February 2013

Critical Infrastructure Protection

Key Points

- National security and international policy concerns about critical infrastructure have evolved as key systems of public life, health, and safety have become increasingly interconnected and dependent on IT infrastructure.
- The unique security challenges of complex critical infrastructures require an unprecedented response. Technology vendors, governments, businesses, and consumers must work together to innovate, develop, and deploy effective solutions.
- The Microsoft Global Security Strategy and Diplomacy team works with national governments, industry, and nonprofit organizations to strengthen and improve cyber security, promote trustworthy plans and policies, and help protect key processes and functions for national and economic security, and public health, safety, and confidence.

BACKGROUND

Governments are increasingly focused on the role critical infrastructures play in supporting the overall economy and security of their nations. 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, or national security.

Advances in software, communications, and IT services have substantially improved and connected these key systems, but their interconnectedness is also a cause for growing concern. Critical infrastructures are attractive targets for criminals, and increasingly sophisticated attacks on interconnected systems have the potential to cause widespread damage and disruption.

The unique security threats to complex critical infrastructures require an unprecedented response. Technology vendors, governments, and businesses must work together to innovate, develop, and deploy effective solutions. Microsoft is dedicated to supporting these relationships and plans to help detect and preempt the sources of threats to critical infrastructure. As part of that commitment, the company formed the Global Security Strategy and Diplomacy team.

MICROSOFT APPROACH

The Global Security Strategy and Diplomacy Team is dedicated to enhancing the security and resiliency of critical infrastructures by increasing the trustworthiness of software and IT services, in part through the development of innovative solutions. In addition, the team collaborates with governments and critical infrastructure owners and operators to reduce and manage risks.

Effective efforts to protect critical infrastructure fall within these three areas:

- **Trustworthy plans and policies.** Clear, effective policies lead to well-defined goals and priorities that help IT professionals secure resources and focus investments on top-priority risks. Microsoft collaborates to develop effective, flexible, and innovative national and global solutions to help secure critical infrastructure.

- **Resilient operations.** Microsoft helps reduce the impact of disruptions in critical infrastructure by sharing best practices and creating a cohesive front when disruptions occur. Greater resiliency will allow IT professionals to manage their environments with greater confidence.
- **Innovative investments.** Continuous innovation leads to advanced security capabilities, and innovative environments allow IT professionals and organizations to benefit from new thinking, improved products, and better processes, guidance, and training. Microsoft supports collaborative efforts to develop innovative practices, programs, education, and research to develop secure solutions for critical infrastructures.

POLICY CONSIDERATIONS

Leaders worldwide are concerned about the security implications of increasingly interrelated global systems, especially economic stability, climate change, and national security. The potential exists for disruptions of critical infrastructure to cause unprecedented, widespread damage (similar to the recent global financial crisis).

These issues pose daunting challenges for those who must predict and manage their outcomes, and they require a united response from governments and businesses. Innovative public-private relationships must develop robust plans to secure and protect critical infrastructures from ever-changing threats and sophisticated attacks. Solutions include:

- **Better, more secure development:** using proven, effective processes similar to the Microsoft Security Development Lifecycle.
- **A unified response:** supporting relationships and investments that identify assets and manage critical function risks.
- **Shared information and tested response mechanisms:** helping governments and critical infrastructure operators maintain situational awareness and respond quickly to prevent, mitigate, and recover from nationally or globally significant threats.
- **Next-generation network technologies:** deploying secure cutting-edge solutions to increase communications capability and resiliency.
- **More information technology security research:** solving existing problems and preparing for those in the future by strengthening the pipeline of academic and professional knowledge through educating, mentoring, and training future professionals and leaders.

Helpful Resources

Microsoft's Security Response Center
www.microsoft.com/msrc

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

The Industry Consortium for Advancement of Security on the Internet
www.icasi.org

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