Cybersecurity Principles for Industry and Government

A Useful Framework for Efforts Globally to Improve Cybersecurity

Danielle Kriz
Director, Global Cybersecurity Policy
Information Technology Industry Council
Washington, DC, United States
dkriz@itic.org

***Abstract*—To better inform the public cybersecurity discussion, in January 2011 the Information Technology Industry Council (ITI) developed a comprehensive set of cybersecurity principles for industry and government [1]. ITI's six principles aim to provide a useful and important lens through which any efforts to improve cybersecurity should be viewed.**

Keywords-Information Technology Industry Council; ITI; principles; cybersecurity; industry; government; framework

I. Introduction

Cybersecurity is rightly a priority for governments globally. 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.

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.

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

II. The Six Principles and Their Importance

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

It is well known that the private sector owns and operates 85% of critical infrastructure in the United States, and that the 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,

978-0-615-51608-0/11 ©2011 EWI

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.

B. Principle 2: Efforts to improve cybersecurity must properly reflect the borderless, global, interconnected cyber infrastructure

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, 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.

C. Principle 3: Efforts to improve cybersecurity must be able to adapt rapidly to emerging threats, technologies, and business methods

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.

D. Principle 4: Efforts to improve cyberspace must be based on risk management

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.

E. Principle 5: Efforts to improve cybersecurity must focus on awareness

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.

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

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 exfiltrate 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 ("cyber acts of war" is still being defined as an international term).

III. CONCLUSION

ITI's principles can guide policymakers in developing and facilitating an effective public policy framework that enhances security while maintaining the overall benefits of cyberspace.

REFERENCES

[1] Information Technology Industry Council, "The IT Industry's Cybersecurity Principles for Industry and Government," http://www.itic.org, January 2011.