CYBER SECURITY
INDUSTRY ALLIANCE

Talking Points for Cyber Security

Preventing Identity Theft, Protecting Intellectual Property and Critical Infrastructure, Increasing Accountability

Why Cyber Security Matters

"Talking Points for Cyber Security" is a concise primer on why cyber security matters. It details threats posed by attacks, describes solutions, and surveys public and private organizations and initiatives for stronger cyber security. Consistent application of cyber security best practices creates stronger security and prevents identity theft and fallout from cyber attacks. Congress is encouraged to use this primer for background during discussion and consideration of issues related to cyber security policy. Questions and requests for more resources may go to Laura Brown, CSIA Policy Analyst at lbrown@csialliance.org.

What you need to know about Cyber Security

In this document, find out about

- Threats
- What Is Vulnerable
- How Attacks Occur
- Who Launches Cyber Attacks
- Solutions

What is Cyber Security?

Cyber security is the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Cyber security may include technology, policies and training to achieve its goal of protecting and assuring information quality.

Cyber Security Is Vital

Three years ago Americans were shocked with the dramatic need to strengthen national security. Following the tragedy of 9/11, physical security has been the appropriate national focus. Now, enhancement of national security requires the added dimension of *cyber security*, especially as technology integrates more deeply with daily life and business in addition to national defense. Cyber attacks and security breaches cost the U.S. economy billions of dollars of direct losses. They shatter innocent lives by fallout from stolen identities. Attacks can ruin businesses and foil military plans with stolen intellectual property. And they may cause downtime and risk stoppage of vital services blocked by catastrophic system failure from weakened critical infrastructure. Cyber security increases accountability, ensuring the integrity of data and financial databases. It is prudent for Congress to address security with a cyber-specific agenda to further protect and strengthen freedoms all Americans.

Cyber Security is Non-Partisan

Cyber security is a non-partisan issue. Work to strengthen cyber security began in the Clinton administration. The Bush administration continued and boosted this work. The bipartisan work to help the government and private sector improve security has created innovations such as an initiative to secure personal healthcare information sent over the Internet. Continued bipartisan efforts to forge stronger cyber security will help protect identities and personal information of U.S. citizens, protect people, businesses and the economy from financial losses, and guarantee the continuous operation of critical services vital to the operation of our information-based society.

Potential Fallout from Cyber Attacks

- Slow systems cut productivity
- Erased or stolen data can trigger financial or strategic loss
- Damaged or stopped systems can interrupt critical services

Threats

What Is Vulnerable to Attack

Any digital system or data that is valuable or confidential is a potential attack target.

Personal Information. Birthplace, birth date, mother's maiden name, Social Security number, credit card numbers, bank account number, health records, court settlements.

Business Information. Customer records, product and sales information, business plans, proprietary product designs, software code, materials and inventory data, financial statements.

Critical Infrastructure Systems. Agriculture, meat, poultry and egg products; banking and finance, chemical; defense industrial base; electric power generation and distribution, and oil and gas production and storage; emergency services including law enforcement; information technology; national monuments and icons; postal and shipping; public health services; telecommunications; transportation systems; water supply.

Government Systems. Security, emergency services, military, etc. rely on critical infrastructure, 85% of which is operated by the private sector.

How Cyber Attacks Occur

Denial of Service. Attack on network that floods it with traffic, preventing passage of normal traffic. DoS can cause severe damage to databases and halt network-based services.

Malware. MALicious softWARE. See Spyware, Trojan horse, Virus, Worm.

Phishing. Scam to steal personal information over the Internet. Email "fishes" by inviting victims to click to a fraudulent but official-looking site (bank, hospital, etc.) and "correct their personal information." Scams reap hundreds of millions of dollars a year.

Spyware. Software surreptitiously logs record of your web surfing for amusement of digital peeping Toms. Spyware can be very dangerous when it logs passwords.

Stupidity. Displaying passwords on a Post-It note stuck to a computer monitor; using passwords like "PASS"; giving out passwords over the phone to cold-callers pretending to be "verifying information" for a bank; not using industry-standard security measures.

Trojan horse. Ostensibly "good" software fools us with a hidden virus, like the hollow wooden horse filled with Greek soldiers fooled Troy.

Virus. Software that exploits a vulnerability by copying itself to other computers over the Internet. Usually requires human trigger like opening an infected email file attachment.

Worm. Like a virus but requires no human trigger for infection and action. Automatically hits vulnerable systems.

Who Launches Cyber Attacks

Kids. Computer aptitude + spare time + desire for mischief = potential for cyber attack. A popular graphical user interface eases the use of free tools to make viruses and worms.

Hackers. Computer geeks who thrive on throwing digital wrenches into information systems. Money is rarely the object, but all relish peer praise in hacker blogs.

Criminals. Money is the object, such as phishing schemes that steal identities, ruin personal lives and scam credit card companies.

Insiders. Employees who are frustrated, laid off or fired may want to get even. Unprotected networks are like leaving a key in the door.

Nation States. North Korea just sent 500 hackers through a 5-year cyber war university program possibly held in China, according to South Korea.

Terrorists. Cyber attacks fit their M.O. to a "T." They cause us to lose faith in our system and policies and prompt fear over the use of information technology.

Solutions

Experts recommend a "multi-layer" policy for cyber security. In plain English, that means there is no silver bullet, no one single application that resolves all cyber security issues. Typical products and processes for particular security issues are:

Anti-Virus Software automatically checks new files entering a PC for infection.

Asset Management Used to match inventory against scans for known vulnerabilities; helps pinpoint specific security holes so those holes can be efficiently repaired through patches or other remediation.

Authentication Digital certificates and secure ID technology verify identities of web sites and authorized users.

Education Teaches users why and how to practice security-wise behavior.

Intrusion Detection/Prevention Technologies that monitor content of network traffic for infections and block traffic carrying infected files or programs.

Encryption Transforms data into password (key)-protected packets that prevent reading by unauthorized users.

Firewall Blocks unauthorized traffic from entering PCs and servers from the Internet.

Patch Fixes vulnerability in software by replacing a portion of faulty code.

Policy Management Enforces security rules and regulations of IT systems.

Vulnerability Management Processes and tools to identify and remediate cyber vulnerabilities in the 5 major classes, including unsecured accounts, misconfigurations, software defects, unnecessary services, and malware (spyware, backdoors, trojans, etc)

New Technologies

Information systems are not static. Industry and government are rapidly deploying new technologies ranging from Voice of Internet Protocol (VOIP), Radio Frequency Identification (RFID) tags, advanced wireless cellular systems such as “WiMax,” and nanotechnology. Each of these areas prompts new issues about the security and reliability of information systems which require attention.

Policies Make a Difference

The Cyber Security Industry Alliance is the only association focused exclusively on cyber security public policy. We work with Federal and state governments to highlight policy issues associated with cyber security. We take a leadership role on bringing the private sector together to address common issues of concern related to cyber security. We do not advocate additional regulation to secure the information infrastructure. We seek to bring clarity to existing regulation such as: Sarbanes-Oxley, the Health Insurance Portability and Accounting Act, Gramm-Leach-Bliley, 21 CFR 11, Federal Information Security Management Act, state legislation, key EU and other international standards and regulations.

Please contact us if you have any questions or issues of concern.

Talking Points provided by the Cyber Security Industry Alliance
2020 N. 14th Street
Suite 750
Arlington, VA 22201
703-894-CSIA

www.csialliance.org