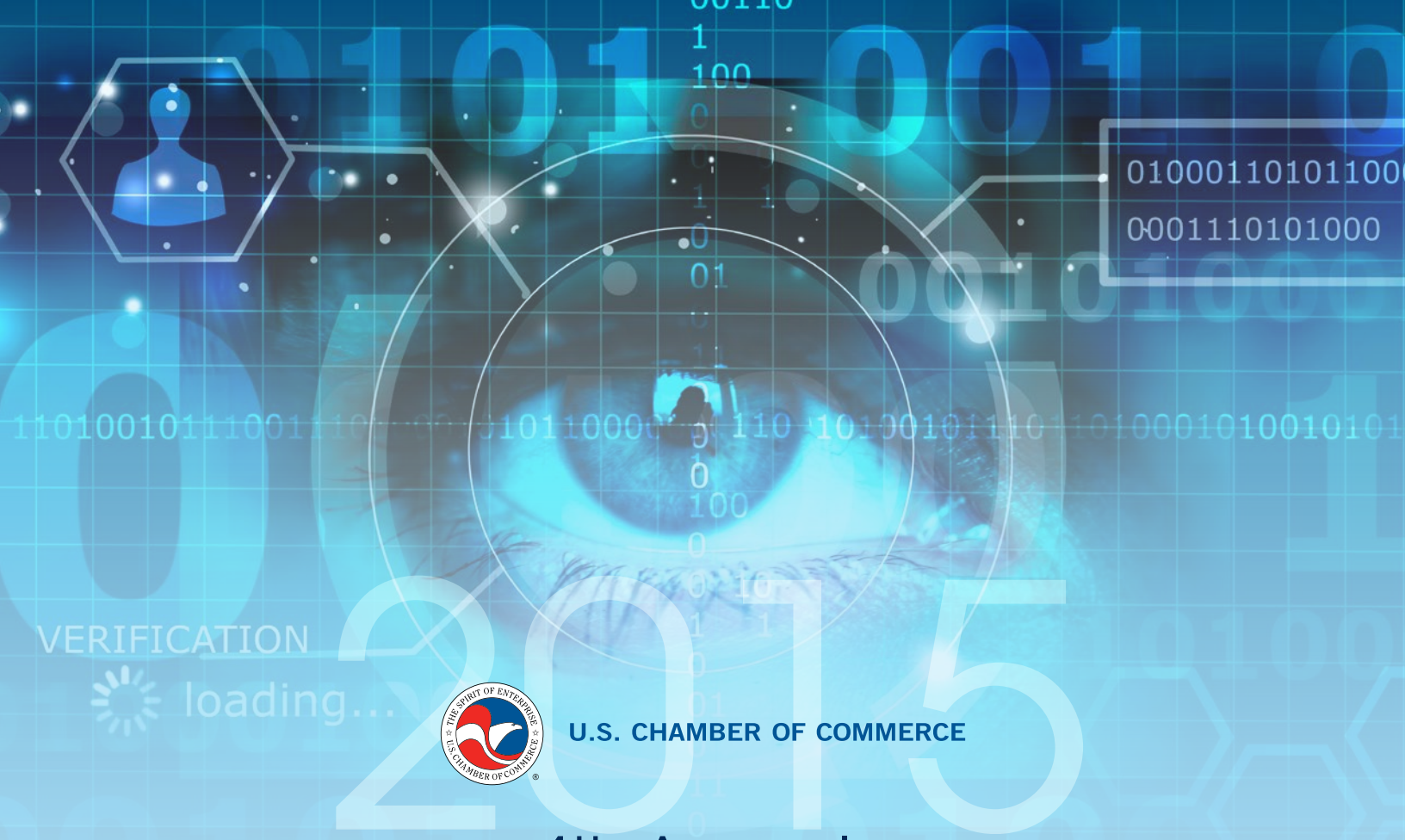

U.S. CHAMBER OF COMMERCE

4th Annual Cybersecurity Summit

October 6, 2015 • Washington, D.C.

