National Cybersecurity Strategy

Microsoft Policy Papers

Cybersecurity has become a national concern

Societies around the globe are growing ever more dependent on information and communications technology (ICT), relying on them for easier access to information and communication, more efficient delivery of government services, and as a key component of national economy. However, this interconnectivity has also created interdependencies and risks that need to be managed at the *national level*. These threats span identity theft and fraud to politically motivated "hacktivism," and sophisticated economic or military espionage, all of which threaten citizens and corporations alike. Enhancing cybersecurity and protecting critical information infrastructures has, therefore, become essential to every nation's security and economic well-being.

Achieving greater cybersecurity is no easy undertaking and requires cooperation between government authorities, the private sector and civil society. National cybersecurity strategies have emerged as the preferred and most effective mechanism for managing risks and responding to threats posed to the ICT infrastructure of a nation. To date over 70 countries have adopted national cybersecurity strategies and a number of international organizations have put forward guidelines and suggestions as to how to make these effective[1].

What is a national cybersecurity strategy?

A national cybersecurity strategy typically takes the form of a policy framework that outlines a vision and articulates the priorities, principles, and approaches needed to understand and manage risks nationally. Priorities for national cybersecurity strategies will vary by country. In some countries, the focus may be on protecting critical infrastructure risks, while other countries may focus on protecting intellectual property or on improving the cybersecurity awareness of newly connected citizens.

Effective national strategies can help meet the cybersecurity needs of all of those communities by, for example:

- Educating citizens about the nature of cybersecurity environment and potential mitigation approaches;
- Opening up a broader societal dialogue on cybersecurity;
- Cleary articulating the national priorities, principles, policies and programs for achieving those;
- Specifying the roles and missions of each government agency and non-governmental organization involved in enhancing cybersecurity;
- Stipulating goals, milestones, and metrics to measure and communicate progress in addressing the issues identified;
- Ensure proper resourcing.

The most successful national strategies share three important characteristics. First, they are embedded in *"living"* documents that have been developed and implemented in partnership with key public and private stakeholders. Second, they are based on *clearly articulated principles* that reflect societal values, traditions, and legal principles. Programs created by government in the name of security can potentially infringe on these rights and values if they are not articulated and integrated as guiding principles. Third, the strategies are based on a *risk-management approach* wherein governments and private sector partners agree on the risks that must be managed, mitigated, or even accepted.

[1] For example:

ITU Cybersecurity Strategies: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

Commonwealth Approach for Developing National Cybersecurity Strategies http://www.cto.int/strategic-goals/cybersecurity/national-strategies/

National Cybersecurity Strategy

Microsoft Policy Papers

Policy Considerations

Microsoft believes that every nation should have a national strategy for cybersecurity, and we strongly support governments taking steps to protect their most essential information and ICT systems, the ones needed to support national security, the economy and public safety. This is particularly important because unlike with the legal regimes covering privacy, which have evolved over time to include strong laws aimed at protecting consumer information, cybersecurity does not have corresponding legal regime. Moreover, many of the organizational structures have not yet been put in place.

As a global services and devices company, Microsoft has observed dozens of national approaches aimed at addressing cyber risk and has developed views about what makes for an effective national cybersecurity strategy. The main driver behind the adoption of a national cybersecurity strategy should be a commitment to securing the national cyber infrastructure and the services upon which a country's digital future and growth depend, while also building trust and confidence in the use of ICT and promoting sustainable development. Moreover, Microsoft recommends the following six foundational principles as the basis for a national strategy:

- Risk-based. Assess risk by identifying threats, vulnerabilities, and consequences, then manage it through mitigations, controls, costs, and similar measures;
- Outcome-focused. Focus on the desired end state, rather than prescribing the means to achieve it, and measure progress towards that end state;
- Prioritized. Adopt a graduated approach to criticality, recognizing that disruption or failure are not equal among critical assets or across critical sectors;
- Practicable. Optimize for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors;
- Respectful of privacy and civil liberties. Include protections for privacy and civil liberties based upon the established privacy and civil liberties policies, practices, and frameworks;
- Globally relevant. Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind wherever possible.

Establishing a national strategy for cybersecurity is an important element of the overall national and economic security strategy for a government. However, a national strategy cannot solve all of a nation's cybersecurity challenges. Incidents will still occur even with the clearest of principles, the most thoughtful of risk-assessment and risk-management frameworks, and the best information-sharing and incident-response capabilities in the world. However, by creating a principled approach to cybersecurity, thinking holistically and realistically about risks and threats to a nation and its most essential enterprises, and deploying strong practices to prevent, detect, contain, and recover from an incident, a nation stands a far greater chance of lessening the severity of an incident. Only then can the digital ground lost to cyber criminals and attackers be reclaimed

For more information refer to our whitepaper: *Developing a National Strategy for Cybersecurity.*[2]

[2] Developing a National Strategy for Cybersecurity: http://download.microsoft.com/download/B/F/0/BF05DA49-7127-4C05-BFE8-0063DAB88F72/Developing_a_National_Strategy_for_Cybersecurity.pdf