February 2013

Cyber Security

Key Points

- Cyber security is the set of activities and resources that enable citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner. Governments face the challenge of developing security practices that address four types of threats: conventional cyber crimes, military espionage, economic espionage, and cyber warfare.

- Microsoft works to help create safer, more trusted computing experiences by continually improving the security of its products and services, developing best cyber security practices, and collaborating with governments and industry partners to reduce threats to cyber security.

- An effective approach to cyber security requires collaboration between the public and private sectors to mitigate threats and vulnerabilities. This collaboration also helps develop sustainable public policy frameworks that advance cyber security and enable innovation in the private sector.

BACKGROUND

Cyber security covers the security of information, operations, and computer systems. It is the set of activities and resources that enables citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner.

Cyber security means different things to different audiences. For businesses, cyber security is about ensuring, through operational and information security, the availability of critical business functions and the protection of confidential data.

For governments, it is about protecting citizens, enterprise, critical infrastructure, and government computer systems from attack or compromise. Governments face the challenge of developing cyber security best practices that address four categories of threats that have the potential to affect public safety and national security.

First, they must protect society from a broad range of conventional cyber crimes, such as fraud or vandalism, perpetrated by individuals, organized crime syndicates, and loosely affiliated groups of "hacktivists." Next, countries may need to combat military espionage that uses computing technologies, as illustrated by repeated allegations of cross-border exfiltration of sensitive military data. Nations must also defend against economic espionage and other such actions where governments have philosophical differences about what constitutes acceptable behavior. Finally, governments must grapple with cyber warfare, forcing a reassessment of traditional notions of war.

With societies around the globe growing ever more dependent on information and communications technologies, the imperative of cyber security will grow significantly over time. Accordingly, policymakers should think strategically about mitigating cyber threats.

MICROSOFT APPROACH

As a business, Microsoft manages risk through ongoing efforts to enhance security in product development, the supply chain, and operations, as well as deepen its understanding of social engineering tactics.

- **Enhancing security in product development.** To address product vulnerabilities, Microsoft uses its Security Development Lifecycle, a security assurance process that relies on a collection of mandatory security activities grouped by the phases of traditional software development.

- **Enhancing security in the supply chain.** To help manage risks to Microsoft's products and services in the supply chain, the company deploys identity and access management controls, the Security Development Lifecycle, policies and procedures that monitor the integrity of Microsoft software, and anti-counterfeit measures.

  Microsoft is also actively involved in industry efforts to develop both best practices for managing risk in the supply chain, and product assurance tools such as the Software Assurance Forum for Excellence in Code (SAFECode).

- **Enhancing operational security.** To help organizations better manage operational security risks, Microsoft shares its security best practices and provides regular software updates. Microsoft's patch management system, with its automated releases for the second Tuesday of each month, enhances operational security through standard, predictable, and regular releases of software patches.

- **Enhancing security against social engineering.** Microsoft helps combat social engineering by sharing its security best practices and developing instructional materials for consumers. It also provides tools like the Windows Internet Explorer SmartScreen Filter, which helps to protect people from evolving social engineering threats.

Building on various internal risk-management programs, Microsoft continually seeks to improve the efficiency and effectiveness of these risk-management approaches. Microsoft shares those practices with industry and policymakers as appropriate.

In addition, Microsoft's Global Security Strategy and Diplomacy team partners with national governments, industry partners, and nonprofit organizations to enhance the security of the Internet. To that end, the team promotes trustworthy plans and policies, and helps protect processes key to national and economic security as well as public health, safety, and confidence.

POLICY CONSIDERATIONS

- Governments should work with the private sector to strengthen the security, privacy, and reliability of the cyber ecosystem and to defend against cyber threats. Microsoft believes that such strategic partnerships and outcome-focused initiatives are critical to advancing a safer Internet.

- In partnership with the private sector, policymakers should build on industry best practices for risk-based, technology-neutral approaches to mitigating cyber threats. When policymakers rely upon tested frameworks, they help ensure that hard-won security gains are maintained and technological innovations are given maximum opportunity to succeed.

- As governments work to advance their national security goals through effective cyber security, they should also consider their unique information technology infrastructures. Public-private partnerships can help identify gaps between national security expectations and what commercially available technologies can offer to address areas of specific concern.

Helpful Resources

Microsoft Global Security Strategy and Diplomacy
www.microsoft.com/gssd

Rethinking the Cyber Threat: A Framework and Path Forward
aka.ms/cyber-threat

Microsoft Security Intelligence Report
www.microsoft.com/sir

Software Assurance Forum for Excellence in Code (SAFECode)
www.safecode.org

Microsoft for Public Safety & National Security: Malicious Software Crimes
aka.ms/DCU-economic-crime