Information Technology
Industry Council

The IT Industry's Cybersecurity Principles for Industry and Government

TABLE OF CONTENTS

Editor's Note: As used in these Principles, the "Information Technology (IT) Industry" refers generally to the technology industry, namely providers of computer and computer network hardware and software, but does not encompass telecommunications equipment vendors. Although ITI's members include the latter, they generally adhere to the security standards and guidelines outlined by the Third Generation Partnership Project (3GPP) and 3GPP2. This document articulates cybersecurity principles developed by IT companies.

EXECUTIVE SUMMARY

Cybersecurity is rightly a priority for both Congress and the Administration. The phenomenal expansion of cyberspace has brought unprecedented economic growth, opportunity, and prosperity. However, it also presents bad actors with completely new threat and crime opportunities. The interests of industry and governments in securing and facilitating cyber-based transactions and activities are fundamentally aligned. All companies want a secure digital infrastructure for commercial transactions. To ensure the continued viability of the infrastructure and growth of their sector, technology companies are highly motivated to design and build security into the DNA of their products and systems. Governments need a secure global digital infrastructure for economic growth, prosperity, efficiency, and protection.

To better inform the public cybersecurity discussion, the Information Technology Industry Council (ITI) is pleased to present this comprehensive set of cybersecurity principles for industry and government. The outcome of extensive discussion among ITI members – which comprise the world's leading technology companies, both producers and consumers of cybersecurity products and services – ITI's six principles provide a useful and important lens through which any efforts to improve cybersecurity should be viewed.

To be effective, efforts to enhance cybersecurity must:

- Leverage public-private partnerships and build upon existing initiatives and resource commitments;
- Reflect the borderless, interconnected, and global nature of today's cyber environment;
- Be able to adapt rapidly to emerging threats, technologies, and business models;
- Be based on effective risk management;
- Focus on raising public awareness; and
- More directly focus on bad actors and their threats.

These principles are summarized on page 9. Subsequent pages focus on each principle: its importance, what industry and governments are already doing in each area, and specific proposals for what more policymakers can do.

ITI and its members look forward to working with policymakers to develop and facilitate an effective public policy framework that enhances security while maintaining the overall benefits of cyberspace.

SETTING THE STAGE

Cyberspace is Fundamental to the Modern Global Economy.

In recent decades, “cyberspace” has grown phenomenally. An interconnected global digital infrastructure, cyberspace includes the Internet, computer systems, hardware, software and services, and digital information. Collectively, cyberspace has brought unprecedented economic growth, opportunity, and prosperity. It is the nervous system of today’s economy - most of our major economic institutions would not operate without it. It enables e-commerce, e-government, information sharing, and trade. In fact, the annual global economic benefits of the commercial Internet equal $1.5 trillion[1]. Cyberspace’s underlying information technologies (IT) have automated entire economic sectors such as finance and manufacturing and continue to create whole new industries and markets. Cyberspace also evolves quickly. Technologically, the connectivity, devices, and uses of today - computing tablets, home networks, smart meters, cloud computing, social networks - have made the cyberspace of today radically different from that of five years ago. Demographically, young generations view social networking and online collaboration as parts of their daily lives. Geopolitically, cyberspace is expanding across borders, making the world smaller. Cyberspace will continue to evolve and change and its future is exciting and in many ways unpredictable.

Cybersecurity is Fundamental to Cyberspace.

The interconnected, global, and digital nature of the cyber infrastructure unfortunately also has presented bad actors with completely new crime opportunities. Security practices serve to counter these opportunities and allow cyber-based transactions and activities to occur. In this area, the interests of industry and governments are fundamentally aligned. Companies across all industry sectors want a secure digital infrastructure for commercial transactions. IT companies build the hardware, software, and services to enable a secure infrastructure and recognize the need for trust in their technologies and services. To ensure the continued viability of the infrastructure and growth of their sector, IT companies are highly motivated to design and build security into the DNA of their products and systems. Governments need a secure global digital infrastructure for similar reasons – economic growth, prosperity, efficiency, and protection - all of which provide tremendous value to their nations’ businesses, citizens, and economies.