Sponsored by:

American Express

ARMOR
BETWEEN YOU AND THE THREAT

CLEARFORCE

DELL

DELL SecureWorks

LIBERTY GROUP VENTURES

SOUTHERN COMPANY

www.cybersecurityadvocacy.com | #cyber15 | @Cybersecurity

National Cyber Security Awareness Month

Save These Dates:
Upcoming Chamber Cybersecurity Events

- **December 15**
  Durham, NC
- **March 10, 2016**
  Detroit, MI

Visit **www.cybersecurityadvocacy.com** to register and for more information.

U.S. CHAMBER OF COMMERCE

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

The U.S. Chamber of Commerce does not endorse any of the products or services associated with the campaign or mentioned in the brochure.

Cybersecurity Campaign

Improving Today. Protecting Tomorrow.™

U.S. CHAMBER OF COMMERCE

4th Annual Cybersecurity Summit

October 6, 2015 | Doors open: 8:30 a.m. | Program: 9:00 a.m.–4:00 p.m.
U.S. Chamber of Commerce | Hall of Flags | 1615 H Street, NW

AGENDA

8:30–8:50 a.m. — Registration and Networking Breakfast

8:50–9:00 a.m. — Welcoming Remarks
- **Ann Beauchesne,** Senior Vice President, U.S. Chamber of Commerce

9:00–9:20 a.m. — The State of Cybersecurity—An Assessment from the White House
- **Michael Daniel,** Special Assistant to the President & Cybersecurity Coordinator, White House

9:20–9:40 a.m. — Keynote Remarks: Role of DHS in Cybersecurity
- **Alejandro Mayorkas,** Deputy Secretary, U.S. Department of Homeland Security

9:40–9:55 a.m. — Security and Energy Sector Cyber Resiliency
- **Elizabeth Sherwood-Randall, Ph.D.,** Deputy Secretary, U.S. Department of Energy

9:55–10:15 a.m. — Industry Keynote Remarks
- **Tom Fanning,** Chairman, President and CEO, Southern Company

10:15–10:45 a.m. — Getting CISA Passed This Year: A Q&A with Senators Burr and Feinstein
- Moderator: **Matthew Eggers,** Senior Director, U.S. Chamber of Commerce
- **The Honorable Richard Burr,** Chair, Senate Select Committee on Intelligence
- **The Honorable Dianne Feinstein,** Vice Chair, Senate Select Committee on Intelligence

Cybersecurity Campaign

Improving Today. Protecting Tomorrow.™

10:45–11:00 a.m.	Networking Break
11:00–11:45 a.m.	Managing Cybersecurity in the C-Suite • Moderator: **Matthew Eggers,** Senior Director, U.S. Chamber of Commerce • **Mike Cote,** Vice President and General Manager, Dell SecureWorks • **Sean Franklin,** Vice President, Cyber Intelligence, American Express • **Stan Harrell,** Senior Vice President, Chief Financial Officer & Chief Information Officer, U.S. Chamber of Commerce • **Dave McCurdy,** President and Chief Executive Officer, American Gas Association • **Kiersten Todt,** President and Managing Partner, Liberty Group Ventures
11:45 a.m.–12:15 p.m.	Networking Break
12:15–1:30 p.m.	Luncheon Keynote Address: Combating Cyber Threats to U.S. National Security • **General James L. Jones,** Former National Security Advisor to the President of the United States
1:30–2:15 p.m.	The International Dynamic: Global Approaches to Cybersecurity Policy, Partnerships, and Innovation Panel • Moderator: **Adam Sedgewick,** Senior Information Technology Policy Advisor, National Institute of Standards and Technology, U.S. Department of Commerce • **Liesyl I. Franz,** Senior Policy Advisor, Office of the Coordinator for Cyber Issues, U.S. Department of State • **John Miller,** Global Cybersecurity Policy, Information Technology Industry Council • **Katie Moussouris,** Chief Policy Officer, HackerOne • **Paula Tolliver,** Chief Information Officer and Corporate Vice President of Business Services, The Dow Chemical Company • **Andy Williams,** Cyber Envoy, Embassy of the United Kingdom
2:15–2:30 p.m.	Networking Break

2:30–3:00 p.m.

Sharing Cyber Threat Information to Protect Business and America

- **Lieutenant General James K. McLaughlin,** Deputy Commander, United States Cyber Command

3:00–3:45 p.m.

