|  |  |
| --- | --- |
| **web_banner** | **Microsoft & Critical Infrastructure Protection** |

**Key Points**:

* Today’s critical infrastructures – banking, communications, transportation, energy, healthcare, government – rely on information technology (IT) to deliver services essential to the public health and safety, commerce, and security of any country.
* Protecting critical infrastructures and ensuring that they can rapidly recover from a wide range of hazards including deliberate attack, human error, technological failure, or natural disaster, requires a public-private partnership.

Societies and governments, and the critical infrastructures on which they depend, face significant and growing cyber-security challenges.

Working with our government partners and industry peers, Microsoft is committed to preempting, detecting, and identifying the sources of cybercrime, both to protect the computing experiences of our customers and the cyber-security of our critical infrastructures.

**Background**:

Governments are increasingly focused on the role critical infrastructures play in supporting the overall economy and security of their nations. While definitions may vary slightly, critical infrastructures are generally thought of as the key systems, and the services and functions they provide that, if disrupted, would have a debilitating impact on public health and safety, commerce, and/or national security. Critical infrastructure services include those provided by the communications, energy, banking, transportation, and public health and safety sectors, as well as essential government services.

Over the past two decades, rapid advances in software, information technology services, and communications have enabled many traditionally separate infrastructures and business operations to become more interconnected. This interconnection has transformed virtually every aspect of society and enables businesses and governments to manage and streamline their operations. Our broad reliance on software, services, and communications, and the benefits they provide, however, also makes them a particularly attractive target of terrorists, criminals, and other sophisticated attackers. To address this threat requires unprecedented cooperation and effective action by technology vendors, governments, businesses, and consumers.

**A Shifting Threat Landscape**

As computing has become more integrated into critical infrastructures and an ingrained part of commerce, the threats to it have become increasingly sophisticated and are now driven by malicious intent. Where publicity once motivated many digital attacks, criminal financial gain spurs most attacks today. So, in addition to viruses and worms that shut down systems, we must contend with spyware that seeks to steal personal information; worms and viruses that hijack computers and install “backdoors” or “bots” that allow the computer to be controlled by an attacker; and automated social-engineering threats where attackers try to trick people into divulging personal data or installing software unknowingly. These trends have shifted the risk-profile for critical infrastructure.

Recent improvements to operating systems, platform software, and network security have forced criminals to change tactics. For example, there is a trend toward attacks farther up the “stack” from the operating system to the application layer. The focus on applications goes far beyond Microsoft applications, and impacts independent software vendors and user communities. These types of attacks are increasingly targeted at specific victims, such as large commercial enterprises with valuable data or a critical infrastructure, and seek to obtain information that has financial value (e.g., bank-account data).

**Trustworthy Computing and Infrastructures**

In 2002, Microsoft launched the Trustworthy Computing (TwC) initiative, which made providing a secure, private, and reliable computing experience for everyone a top company priority. Microsoft’s commitment to TwC does not end at the desktop. Rather, TwC includes enabling the most critical components of infrastructures to operate within a cyber ecosystem that is more secure and resilient. In December 2006, Microsoft formed a dedicated Critical Infrastructure Protection Team to better address the unique challenges faced in protecting critical infrastructure. Our goal is to enhance critical infrastructure security by increasing the trustworthiness of software and IT services, and by collaborating with governments and critical infrastructure providers to reduce and manage risks.

Security has been and remains an area of continued focus for Microsoft, and we have made significant progress with the recent release of Windows Vista and Office 2007. Both products were developed using the Security Development Lifecycle, a process that Microsoft has adopted for the development of software that needs to withstand malicious attack, and both have new security features.

But, technology alone won’t address the challenge. Taking a holistic defense-in-depth approach – including the use of more secure technologies engineered from the start with security in mind, the timely installation of security updates, the use of anti-virus and anti-spyware solutions, and the adoption of risk-management practices and user-education programs – can equip organizations to better protect themselves from evolving threats. Microsoft is actively assisting customers in these areas: continually making computer updates easier and more automatic; providing anti-virus and anti-spyware (Windows Defender) solutions and the free Microsoft Malicious Software Removal Tool, as well as usable guidance for enterprises and end-users. Separate from what Microsoft does on its own, we are working in partnership with governments and industry to help protect critical infrastructures by protecting the IT ecosystem.

**Continuing Commitments**

Societies and governments, and the critical infrastructures on which they depend, face significant and growing cyber-security challenges. Working with our government partners and industry peers, Microsoft is committed to preempting, detecting, and deterring cyber-criminals, both to protect the computing experiences of our customers and the cyber-security of our critical infrastructures.