FOR IMMEDIATE RELEASE

The National Cyber Security Alliance and Nasdaq Host Timely, Enterprise-focused Discussion about Cybersecurity Risk Management and Emerging Threats

Maureen K. Ohlhausen, Acting Chairman of the Federal Trade Commission, conducts fireside chat followed by two panels led by industry experts.

WASHINGTON, D.C., March 13, 2017 – Today at the Nasdaq MarketSite in New York City, leadership from the National Cyber Security Alliance (NCSA) and Nasdaq will conduct a fireside chat with Acting Federal Trade Commission (FTC) Chairman Maureen K. Ohlhausen. Acting Chairman Ohlhausen will share the FTC's approach to cybersecurity along with insights about likely priorities for the Trump administration. Immediately following her talk, two panels of industry experts will provide insight into emerging cybersecurity threats and address how businesses can normalize a culture of strong cybersecurity over time.

There is a growing understanding that cybersecurity is an enterprise-wide issue – touching legal, reputational, operational and regulatory risks. Yet senior executives face complex challenges balancing business decisions and cybersecurity without a full understanding of how to strategically manage enterprise-wide cybersecurity risks and effectively communicate those risks to employees. All organizations need to identify and implement strategies that work for their company's structure, create and adhere to a cybersecurity plan and empower all employees to be safe and secure online. Today's discussions will delve into how to build a strategic approach to and culture of cybersecurity across the enterprise with a focus on the role of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, emerging trends in risk mitigation and best practices for senior leaders. This event is the first in a series of three slated for 2017 that will tackle timely and relevant cybersecurity topics critical to the business world**.**

"No matter the industry or size of the company, having adequate cybersecurity is essential. NCSA strongly recommends establishing a culture of cybersecurity in the workplace. Leadership is critical, and building off the basics – identifying the critical information, protecting it and having a plan if something goes wrong – is the starting point," said Michael Kaiser, NCSA's executive director. "Organizations focusing on their resistance and resilience from cyber threats will be the best prepared."

The first panel, *Policy to Practice: Operationalizing a Strategic Approach to Cybersecurity Risk Management*, moderated by Jason Crabtree, co-founder and CEO, Fractal Industries, will discuss approaches and key strategies for managing cyber risk. Panelists include Todd Thibodeaux, president and CEO at CompTIA; Virginia Gambale, managing partner of Azimuth Partners, LLC and Colleen Valentine, senior manager, Information Security Group at Nasdaq.

"It's an economic and societal imperative to train and certify hundreds of thousands of IT professionals with the analytical skills they need to address the complexity and diversity of threats as they multiply," said CompTIA President and CEO Todd Thibodeaux**.** One of the key ways to improve risk management is to train more professionals. CompTIA is acutely aware of the shortage of qualified cybersecurity specialists and has an innovative tool, CyberSeek, which is designed to provide policy makers, employers and security professionals with greater visibility into the demand for cybersecurity professionals nationwide. CyberSeek was created in partnership using labor market analytics from Burning Glass Technologies and NIST.

The *Policy to Practice* panel will immediately follow with a well-timed discussion about *Emerging Trends: Cybersecurity Threats in 2017.* Moderated by Howard Edelstein, chairman of Biocatch, panelists include Scott Behm, vice president for Information Security at LifeLock, a Symantec company; Jonathan Goldberger, director, Advanced Security Services at Cisco; Mike Viscuso, CTO and co-founder of Carbon Black and Alex Mosher, vice president of Cyber Security at CA Technologies. This panel will focus on a variety of issues regarding cybersecurity threats facing businesses today.

"Maintaining customer trust is vital in today's fast-paced business environment," said Anthony Grieco, senior director and trust strategy officer, Cisco. "With the understanding that there will always be budget and talent constraints, businesses must focus on relentless improvement measured via efficacy, cost and well-managed risk. Security must be every organization's priority – with commitments to training, evaluating the effectiveness of cybersecurity investments, and investing in the best safeguards to minimize risk against current and emerging threats."