Strengthening Cybersecurity Together: Sector Cooperation, Interdependencies, and Challenges Panel

- Moderator: **Bradley Hayes,** Director, U.S. Chamber of Commerce
- **Steve Harris,** Vice President and General Manager, Dell Inc.
- **Jeff Schilling,** Chief of Customer Operations and Security, Armor
- **The Honorable Phyllis A. Schneck, Ph.D.,** Deputy Under Secretary for Cybersecurity and Communications, U.S. Department of Homeland Security
- **Jim Trainor,** Acting Assistant Director Cyber Division, Federal Bureau of Investigation

3:45 p.m.

Closing Remarks

- **Ann Beauchesne,** Senior Vice President, U.S. Chamber of Commerce

Cybersecurity Campaign

Improving Today. Protecting Tomorrow.™

THANK YOU

The U.S. Chamber thanks the following companies for sponsoring the Cybersecurity Summit in Washington, D.C.

Sponsors

American Express

ARMOR
BETWEEN YOU AND THE THREAT

CLEARFORCE

DELL

DELL SecureWorks

LIBERTY GROUP VENTURES

SOUTHERN COMPANY

Partner

National Cyber Security Awareness Month

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. The framework was developed in collaboration with public and private organizations, including companies, trade associations, and the U.S. Chamber's Cybersecurity Working Group.

The framework features a number of industry-vetted actions that businesses can take to assess and strengthen their state of security over time. It provides organizations—including their customers, partners, and suppliers—with common language for understanding their current cybersecurity posture, setting goals for cybersecurity improvements, and much more.

Hackers Can Hack Anywhere

Even though Congress was away from Washington in August, hackers kept hacking—24/7. That's why we need commonsense legislation like the Cybersecurity Information Sharing Act (CISA), S. 754. This bipartisan bill will protect businesses while they're keeping your valuable data and devices safe.

Let's strengthen the security of America's cyber networks.

Tell Congress to pass cybersecurity legislation now.

#VOTECISA

@cybersecurity

THE SPIRIT OF ENTERPRISE U.S. CHAMBER OF COMMERCE

www.cybersecurityadvocacy.com

Protecting America's Cyber Networks Coalition

Cybersecurity Information-Sharing Legislation: It's About Protecting America's Cyber Networks, Not Surveilling You

August 10, 2015

Some privacy groups perpetuate themyth that personal information is typically necessary to identify cyber threats, and that cybersecurity information-sharing legislation is equal to surveillance. The caption below isn't a series of typos. It shows a typical example of cyber threat information—technical and sterile data—that businesses share and receive from industry and government partners to counter cyberattacks. It contains no personal information—and that's the point.

```
#NCF Dec 27 2012—DDoS Rules

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (ms-
g:"ZBC DDoS - HTTP Header Structure with Hex Byte URI seen";
flow:established,to_server; content:"Keep-Alive|3a 20|"; http_header;
fast_pattern; content:!"gzip"; http_header; content:"Connection|3a
20|Keep-Alive"; http_header; nocase; pcre:"/[\?&][a-f0-9]{5,6}$/U";
classtype:web-application-attack; sid:40000006; rev:4;)
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"ZBC
DDoS - KamiKaze"; flow:established,to_server; content:"CLIENT-IP|3a
20|"; http_header; fast_pattern; content:"Via|3a 20|"; http_header;
content:"X-FORWARDED-FOR|3a 20|"; http_header; classtype:web-ap-
plication-attack; sid:40000007; rev:1;)
```

The surveillance myth and other falsehoods are used to oppose positive information-sharing legislation, particularly S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015, which the Senate is expected to vote on in the fall. To set the record straight, it is important to debunk five myths held by a small, but vocal, group of lawmakers and privacy interests.

Myth: Shared cyber threat information is broad in scope.

Fact: CISA's definition of cyber threat indicators (CTIs) is very limited. Businesses and government entities may only share the tactics, techniques, and procedures used by malicious actors to compromise the computer networks of their victims. In the vast majority of cyber incidents, CTIs do not implicate a person's behavioral, financial, or social information.

Myth: CISA is a surveillance bill.

Fact: CISA does not authorize the government to surveil individuals, such as targeting crimes unrelated to cybersecurity. First, a revised version of CISA eliminates the government's ability to use CTIs to investigate and prosecute "serious violent felonies"—which is a significant pro-privacy change to the bill.