Cybersecurity is Advancing in Tandem with Cyberspace.

The growth of cyberspace will continue to advance if interoperability, openness, stability, resiliency, economic growth, and risk mitigated by security guide its development. In the right policy environment, we can increase security while maintaining cyberspace’s overall benefits. A host of tools and approaches are available to consumers, businesses, governments, infrastructure owners and operators, and the IT industry to meet our shared security challenges and goals. These evolving tools include information sharing, risk management models, technology, training, and the development of globally accepted security standards, guidelines, and best practices. Public policy will play an important role in encouraging the use and improvement of these tools and helping to shape the expectations and actions of stakeholders on cybersecurity.

[1] “The Internet Economy 25 Years After .Com: Transforming Life and Commerce,” Information Technology and Innovation Foundation (ITIF), March 2010.

SIX CYBERSECURITY PRINCIPLES

As industry and governments work together to develop the right policy framework to enhance cybersecurity, there are six guiding principles to follow:

1. **Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments.** By partnering with government the IT industry has provided leadership, resources, innovation, and stewardship in every aspect of cybersecurity for more than a decade. Cybersecurity efforts are most effective when leveraging and building upon these existing initiatives, investments, and partnerships.

2. **Efforts to improve cybersecurity must properly reflect the borderless, interconnected, and global nature of today's cyber environment.** Cyberspace is a global and interconnected system that spans geographic borders and traverses national jurisdictions. The United States should exercise leadership in encouraging the use of bottom-up, industry-led, globally accepted standards, best practices, and assurance programs to promote security and interoperability.

3. **Efforts to improve cybersecurity must be able to adapt rapidly to emerging threats, technologies, and business models.** IT is an innovative and dynamic sector with rapidly changing and evolving technologies. Cybersecurity efforts must be equally dynamic and flexible to effectively leverage new technologies and business models and address new, ever-changing threats.

4. **Efforts to improve cybersecurity must be based on risk management.** Security is not an end state. Rather, it is a means to achieve and ensure continued trust in various technologies that comprise the cyber infrastructure. Cybersecurity efforts must facilitate an organization's ability to properly understand, assess, and take steps to manage ongoing risks in this environment.

5. **Efforts to improve cybersecurity must focus on awareness.** Cyberspace's owners include all who use it: consumers, businesses, governments, and infrastructure owners and operators. Cybersecurity efforts must help these stakeholders to be aware of the risks to their property, reputations, operations, and sometimes businesses, and better understand their important role in helping to address these risks.

6. **Efforts to improve cybersecurity must more directly focus on bad actors and their threats.** In cyberspace, as in the physical world, adversaries use instruments (in this case, technology) to carry out crime, espionage, or warfare. Cybersecurity policies must enable governments to better use current laws, efforts, and information sharing practices to respond to cyber actors, threats, and incidents domestically and internationally.

WHAT SHOULD POLICYMAKERS BE DOING?

For each of these principles, ITI has developed specific proposals for how policymakers can augment current efforts underway. These proposals are found on the following pages.

PRINCIPLE 1: Efforts to improve cybersecurity must leverage public-private partnerships and build upon existing initiatives and resource commitments.

Why is this important?

It is well-known that the private sector owns and operates 85% of critical infrastructure in the United States, and that the information technology (IT) industry creates nearly the entire cyberspace infrastructure. What is not known is the multitude of ways in which the IT industry works cooperatively with national, state, and local governments to improve cybersecurity and ensure that approaches to cybersecurity are adaptive and effective. For well over a decade, IT companies have provided leadership, subject-matter experts, technical and monetary resources, innovation, and stewardship to enable all stakeholders to better manage and mitigate cybersecurity risk. Cyberspace would be much less secure in the absence of these partnerships and initiatives.

What are we doing now?