"Identity fraud is a widespread problem, affecting more than 15 million Americans in 2016," said Neil Daswani, chief information security officer at LifeLock, a Symantec company. "Fraudsters are growing more sophisticated even as defense systems improve, so educating consumers about safer behavior online is more relevant than ever."

Resources

NCSA: NCSA's Technology Checklist for Businesses will help you identify the technology your business needs to protect, and shares basic security tips, considerations and resources that can assist in detecting, responding to and recovering from cyber incidents.

U.S. Department of Homeland Security:

- The DHS C³ Voluntary Program helps organizations of all sizes combat the cyber threat. This no-cost program helps industry improve their cyber resilience by promoting awareness and use of the National Institute for Standards and Technology Cybersecurity Framework. Please visit www.us-cert.gov/ccubedvp for more information.
- NICCS Portal: The National Initiative for Cybersecurity Careers & Studies (NICCS) Portal is the nation's premier website for cybersecurity workforce development, careers, and studies. It is an online resource for cybersecurity training that connects industry with cybersecurity training providers throughout the nation. Currently, with over 3,000 courses listed, organizations can utilize this tool to locate various cybersecurity courses in one's area and keep cybersecurity skills and knowledge current and relevant to an evolving career field. Visit the NICCS Portal at www.niccs.us-cert.gov.
- Cybersecurity Questions for CEOs Tip Card provides key questions to guide leadership discussions about cybersecurity risk management for companies, along with key cyber risk management concepts. You can find this resource as well as others in the DHS Stop.Think.Connect. Campaign's Toolkit for Industry at wwww.dhs.gov/publication/stopthinkconnect-industry-resources.

Cisco: Cisco 2017 Annual Cybersecurity Report provides a complete overview of the latest cyber attacks and defensive measures, as well as the impact on business growth and success. It highlights the challenges and opportunities for security teams against the constant evolution of cybercrime and shifting attack methods.

Federal Trade Commission: From personal data on employment applications to network files with customers' credit card numbers, sensitive information pervades every part of many companies. Get your business up to speed on security basics with The Federal Trade Commission's Start with Security and Protecting Personal Information guides.

CompTIA: In February 2017, CompTIA unveiled a groundbreaking, vendor-neutral certification, CompTIA Cybersecurity Analyst (CSA+), the first of its kind to bring behavioral analytics to the forefront of assessing cyber threats. The CompTIA CSA+ certification will offer broad-spectrum validation of knowledge and skills required to configure and use cyber-threat detection tools, perform data analysis and interpret the results to identify vulnerabilities, threats and risks to an organization. It certifies knowledge of a data-driven approach to information security.

About the National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) is the nation's leading nonprofit, public-private partnership promoting cybersecurity and privacy education and awareness. NCSA works with the U.S. Department of Homeland Security (DHS) and NCSA's Board of Directors, which includes representatives from ADP; Aetna**;** AT&T Services, Inc.; Bank of America; Barclays; BlackBerry Corporation; CDK Global; Cisco; Comcast Corporation; ESET North America; Facebook; Google; Intel Corporation; LifeLock (a Symantec company); Logical Operations; Mastercard; Microsoft Corp.; NXP Semiconductors; PayPal; PKWARE; Raytheon; RSA, the Security Division of EMC; Salesforce; SANS Institute; Symantec; TeleSign and Visa Inc. NCSA's core efforts include National Cyber Security Awareness Month (October); Data Privacy Day (January 28) and STOP. THINK. CONNECT.™, the global online safety awareness and education campaign cofounded by NCSA and the Anti Phishing Working Group, with federal government leadership from DHS. For more information on NCSA, please visit staysafeonline.org/about-us/overview/.

Cisco, CompTIA and LifeLock (a Symantec company) are Platinum Sponsors and Fasoo and Logical Operations are Silver Sponsors for this inaugural 2017 NCSA and Nasdaq Cybersecurity Summit series. The Summit is also supported by the Business Council for International Understanding (BCIU), Business Executives for National Security (BENS) and the National Association of Corporate Directors (NACD).

Media Contact:
Jessica Beffa
720-413-4938
ncsa@thatcherandco.com