Second, network "monitoring" conducted by businesses under CISA is limited to cybersecurity purposes, similar to CTIs. Monitoring can only be conducted on a company's own information systems. Further, monitoring under CISA is not intended to equate the meaning of "monitoring" as used in the context of federal criminal wiretap law or electronic surveillance under the Foreign Intelligence Surveillance Act (FISA). Any other monitoring by companies would require

authorization beyond what CISA grants. Third, Senator Dianne Feinstein, a California Democrat, said on the Senate floor on August 5 that CISA is not a surveillance bill, and that the bill was amended several times to address critics' concerns.

> [CISA] is not a surveillance bill. . . . It gives the Attorney General [and the Secretary of Homeland Security] the obligation to come up with secure guidelines to protect private information. . . . We have taken every step to prevent privacy violations from happening under this bill. Yet there are individuals who still raise that as a major concern. *I believe it is bogus.* I believe it is a detriment to us in taking this first step to protect our American industries. If we don't pass it, the thefts are going to go on and on and on [italics added].

Myth: The bill allows companies to use offensive measures or "hack back."

Fact: CISA does not permit so-called hacking back—companies are not authorized to destroy or render computer systems unusable. The bill ensures that "defensive measures" (DMs) are properly bounded. The managers' amendment clarifies that companies are not allowed to gain unauthorized access to a computer network.

Myth: CISA does not require businesses to remove personal data from threat indicators.

Fact: CISA contains multiple, overlapping provisions to guard and respect privacy. For example, in those rare instances where an individual's personal information is embedded within CTIs or defensive measures, CISA calls for public and private entities to remove such personal information unrelated to a cyber threat when sharing CTIs and DMs—and the federal government must do the same.

Myth: Businesses are encouraged to share information with the Department of Defense (DoD) and the National Security Agency (NSA).

Fact: Businesses are not granted liability protection when sharing CTIs with the DoD and the NSA—which preserves the status quo. CTIs that businesses pass on to the federal government must go through the Department of Homeland Security (DHS), which is a civilian entity.

CISA's authors, Senators Richard Burr, a Republican from North Carolina, and Feinstein, have recently revised their bill to increase its privacy protections. Among other things, the managers' amendment further limits the sharing of cyber threat data to "cybersecurity purposes." Closely related, the revised measure eliminates the government's use of cyber threat indicators to investigate and prosecute "serious violent felonies," thus putting to rest false claims that CISA is a surveillance bill. The managers' amendment also ensures that the use of DMs does not allow an entity to gain unauthorized access to a computer network. The bill writers have worked diligently to address the concerns of privacy and civil liberties organizations.

CISA passed the Senate Select Committee on Intelligence in March with broad support from both political parties and industry. The bipartisan bill would help businesses achieve timely and actionable situational awareness to improve theirs and the nation's detection, mitigation, and response capabilities against cyber threats. CISA represents a workable compromise among many stakeholders. CISA safeguards privacy and civil liberties; it is not a surveillance bill.

Agricultural Retailers Association (ARA)
Airlines for America (A4A)
Alliance of Automobile Manufacturers
American Bankers Association (ABA)
American Cable Association (ACA)
American Chemistry Council (ACC)
American Coatings Association
American Fuel & Petrochemical Manufacturers (AFPM)
American Gaming Association
American Gas Association (AGA)
American Insurance Association (AIA)
American Petroleum Institute (API)
American Public Power Association (APPA)
American Water Works Association (AWWA)
ASIS International
Association of American Railroads (AAR)
Association of Metropolitan Water Agencies (AMWA)
BITS–Financial Services Roundtable
College of Healthcare Information Management Executives (CHIME)
CompTIA–The Computing Technology Industry Association
CTIA–The Wireless Association
Edison Electric Institute (EEI)
Electronic Payments Coalition (EPC)
Electronic Transactions Association (ETA)
Federation of American Hospitals (FAH)
Food Marketing Institute (FMI)
Global Automakers
GridWise Alliance
HIMSS–Healthcare Information and Management Systems Society
HITRUST–Health Information Trust Alliance
Large Public Power Council (LPPC)
National Association of Chemical Distributors (NACD)
National Association of Manufacturers (NAM)
National Association of Mutual Insurance Companies (NAMIC)
National Association of Water Companies (NAWC)
National Business Coalition on e-Commerce & Privacy
National Cable & Telecommunications Association (NCTA)
National Retail Federation (NRF)
National Rural Electric Cooperative Association (NRECA)
NTCA–The Rural Broadband Association
Property Casualty Insurers Association of America (PCI)
The Real Estate Roundtable
Retail Industry Leaders Association (RILA)
Software & Information Industry Association (SIIA)
Society of Chemical Manufacturers & Affiliates (SOCMA)
Telecommunications Industry Association (TIA)
Transmission Access Policy Study Group (TAPS)
United States Telecom Association (USTelecom)
U.S. Chamber of Commerce
Utilities Telecom Council (UTC)