The IT industry leads and contributes to a range of significant public-private partnerships, including information sharing, analysis, and emergency response with governments and industry peers. Some key examples follow.

- The U.S. IT industry formed and funds the IT Sector Coordinating Council (IT-SCC) to work closely with the Department of Homeland Security (DHS) to ensure better preparedness and coordination of critical infrastructure protection (CIP) initiatives.

- Major U.S. IT companies founded and operate the IT Information Sharing and Analysis Center (IT-ISAC), a non-profit operational center established to exchange information among companies and with DHS to identify, manage, and mitigate IT infrastructure risks.

- Major U.S. IT companies participate in the Industry Consortium for Advanced Security on the Internet (ICASI), an industry-driven global initiative to share information on product vulnerabilities.

- U.S. IT companies participate in national advisory committees such as the Federal Bureau of Investigation (FBI)'s National Cyber Forensics Training Alliance and the Forum of Incident Response and Security Teams (FIRST).

- U.S. IT companies work closely with the National Institute of Standards and Technology (NIST) to provide input into NIST's security standards and guidelines for U.S. Federal non-classified computer systems.

- U.S. IT companies participate in DHS's Software Assurance (SwA) Program, which spearheads the development of practical guidance and tools and promotes research and development (R&D) to reduce software vulnerabilities and improve the routine development and deployment of trustworthy software products.

What more can policymakers do?

Although many of these public-private partnerships are working well, and form an important baseline, they can be improved or better utilized. Policymakers should:

- Recognize that many public-private partnerships have been in existence for a decade and include a significant amount of trust between actors as well as significant resource commitments by all involved.

- Leverage and build upon existing partnerships and efforts to the fullest extent possible, including those that work to advance critical infrastructure protection. *Congress and the Administration can both contribute to this effort.*

- Determine which public-private partnership(s) may be addressing issues about which policymakers are concerned, and leverage them as appropriate before proposing something new (particularly before proposing any new structure at odds with such partnerships). *Congress and the Administration can both contribute to this effort.*

- Identify any concerns about current public-private partnerships and suggest means for improvement before proposing entirely new public-private partnerships be built from scratch. *Congress and the Administration can both contribute to this effort.*

- Better understand the public- and private-sector roles and responsibilities, under existing authority, related to public emergencies, and identify any gaps. *The Administration should lead on this effort.*

- Eliminate barriers that preclude the sharing of specific, actionable threat information between the public and private sectors. *The Administration should lead this effort.*

- Better share specific, actionable information on cyber threats with private-sector actors so that the latter can react more quickly and sufficiently. *The Administration should lead on this effort.*

- Ensure that NIST continues to serve as the U.S. Federal coordinator for cybersecurity best practices and guidelines. *Congress should lead on this effort.*

- Take definitive steps to improve federal cybersecurity by consistently and fully implementing throughout U.S. Federal networks industry-led, globally recognized cybersecurity standards and best practices. *The Administration and Congress can both contribute to this effort.*

PRINCIPLE 2: Efforts to improve cybersecurity must properly reflect the borderless, interconnected, and global nature of today's cyber environment.

Why is this important?

Cyberspace is a global and interconnected domain that spans geographic borders and national jurisdictions. To support the growth, operation, maintenance, and security of this domain, information technology (IT) companies continually innovate and invest in the development of globally deployable products and services. Cyberspace's stakeholders - consumers, businesses, governments, and infrastructure owners and operators - seek a consistent, secure experience in cyberspace.

