Policy recommendations

Modern cybercrime prevention

The opportunity

The combination of expanded access to the internet, the explosive increase in connected devices, and the rapid expansion of innovative cloud-based services is creating tremendous economic and social opportunities for consumers, governments, and businesses.

The challenge

Today, governments are struggling to confront the growing threat, sophistication, and prevalence of cybercrime, including: identity theft; online scams and fraud; malware distribution schemes; attacks against the integrity of data and systems; and the online distribution of illegal content.

Increasingly, these crimes are committed by organized groups operating in one country that target victims in another. The cross-border nature of cybercrime complicates enforcement, and inadequate legal frameworks in some countries have created safe havens for cybercriminals.

The financial impact of all this cybercrime is large and growing. In 2015, the British insurance company Lloyd's estimated that cyberattacks cost businesses as much as 400 billion U.S. dollars a year, an amount that is expected to increase in the years ahead.

In addition to these economic costs, there are less tangible impacts including lost confidence in internet commerce, the erosion of individual privacy, and diminished trust in online services.

Each of these effects threatens to slow adoption of cloud-based innovation and reduce the benefits of promising new technologies.

Policy recommendations

Harmonization of cybercrime laws around the world combined with initiatives to facilitate faster and more effective coordination between law enforcement agencies is essential. These efforts can be pursued in an environment where each country respects the sovereignty of other nations, and where the fundamental rights and liberties of citizens are fully respected. To strengthen enforcement in a balanced way, governments should consider the following steps:

Strong enforcement and balanced rules. To fight cybercrime effectively, law enforcement and industry must have the legal tools necessary to pursue cybercriminals wherever they are. Governments should work to update their criminal laws so that they are capable of addressing both existing and emerging threats posed by online criminals. At the same time, these laws should be conscious not to adversely affect innovation or the adoption of new technologies. They should also support efforts at industry self-regulation.

Adopt laws that are consistent with broadly accepted international conventions. The Council of Europe's Budapest Convention provides a good model for cybercrime legislation that can help harmonize laws and drive better cooperation across borders. Such international coordination and cooperation will help eliminate safe havens for malicious actors and minimize the risks that arise when intermediaries and other innocent parties are subject to conflicting obligations or liabilities.

Facilitate information sharing. In some cases, companies with information about online crimes face potential liability under privacy, data protection, or other laws if they voluntarily share that information with law enforcement.

To facilitate and encourage timely cooperation, governments should clarify rules for data-sharing by companies with law enforcement. Lack of clarity about rules for information-sharing and liability risks may prevent companies from working with law enforcement agencies, even when cooperation could be critical to preventing or responding to cybercrime. In addition—as described in the recommendations for government access to data—enhancing the procedures and mechanisms for international, cross-border cooperation by modernizing mutual legal assistance processes will help streamline enforcement efforts and help clarify important issues related to jurisdiction and access to evidence.

Develop new ways to prevent cybercrime. Current efforts to enforce laws against cybercrime are woefully inadequate given the enormity of the problem. New approaches to going after the criminals are needed. One example may be a pilot program launched by the City of London police in partnership with private law firms using civil courts to seize cybercriminals' assets. Finding other ways to scale enforcement efforts will be critical.

Work with industry on best practices and emerging issues. Governments can take advantage of the expertise and resources of the private sector in the fight against cybercrime. Opportunities include working with industry to educate enforcement officials about new and emerging threats that technology suppliers experience in the real world and that their customers see as priorities. Governments often lack sufficient resources to deal effectively with cybercrime. Working with the private sector can help them achieve greater success, which will help drive trust in online computing.

Evidence and further reading:

Convention on Cybercrime (Budapest Convention)

The Guardian: "Police to Hire Law Firms to Tackle Cyber Criminals in Radical Pilot Project"

For links to this and other resources, please visit:
http://www.microsoft.com/cloudforgood