SELECT CYBERSECURITY RESOURCES

www.uschambersmallbusinessnation.com/toolkits/cybersecurity
U.S. Chamber of Commerce cybersecurity tool kit, including Internet Security Essentials for Business 2.0

http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf
National Institute of Standards and Technology's (NIST's) Small Business Information Security: The Fundamentals (revision 1) guidebook

www.nist.gov/cyberframework
NIST—Framework for Improving Critical Infrastructure Cybersecurity (the framework)

www.us-cert.gov/ccubedvp
Department of Homeland Security (DHS)—Critical Infrastructure Cyber Community C³ (C-Cubed) Voluntary Program

www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf
Department of Justice (DOJ) Computer Crime and Intellectual Property Security Section's Best Practices for Victim Response and Reporting of Cyber Incidents

www.secretservice.gov/ectf.shtml
Secret Service Electronic Crimes Task Force (ECTF)—links to more than 20 state and local ECTFs

www.ic3.gov
Internet Crime Complaint Center (I3)—accepts, develops, and refers complaints about cybercrime

www.us-cert.gov/home-and-business
United States Computer Emergency Readiness Team (US-CERT) cybersecurity resources for home and business

www.pcisecuritystandards.org/smb
PCI Security Standards Council—links to information and recommendations for SMBs

www.nacdonline.org/cyber
National Association of Corporate Directors (NACD)—Cyber-Risk Oversight handbook to help boards and senior executives manage cyber threats and risks

GETTING STARTED— TOP (LOW-COST) TIPS

Every desktop computer or handheld digital device is vulnerable to attack. The consequences of such an attack can range from simple inconvenience to financial catastrophe. Cybersecurity is an ongoing, risk-management activity—there is no end state. The U.S. Chamber selected a number of cybersecurity recommendations that many experts tend to emphasize and have packaged them under four broad categories: set up a secure system, protect business data, train your workforce, and be prepared to respond to an incident.

SET UP A SECURE SYSTEM

• **Designate a person to handle security and preparedness.** This role can be part time or full time depending on the scope and complexity of your business operations. The person in this position performs a number of functions, such as determining which information assets require protection, maintaining an inventory of the computer equipment needed to fulfill critical business functions in case of a disaster, and developing a plan for responding to cybersecurity incidents. This person should be aware of regulatory requirements and guidance documents regarding data security.

• **Control network access.** One of the best and easiest ways to protect your network is to limit the sites that employees can visit and what they can download and install onto a system. To decrease the chances of an employee navigating to a malicious site or downloading a virus-laden program, business owners should install a firewall with strong access controls. These important safeguards will help protect your business' network from malware, viruses, and other Internet threats.

• **Defend company computers.** Running a small business can leave little time for practicing good cybersecurity. However, relatively simple actions can help strengthen your business' systems and devices. Keep all software current, including your operating system and Web browser. Take time to install security updates and patches if they cannot be done automatically.

PROTECT BUSINESS DATA

• **Organize business data and assess its risk.** Sometimes small business owners or managers say, "We don't have any sensitive stuff to protect," which is more a function of feeling busy, rather than truly believing that their data do not need protecting. Small businesses have an array of information (e.g., personnel records, blueprints, tax forms, and customer orders) that require protection.

• **Small businesses should organize the information they keep, know where it is stored, and prioritize it by level of importance—think of this process as information security triage.** They should also identify the digital and physical locations of business data. Consider what data can be separated or segmented on the information network or system so that it's not immediately and easily accessible to bad actors.

• **Manage the security of business data.** You keep valuable and sensitive data on your computer. You may have sensitive information about your company, clients, or personal bank statements on a laptop you use both at home and at work. Establish an acceptable use policy for information resources and IT systems.