Efforts to improve cybersecurity should reflect cyberspace's borderless nature and be based on globally accepted standards, best practices, and international assurance programs. This approach will improve security, because nationally focused efforts may not have the benefit of the best peer-review processes traditionally found in global standards bodies, because proven and effective security measures must be deployed across the entire global digital infrastructure, and because the need to meet multiple, conflicting security requirements in multiple jurisdictions raises enterprises' costs, demanding valuable security resources. This approach will also: 1) improve interoperability of the digital infrastructure, because security practices and technologies can be better aligned across borders; 2) permit more private-sector resources to be used for investment and innovation to address future security challenges; 3) increase international trade in cybersecurity products and services that can be sold in multiple markets; and 4) allow countries to comply with their international commitments, such as the World Trade Organization (WTO)'s Technical Barriers to Trade Agreement (TBT), which calls for non-discrimination in the preparation, adoption, and application of technical regulations, standards, and conformity assessment procedures; avoiding unnecessary obstacles to trade; harmonizing specifications and procedures with international standards as far as possible; and the transparency of these measures.

What are we doing now?

The IT industry is actively involved in developing globally accepted cybersecurity standards, best practices, and international assurance programs. Some key examples follow.

- U.S. IT companies contribute to global cybersecurity standards development through the International Organization for Standardization (ISO), Organization for the Advancement of Structured Information Standards (OASIS), Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and numerous other organizations.

- U.S. IT companies, the U.S. Government, and foreign governments work to implement, improve, and expand the Common Criteria for Information Technology Security Evaluation (CC), the international standard (ISO 15408) for computer product assurance security certification. The CC is both the ISO standard and a multi-lateral agreement - Common Criteria Recognition Arrangement (CCRA) - among 26 countries including the U.S., Japan, the UK, Australia, Germany, Korea, and India.

- U.S. IT companies worked with the Department of Defense to found the Trusted Technology Forum (TTF), a global industry-led standards initiative that will allow technology companies, customers, government, and supplier organizations to create and promote guidelines for manufacturing, sourcing, and integrating trusted, secure technologies.

- The U.S. and other governments participate in bilateral and multilateral efforts to facilitate international government-industry cooperation on global cybersecurity best practices. Examples include bilateral critical infrastructure protection (CIP) forums between the U.S. Government and our trading partners including Japan and the EU, and the Congressionally mandated biennial Cyber Storm exercise series run by the Department of Homeland Security (DHS), which is designed to test and improve communications, policies, and procedures in response to various cyber threats.

What more can policymakers do?

Some policymakers' proposals refer to cybersecurity standards, best practices, and product assurance. Policymakers should:

- Support industry and government collaboration to review and continue to improve the CC product assurance standard as necessary, and maintain focus on the CC and the CCRA as critical components of global cybersecurity. *The Administration should lead on this effort.*

- Make the preservation and promotion of a global market a primary goal in any product assurance requirements, and avoid U.S. Government-specific requirements. *Congress and the Administration can both contribute to this effort.*

- Carefully view any U.S. policies from a global perspective. Any U.S. policies that are non-globally compatible, whether implemented through law or regulation (or sometimes if merely proposed) will be emulated around the world. Some countries also may use such policies or proposals as a starting point for their own additional domestic regulatory intrusions that will balkanize the global marketplace. *Congress and the Administration can both contribute to this effort.*

- Recognize and reaffirm the United States' leadership role in promoting international adoption of industry-led, globally recognized cybersecurity standards and best practices. Among other ways, the U.S. can do this by demonstrating progress in implementing such standards and best practices in U.S. Federal systems. *Congress and the Administration can both contribute to this effort.*

- Proactively seek dialogues with our trading partners about the use and benefits of industry-led, globally recognized standards and best practices that will achieve the requisite levels of security needed to meet national security concerns while preserving interoperability, openness, and economic development. *The Administration should lead on this effort.*

- Counter other countries' attempts to enact non-globally compatible cybersecurity-related standards, practices, and requirements that threaten to balkanize cyberspace and make it less secure. *The Administration should lead on this effort.*

PRINCIPLE 3: Efforts to improve cybersecurity must be able to adapt rapidly to emerging threats, technologies, and business models.

Why is this important?

