background in information technology security, compliance, and incident/risk management for Wyndham Hotel Group International and MasterCard Worldwide, will provide an overview of the threat landscape, a review of various defense strategies, and a review of return on investment in security.

11:15 a.m.–11:30 a.m. **Room Change Break**

11:30 a.m.–12:15 p.m. **Panel Discussion: Community Cyber Defense for the Port**
Moderator: Mark Lester, Chief Information Security Officer, South Carolina Ports Authority

- **Pat Barber,** Private Terminal Manager, Carver Maritime, LLC
- **Mike Riggs,** CISSP, Director of Avian Evangelism, Perch Security
- **Anna Thies**, Director of Operations, The Maritime Association of South Carolina
- **Cdr. Nicholas Wong,** Deputy Commander, Coast Guard Sector Charleston

Cybercrime has centered on financial services for the simple reason that that's where the money is. However, that's changing. Ports, as hubs of both physical and digital activity, have been getting more attention from bad guys. There have been attacks that have shut down ports, diverted cargo, and spoofed GPS systems. Many interdependent companies look to the ports for their economic success, and they are recognizing that their security posture is tied closely to others in the port supply chain. The Maritime Association of South Carolina is on the forefront of preparing for large and small cyberattacks by forming an Information Sharing and Analysis Organization (ISAO), or simply a community cyber defense. In this session, participants will hear from the team that is putting the program together, how the program will strengthen cybersecurity, reduce risk, and how others can get involved.

12:15 p.m.–12:30 p.m. **Room Change Break**

12:30 p.m.–1:30 p.m. **Luncheon**

Welcoming Remarks
Ted Pitts, President and Chief Executive Officer, South Carolina Chamber of Commerce

Luncheon Keynote: Combating Cyber Threats to U.S. National Security
Gen. Michael Hayden, USAF (Ret.), former Director of the CIA and NSA and Principal, The Chertoff Group

U.S. businesses face blended threats—criminal and national security—to their digital networks. In today's interconnected economy, industry is a key partner in confronting these threats. A seemingly small cyber intrusion by a criminal actor on a U.S. business may transmit personally identifiable information to a terrorist network or fund militant activity on battlefields far from U.S. jurisdiction. Gen. Michael Hayden will discuss these cyber threats and actors and how critical cooperation between businesses and federal agencies works to disrupt cyberattacks.

1:30 p.m.–1:45 p.m. **Networking Break**

1:45 p.m.–2:30 p.m. **The "S" in IoT Stands for Security**

Moderator: Bess K. Hinson, Associate, Morris, Manning & Martin, LLP

- **Nelson Hastings,** Project Leader, Applied Cybersecurity Division, National Institute of Standards and Technology, U.S. Department of Commerce
- **James O'Dell,** Senior Security Strategist, AT&T
- **Mark Pelletier**, Vice President, Scientific Research Corporation
- **Trent Salvaggio**, Ph.D., Executive Director, IoT Talent Consortium

A cybersecurity storm is brewing over the rapid adoption of the consumerization of the Internet of Things. The implications to critical infrastructure and national security are enormous when such a high volume of these consumer devices are so easily hacked. Are we doing the right things to prepare? This panel will share real-world data and how lessons learned from industry can influence our approach to combating the coming storm.

2:30 p.m.–3:15 p.m. **LIVE HACK: How Not to Code and Build IoT Devices and Deal with Responsible Disclosure**

Mark Harrison, Consultant, Pen Test Partners

The world has woken up to the internet of things, but it is clear that the IoT has not woken up to its responsibilities. With every new product comes the risk that it will disclose private user data, provide an increased attack surface, and further enable mega DDoS attacks. Harrison will show you how hackers can abuse IoT devices because of poor standards and how some manufacturers attempt to dodge their responsibilities.

3:15 p.m.–3:30 p.m. **Networking Break**

3:30 p.m.–3:45 p.m. **Day of Cyber Winner, Industry Excellence, Academic Excellence, Government Excellence Awards Presentations**

Tom Scott, Executive Director, SC Cyber

3:45 p.m.–4:00 p.m. **SC Cyber: A Change Engine for the Software Defined Economy**

MG (USA Ret.) Les Eisner, Founder, SC Cyber

4:00 p.m. **Closing Remarks**

Christopher D. Roberti, Senior Vice President, Cyber, Intelligence, and Security Division, U.S. Chamber of Commerce (M.C.)