• **Back up data regularly.** There are many risks to our data, such as hardware or software malfunctions, natural disasters, emergencies, and theft. Malware-enabled cyberattacks can lead to data loss and can either destroy your computer or render it useless. Important files can be lost by accidental deletion too.

Data backup is a relatively simple, three-step process: (1) Make copies of the data on your computer(s); (2) select the appropriate hardware to store the backup data; and (3) safely store the backup device that holds your copied files.

• **Dispose of data and media safely and securely.** Hard drives and other disposable computer equipment may contain saved information even if that information has been "deleted." Information that is deleted from a computer may be retrieved through recovery tools.

Assume that at some point sensitive information may have been stored and is still retrievable from all electronic storage media, such as computer and network hard drives, external hard drives, CDs, DVDs, floppy disks, tapes, flash drives, and mobile phones. Be sure to dispose of computer data in a way that follows best practices and is consistent with legal requirements.

TRAIN YOUR WORKFORCE

• **Defend your computer.** The security of your computers and data is crucial for your employees and your company. Lost or stolen information can reveal company secrets or expose your confidential or personal information.

Strengthen your computer's defenses by keeping all software, including your Web browser, current with automatic updates. Install legitimate antivirus and antispyware software. Protect your company's wireless router with strong passwords or phrases. Don't be tricked into downloading malicious software. Think carefully before opening attachments or clicking links in unusual email or instant messages (IM) on a social network.

• **Protect sensitive business data—and watch out for scams.** Don't put sensitive and confidential information in email or instant or text messages; it may not be secure. Think carefully before you open attachments or click links in unusual messages, on a social network, or in random pop-up windows. If you're unsure if a message is genuine—even from a co-worker—contact the sender using a different device or account. Never give sensitive information, such as a user name or password, in response to a phone call, an email, or other online request (even from a co-worker).

• **Create strong passwords and keep them secret.** Passwords provide the first line of defense against unauthorized access to your computer. Weak passwords make it easier for attackers to access your computers and network. Strong passwords are considerably harder to crack, even with the latest password-cracking software.

Secure passwords and passphrases have at least eight characters and utilize upper and lower case letters, numbers, and symbols (!, @, #, $, %, etc.). Don't include your real name, Social Security number, company name, or a complete dictionary word in your password or passphrase. Common brand names are also not recommended.

• **Guard your data when on the go.** Treat all public Wi-Fi as a security risk. Do not expect privacy in Internet cafes, hotels, offices, or public places when traveling. When connecting to a public wireless network, it's a best practice to choose the most secure option even if you have to pay for it. Some wireless networks offer a network

key or certificate that encrypts (or scrambles) data as they travel between your laptop and the router.

• **Use flash drives carefully.** Minimize the chance that you'll infect your company network with malware. Don't put any unknown flash (or USB) drive into your computer.

BE PREPARED TO RESPOND TO AN INCIDENT

• **Log Monitoring.** Whether your business is large or small, managers should continuously monitor their log data. The Chamber recommends using indexing technologies in lieu of a database to help collect, analyze, and correlate logs so that they are usable. Indexing solutions don't require preformatting data at collection time.

These technologies include search capabilities, automated searches, statistical analysis, and data visualization. Machine data can be collected and indexed in real time, and users can interact with their data using a familiar interface for searching through structured and unstructured log data to identify and highlight abnormal activities.

• **Make a plan to address cyber incidents.** Has your system been compromised? How did it happen? What do you do? At some point, your business may experience an information security incident, if it hasn't already, and the incident may jeopardize your computer security.

Fast and efficient responses can lead to quick recovery, minimize damage, and help prevent future incidents. All end users should be familiar with symptoms that may indicate an incident and need to know what to do. Threats against your business computers can easily spill over to others' computers and vice versa.

The Chamber's cybersecurity booklet, Internet Security Essentials for Business 2.0, goes into each of these tips in greater detail and is accessible at www.uschamber.com/internet-security-essentials-business-20.