Information technology (IT) is an innovative and dynamic industry, and cyberspace relationships evolve continuously among its stakeholders. Cyberspace's technologies - the Internet, computer systems, hardware, software, and services, ubiquitous devices, and digital information - change constantly. Devices to connect to cyberspace, such as networked home devices and computing tablets, are constantly updated and upgraded. New business and service delivery models such as mobile applications, social networking, and cloud computing are emerging. Criminals or other actors are constantly modifying and adapting their techniques. Cybersecurity efforts must be flexible so that they can effectively leverage new technologies and business models, address constantly changing threat dynamics, and manage new risks and vulnerabilities. They also must use technologies, people, and processes.

What are we doing now?

There are a variety of effective industry and government efforts to develop cybersecurity measures that establish a layered approach to information security, and are continually updated by security experts around the globe, evolving as threats evolve. Some key examples follow.

- The U.S. IT industry collaborates with the U.S. Government to develop voluntary consensus-driven standards that meet private- and public-sector needs. This collaboration has resulted in better, flexible standards – such as website accessibility standards for people with disabilities - and has given the public access to better and cost-effective technologies and products.

- The U.S. IT industry has established new standardization efforts addressing emerging cybersecurity risk concerns, such as the Kantara Initiative, Open Identity Exchange (OIX), OpenID Foundation, and the Information Card Foundation, which are focusing on identity management.

- U.S. IT companies work to advance their own software assurance via company-specific programs as well as voluntary consortia such as the Open Group and Software Assurance Forum for Excellence in Code (SAFECode).

- Less than a half dozen of the major U.S. IT companies combined spend more than $30 billion annually on research and development (R&D). A significant amount of this investment is focused on security.

What more can policymakers do?

Some policy proposals to improve cybersecurity would designate or mandate specific technologies, business practices, or risk management measures. Policymakers should:

• Ensure any proposals are technology neutral and flexible enough to promote technological innovation. *Congress and the Administration can both contribute to this effort.*

• Utilize and support processes for developing best practices that are industry-led. *Congress and the Administration can both contribute to this effort.*

• Actively encourage and support the global standards development work undertaken through proven private/public partnerships and the diversity of standards development organizations. *Congress and the Administration can both contribute to this effort.*

• Minimize or eliminate different or conflicting security requirements and policies existing within or among U.S. Federal agencies that should be adhering to common sets of requirements and policies established for civilian and defense/intelligence networks. *Congress and the Administration can both contribute to this effort.*

• For U.S. Federal systems, rationalize and streamline security requirements that have become unnecessarily burdensome, such as extensive paperwork mandates and inordinately lengthy testing, certification, and accreditation requirements. This will allow acquirers to more quickly adopt the latest, most secure solutions and practice more effective operational risk management and continuous monitoring. *Congress and the Administration can both contribute to this effort.*

• When attempting to address new security threats to U.S. Federal systems, determine which current or emerging federal security requirements or frameworks could adequately address these threats before proposing new requirements, authorities, or review processes. *Congress and the Administration can both contribute to this effort.*

• When updated requirements for U.S. Federal systems are determined necessary, ensure that they build upon, modify, or replace existing requirements so as to maintain a clear, streamlined, and integrated approach to federal cybersecurity. *Congress and the Administration can both contribute to this effort.*

• Promote greater research and development (R&D) in cybersecurity such as by 1) extending and making permanent the R&D tax credit, and 2) supporting long-term government R&D in cybersecurity, such as by increasing funding for the federal Networking and Information Technology Research and Development (NITRD) Program. *Congress should lead on this effort.*

• Actively support and fully operationalize industry-government partnerships to identify, sort, and prioritize cyber threats to ensure approaches to security are adaptive, appropriate, and effective. *Congress and the Administration can both contribute to this effort.*

• Leverage existing partnerships and efforts in the area of critical infrastructure protection before broadening the scope and definition of “critical infrastructure” or increasing regulations in this area. *Congress and the Administration can both contribute to this effort.*

• Convene a discussion with all interested stakeholders on whether and how to update the definition of “critical infrastructure” and develop a dynamic assessment model that can respond to changing technologies and risks. *The Administration should lead on this effort.*

PRINCIPLE 4: Efforts to improve cybersecurity must be based on risk management.

