2015 Cybersecurity Conference

December 15, 2015, 7:00 a.m.–2:00 p.m.

Sheraton Imperial RTP | Imperial Ballroom | 4700 Emperor Blvd | Durham, NC 27703

7:00—8:00 REGISTRATION AND NETWORKING BREAKFAST

8:00—8:15 WELCOMING REMARKS

- **Lew Ebert**, President and CEO, North Carolina Chamber of Commerce (confirmed)
- **Ann M. Beauchesne**, Senior Vice President, U.S. Chamber of Commerce (emcee)

8:15—8:45 MORNING KEYNOTE: ROLE OF DHS IN CYBERSECURITY

Russell C. Deyo, Under Secretary for Management, Department of Homeland Security (confirmed)

Cybersecurity is a top priority for DHS. Cyber threats are increasing in frequency, scale, and sophistication. Cybersecurity must be a partnership between government and industry. Deyo will discuss how DHS executes its mission as the central federal interface for the private sector in responding to and recovering from cyber threats. Deyo will also detail how DHS is improving and expanding its capability to send and receive cyber threat information to the private sector.

8:45—9:00 ELECTRIC SECTOR PERSPECTIVES ON CYBERSECURITY

A.R. Mullinax, Executive Vice President, Strategic Services, Duke Energy (confirmed)

The power grid is a complex, interconnected network that can be vulnerable to cyber and physical attacks. Mullinax will talk about Duke Energy's efforts to safeguard the electric grid by investing in tools, technology, and talent to create more resilient networks, promote robust information sharing in the electric sector and with government partners, and develop incident response plans.

9:00—9:45 PANEL DISCUSSION: RISKS, COSTS, DISPUTES, AND LITIGATION

Moderator: Alicia A. Gilleskie, Partner, Smith Anderson

- **Jackson W. Moore**, Partner, Smith Anderson
- **John H. Jo**, Partner, Smith Anderson
- **Alex Pearce**, Privacy Counsel, SAS Institute Inc.

A few years ago, cyberattacks against the government and corporations were on the margins of news stories. But after the attacks waged against major corporations and OPM, people realize that these attacks are no joke. Have you considered your organization's legal exposure? A panel of experts will discuss the costs of a breach or potential breach, the data regulatory landscape and possible regulator fines and penalties, and steps for planning, responding to, and mitigating the effects of a breach.

9:45—10:05 CYBER THREATS TO U.S. BUSINESSES

Denise Anderson, Executive Director, NH-ISAC (invited)

Nation-states, or their proxies, and cyber criminals steal our login credentials, payment card data, trade secrets, and much more on a daily basis. Cybercrime costs the global economy about $445 billion in a typical year. Aside from the monetary costs, businesses risk loss of consumer confidence and reputation. Krebs will talk about these threats and why businesses of all sizes need to adopt basic Internet security practices to reduce their network weaknesses and make the price of successful hacking steep.

10:05—10:20 **NETWORKING BREAK**

10:20—10:40 **PROTECTING YOUR CYBER NETWORK USING THE NIST FRAMEWORK**
Adam Sedgewick, Senior Information Technology Policy Advisor, National Institute of Standards and Technology (confirmed)

Cybersecurity experts often say that there are two types of businesses—those that have been hacked and know it, and those that have been hacked and don't know it yet. In 2014, the National Institute of Standards and Technology (NIST) released a cybersecurity framework to help businesses start a cybersecurity program or improve an existing one. Sedgewick will discuss best practices to help early users of the framework better understand it, give business owners tools and tips for strengthening a cybersecurity program, and explore ways to communicate about cyber with small and midsize supply chain partners.

10:40—11:25 **SECURING THE CYBER SUPPLY CHAIN PANEL**
Moderator: Bradley Hayes, Director, U.S. Chamber of Commerce (confirmed)
- **John Cassidy**, Branch Director, Cybersecurity Division, CenturyLink (confirmed)
- **Terrell Garren**, Vice President and Chief Security Officer, Duke Energy (confirmed)
- **Joe Jarzombek**, Director of Software & Supply Chain Assurance, Office of Cybersecurity & Communications, National Protection & Programs Directorate, U.S. Department of Homeland Security (confirmed)

Risks to the supply chain can take multiple forms (e.g., natural, accidental, financial, cyber). However, there are a wide variety of both public- and private-sector efforts under way to manage cyber supply chain risk, which is an emerging and complex area. This panel will examine what malicious actors seeking to get access to (and do) once inside a company's network, what steps—from basic to more sophisticated—most businesses can undertake to guard their cyber supply chains, and the importance of timely cyber threat information sharing.

11:25—11:55 **LAW ENFORCEMENT ENGAGEMENT**
Moderator: Bradley Hayes, Director, U.S. Chamber of Commerce (confirmed)
- **Stanley Crowder**, Special Agent, U.S. Secret Service (confirmed)
- **Jessica Nye**, Supervisory Special Agent, Federal Bureau of Investigation (confirmed)

The FBI and the Secret Service are often the first entities to learn of criminals' access to company networks. The U.S. Chamber engages law enforcement to build trusted public-private relationships, which are essential to confirming a crime and beginning a criminal investigation. This panel will discuss the respective roles of the FBI and the Secret Service, how law enforcement shares cyber threat data with businesses, and the importance of reporting cyber incidents to law enforcement.

11:55—12:10 **NETWORKING BREAK**

12:10—1:10 **LUNCHEON KEYNOTE: EMERGING CYBER THREATS TO U.S. NATIONAL & ECONOMIC SECURITY**
James Comey, Director, Federal Bureau of Investigation (invited)

The growing number of serious attacks on essential cyber networks is one of the most serious economic and national security threats our nation faces. FBI Director Comey will discuss the evolving cybersecurity threat and the tools and resources the Bureau is utilizing to combat the threat.

1:10 – 1:25 **A DECADE OF DATA BREACHES – WHERE ARE WE NOW?**
Alicia A. Gilleskie, Partner, Smith Anderson

1:25 – 1:55 **EVOLUTION OF CYBERSECURITY IN UNIVERSITIES AND HIGHER EDUCATION PANEL**
Moderator: Yi Deng, Ph.D., Dean and Professor, UNC Charlotte, College of Computing & Informatics (confirmed)

- **Richard Biever**, Chief Information Security Officer, Duke University (confirmed)
- **Douglas Reeves**, Professor of Computer Science, Associate Dean of Graduate Programs for College of Engineering, North Carolina State University Department of Computer Science (confirmed)
- **Daniel Stein**, National Cybersecurity Training and Education Program Director, Office of Cybersecurity & Communications, National Protection & Programs Directorate, U.S. Department of Homeland Security (confirmed)

Many experts believe that technology alone can not solve cybersecurity. Products and solutions are regularly brought to market to address emerging threats, and the private sector is sharing best practices across sectors. The question now is about people. How are educational institutions building programs to funnel more talent into the pipeline, and how are colleges and universities recruiting students to these programs.

1:55 – 2:00 **CLOSING REMARKS**
Ann M. Beauchesne, Senior Vice President, U.S. Chamber of Commerce

Presenting Sponsors

DUKE ENERGY®

SMITH ANDERSON

Co-Hosts

North Carolina Chamber
A force for business.

U.S. CHAMBER OF COMMERCE

Strategic Partner

CARY CHAMBER OF COMMERCE

NCRMA EST. 1902
NC Retail Merchants Association