NATIONAL SECURITY AND EMERGENCY PREPAREDNESS DEPARTMENT

The U.S. Chamber's National Security and Emergency Preparedness Department was established in 2003 and develops and implements the Chamber's homeland and national security policies. The department works through the National Security Task Force, a policy committee composed of roughly 200 Chamber members representing a broad spectrum of the nation's economy. The Task Force's Cybersecurity Working Group identifies current and emerging issues, crafts policies and positions, and provides analysis and direct advocacy to government and business leaders.

The department champions members' views through outreach to congressional lawmakers and staff, regulatory filings with federal agencies, meetings with agency and department officials, communications with the media, and public forums with elected and appointed officials and members of the business community. The department offers positive solutions to Washington leaders on an array of homeland and national security challenges that impact the strength of the nation and the global economy.

To learn more about the National Security and Emergency Preparedness Department or the Cybersecurity Working Group, contact Ann M. Beauchesne (abeauchesne@uschamber.com), senior vice president, Matthew J. Eggers (meggers@uschamber.com), senior director, or Vincent Voci (vvoci@uschamber.com), policy manager, or call 202-463-3100.

U.S. Chamber's Matthew Eggers to Speak at the Cybersecurity Business Roundtable II Hosted by the Virginia Beach Department of Economic Development

Tuesday, October 13
2:00 – 6:00 p.m.
Location: Town Center Virginia Beach, One Columbus Center, Suite 700, Virginia Beach, VA 23462

Please join the Virginia Beach Department of Economic Development for a collaborative discussion with Matthew Eggers, senior director for National Security & Emergency Preparedness at the U.S. Chamber of Commerce. He will discuss the intersection of cybersecurity policy, the workforce, and community development.

Chamber contact: Matthew Eggers – meggers@uschamber.com

U.S. Chamber's Ann Beauchesne to Speak at the Cybersecurity and American Businesses Event Hosted by the Washington Cyber Roundtable

Wednesday, October 14
2:00 – 5:00 p.m.
Location: Maggiano's Little Italy, 2001 International Drive, McLean, VA 22102

Please join the Washington Cyber Roundtable for a collaborative discussion with Ann Beauchesne, senior vice president for National Security & Emergency Preparedness at the U.S. Chamber of Commerce. She will share her perspectives on current cyber threats to business, cyber risk management with the NIST framework and industry best practices, and legislation addressing cyber threat information sharing.

Chamber contact: Ann Beauchesne – abeauchesne@uschamber.com
More information: www.washingtoncyber.com

U.S. Chamber's Bradley Hayes to talk about Cybersecurity at the "Latest Issues Affecting Business" session

Wednesday, October 14
1:45 – 3:15 p.m.
Location: Nashville, TN

Bradley Hayes, Director, Congressional and Public Affairs at the U.S. Chamber of Commerce, will share his perspectives on current cyber threats to business, cyber risk management with the NIST framework and industry best practices, and legislation addressing cyber threat information sharing during the U.S. Chamber of Commerce's Regional Government Affairs meeting 'pods' section

Chamber contact: Bradley Hayes – bhayes@uschamber.com

U.S. Chamber's Matthew Eggers to Moderate "Cybersecurity in the Health Care World: What's at Risk and Why You Should Care" Panel Discussion at Second Annual Cyber Education Summit

Thursday, October 15
10:15 a.m.
Location: Georgia Regents University | J. Harold Harrison Education Commons Building, 1301 R.A. Dent Boulevard, Augusta, GA 30912

In a world where we are increasingly dependent on technology and almost all information is transmitted over the Internet, why should we be concerned? Where are the current threats and how can we prepare to protect our R&D pertaining to drug development and clinical trials? What other threats should the health care community be aware of with regard to medical device and equipment vulnerabilities? This discussion will explore existing and future threats and the possible need to cross-reference cybersecurity training and expertise in the health care education realm.

Chamber contact: Matthew Eggers – meggers@uschamber.com
www.gru.edu/cybersummit

THANK YOU

The U.S. Chamber thanks the following companies for sponsoring the Cybersecurity Summit in Washington, D.C.

Sponsors

American Express

ARMOR
BETWEEN YOU AND THE THREAT

CLEARFORCE

DELL

DELL SecureWorks

LIBERTY GROUP VENTURES

SOUTHERN COMPANY

Partner

National Cyber Security Awareness Month

U.S. CHAMBER OF COMMERCE

1615 H Street, NW | Washington, DC 20062-2000
www.uschamber.com