Why is this important?

Security is not an end state. It is a means of ensuring that the benefits from the digital infrastructure continue to grow. No sector of the economy, whether offline or online, is – or can ever be – 100% secure and without some inherent risk. We will never be completely free from natural disasters, crime, espionage, war, airplane or automobile accidents, project failures, credit risks, threats to public health, or terrorists. However, in all of these scenarios, practitioners use risk management to identify risk, assess risk, and take steps to manage risk to an acceptable level. Strategies to manage risk include avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Cybersecurity must be part of an overall risk management framework, incorporating technology, people, and processes.

What are we doing now?

The information technology (IT) industry and governments are continuously developing and utilizing a range of risk management strategies and best practices for cyberspace. Some key examples follow.

- Industry standards such as International Standards Organization / International Electrotechnical Commission (ISO/IEC) 27001 and 27002 and similar international standards establish practices and controls to manage cybersecurity risks.

- National Institute of Standards and Technology (NIST) risk management standards and special publications - created with extensive industry input - are built around risk assessment and risk management.

- The U.S. IT industry contributes to the National Infrastructure Protection Plan (NIPP), a framework announced by the Department of Homeland Security (DHS) in 2006 to help government agencies and their partner organizations protect the nation's critical infrastructure and other key resources (CIKR) against damage or loss due to terrorist attack, natural disaster, or other catastrophe.

- Major U.S. IT companies build risk management into their ongoing daily operations through legal and contractual agreements, cybersecurity operational controls, adherence to global risk management standards, and a host of other practices.

What more can policymakers do?

- Understand that security is about risk management and taking measures appropriate to the value and consequences of the information in question.

- Ensure that any cybersecurity measures are flexible so as to allow organizations to properly assess and mitigate risk appropriate for their infrastructures and risk tolerance models. *Congress and the Administration can both contribute to this effort.*

- Understand and accept real risk management prioritization for cyberspace and develop and implement policies based upon thoughtful, ongoing risk management assessments. *Congress and the Administration can both contribute to this effort.*

PRINCIPLE 5: Efforts to improve cybersecurity must focus on awareness.

Why is this important?

Cyberspace's stakeholders - consumers, businesses, governments, and infrastructure owners and operators - need to know how to reduce risks to their property, reputations, and operations. However, many stakeholders are not aware of and also do not adequately utilize the range of tools available to them to do so, such as information sharing, risk management models, technology, training, and globally accepted security standards, guidelines, and best practices. Raising awareness so that cyberspace's stakeholders can use these tools is critical to improving cybersecurity.

What are we doing now?

There are a variety of effective information technology (IT) industry and government efforts to raise cybersecurity awareness. Some key examples follow.

- U.S. IT companies founded the National Cyber Security Alliance (NCSA), a non-profit organization focused on conducting cybersecurity education and awareness programs. NCSA has become the premier cross-sector umbrella organization for public-private collaboration to increase cybersecurity awareness at home, school, and work. NCSA is also a lead partner, with the Anti-Phishing Working Group (APWG), in the "StopThinkConnect" national awareness campaign with the Department of Homeland Security (DHS).

- NCSA's National Cyber Security Awareness Month, first launched in 2003, is a multi-faceted effort held each October to disseminate security messages and information through grassroots, traditional, and social media channels.

- The Federal Trade Commission (FTC)'s OnGuard Online program provides practical tips from the federal government and the technology industry to help citizens to guard against Internet fraud, secure their computers, and protect their personal information.

- EDUCAUSE, a nonprofit association formed to advance higher education by promoting the intelligent use of IT, provides extensive information and resources on cybersecurity for the higher education community.

What more can policymakers do?

Cyberspace's stakeholders should be more aware of risks, aware of how they can secure and protect their things of value, and be responsible for taking action accordingly, just as in the offline world. Policymakers should:

- Continue to support and sponsor National Cybersecurity Awareness Month activities, and consider expanding the length of these activities beyond one month per year. *Congress and the Administration can both contribute to this effort.*

- Bolster outreach campaigns by specifically targeting those populations without dedicated IT staffs (home users, older adults, students, small businesses) with awareness videos, commercials, and free help. *The Administration should lead on this effort.*

- Build on the StopThinkConnect campaign to develop a new, general "Smokey Bear" or "McGruff the Crime Dog"-type campaign to be targeted at younger Americans regarding the importance of taking personal action. *The Administration should lead on this effort.*

- Better utilize and fund existing federal awareness programs, namely the National Cyber Security Alliance (NCSA), and ensure that U.S. Government efforts to raise awareness are coordinated among agencies to minimize redundancies and maximize impact. *The Administration should lead on this effort*.

- Promote practical, entry-level security skills in U.S. community colleges, and effectively implement the National Initiative for Cybersecurity Education (NICE) program in partnership with the private sector. *The Administration should lead on this effort.*

PRINCIPLE 6 : Efforts to improve cybersecurity must more directly focus on bad actors and their threats.

Why is this important?

Cybersecurity means understanding and mitigating threats in addition to vulnerabilities and consequences. Too often we downplay the importance of managing threats, and do not pay it the attention it needs, because it is a difficult area. Cyberspace, with its global connectivity, poses considerable challenges to those tasked with protecting it. The breadth of criminal activity and number of bad actors make getting ahead of the actors and crafting responses to incidents difficult. At the same time, we must acknowledge the analogies between the off-line and on-line worlds. These are traditional actors and crimes - the difference is the medium - and there are traditional laws and government bodies that have long been tasked with dealing with them.

Cyber threats can be grouped into four categories.

- *Crime. This includes cases in which computers are used for criminal purposes such as fraud, extortion, piracy, or theft, or used as tools to commit traditional offenses (e.g., distribution of child pornography or denial-of-service attacks).*

- *Commercial espionage. This includes cases in which competitors deliberately target the economic intelligence - namely trade secrets - of their competitors. Trade secrets include financial, business, scientific, technical, economic or engineering information, client lists, research documents, prototypes or plans for new products or services, and personnel records.*

- *Nation-state espionage. This includes cases in which governments intrude into and ex filtrate large amounts of sensitive government data from adversaries' government agencies and/or military industrial base, or engage in espionage against commercial interests.*

- *Warfare. This is a discrete category of actions by governments or terrorist groups that constitute acts of war.*[2]

[2] "Cyber acts of war" is still being defined as an international term.

What are we doing now?

Increasing attention is being paid to deterring cyber threats, especially by those governments that have the power to investigate criminal activity and the tools to respond. The IT industry takes steps as well. Some key examples are below.

- The Federal Bureau of Investigation (FBI)'s Cyber Division has specially trained cyber squads at FBI headquarters and field offices staffed with agents and analysts who investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud. The FBI partners with the Departments of Defense, Homeland Security, and others in this work.

- The Secret Service's nationwide network of Electronic Crimes Task Forces (ECTFs) brings together federal, state, and local law enforcement, prosecutors, private industry, and academia to prevent, detect, mitigate, and aggressively investigate attacks on the nation's financial and critical infrastructures.

- The Economic Espionage Act of 1996 makes the theft or misappropriation of a trade secret a federal crime. The FBI's Economic Espionage Unit uses this law to investigate economic espionage and punish criminals and spies.

- The U.S. Immigration and Customs Enforcement (ICE) Cyber Crime Center (C3) develops and coordinates investigations related to cyber crimes, child exploitation, and digital forensics. For example, its Cyber Crimes Section (CCS) investigates fraud, theft of intellectual property rights, money laundering, identity and benefit fraud, and other illegal activities.

- The Federal Trade Commission (FTC) has taken action against identity theft for a decade, providing tools to consumers, businesses, and law enforcement. The FTC's national education campaign - AvoID Theft: Deter, Detect, Defend - aims to empower consumers to protect themselves against identity theft and to minimize its damage.

- The 2004 Council of Europe Convention on Cybercrime is a binding international treaty that lays down guidelines for all governments wishing to develop legislation against cybercrime. Open to signature by non-European states, the convention also provides a framework for international cooperation in this field. It currently has 43 signatories, although only half have ratified the Convention. The U.S. Senate ratified the Convention in 2006.

- Major U.S. information technology (IT) companies utilize various methods to deter cyber threats such as training employees to understand techniques used by bad actors, limiting access to sensitive materials, and implementing tools to identify untrusted and improper behavior on networks and taking appropriate action.

- U.S. IT companies undertake various efforts to minimize being subject to commercial espionage such as ensuring information is properly stored and secured, utilizing proper disposal procedures such as deleting and destroying potentially sensitive data when no longer needed, utilizing non-disclosure agreements, and conducting background checks on potential employees.

What more can policymakers do?

Law enforcement and national security are core government functions. In both the off-line and on-line worlds, the government can best undertake this responsibility with the right laws, efforts, and information sharing practices. Policymakers should:

- Provide more resources for law enforcement to aggressively prosecute criminals globally. *Congress should lead on this effort.*

- Focus on identifying, sorting, and prioritizing threats and incidents conducted in cyberspace. *The Administration should lead on this effort.*

- Identify countries that have become safe havens for perpetrators of crime and fraud and target them for diplomatic and enforcement initiatives formulated to change their practices. *The Administration should lead on this effort.*

- Better leverage and build upon existing bilateral and multilateral agreements on cross-border prosecutions of crime and espionage before proposing new efforts or treaties. *The Administration should lead on this effort.*

- Ensure that any new bilateral or multilateral agreements, treaties, or other governance frameworks on cross-border prosecutions of crime and espionage are technology neutral and flexible enough to evolve and address emerging and new types of cyber threats. *The Administration should lead on this effort.*

- Authorize and deploy financial and technical assistance to developing countries to help them to improve their own enforcement efforts, such as by passing cyber crime legislation where it is needed, developing the law enforcement capability and capacity to fight cyber crime, and joining international efforts. *Congress should authorize and the Administration should enable this assistance.*

About the Information Technology Industry Council (ITI)

The Information Technology Industry Council (ITI) is the premier voice, advocate, and thought leader for the information and communications technology (ICT) industry. ITI is widely recognized as the tech sector's most effective advocacy organization in Washington D.C., and in various foreign capitals around the world.

ITI's members are global leaders in innovation--from all areas of the ICT sector including hardware, services, and software--the products our members create are the face of global economic growth and the heart and soul of improving peoples' lives.

ITI is dedicated to advocating for its member companies through three main divisions: Environment and Sustainability, Global Policy, and Government Relations. In these divisions ITI engages in a broad range of issues around corporate tax, trade, telecommunications, cybersecurity, workforce and STEM initiatives, accessibility, and environmental sustainability.

To help its member companies achieve their policy objectives, ITI builds relationships with Members of Congress, Administration officials, and state and foreign governments; organizes industry-wide consensus on policy issues; and enables access to global markets by working to enact innovation-friendly government policies.

ITI is the only high-tech association that compiles a comprehensive voting guide each Congress that serves as a report card for Members as well as a reflection of ITI's legislative priorities.   In addition, ITI annually publishes a High-Tech Education Report that highlights the educational initiatives its member companies are spearheading and funding to meet the needs of America's 21st century workforce.

As ICT innovation continues to propel global economic growth, impacting not only the way businesses and governments are run, but also the everyday lives of people worldwide, ITI will be there to represent the world's leading technology companies.

To learn more, please visit www.itic.org.

The IT Industry's Cybersecurity Principles for Industry and Government

Information Technology
Industry Council

Information Technology Industry Council (ITI)
1101 K Street, N.W.
Suite 610
Washington, D.C. 20005
T: 202-737-8888
www.itic.org