Developing a National Strategy for Cybersecurity

FOUNDATIONS FOR SECURITY, GROWTH, AND INNOVATION

Cristin Flynn Goodwin
J. Paul Nicholas

October 2013

Contents

Executive Summary

Cybersecurity has become a priority for governments around the world. Major cyberattacks, data losses, and compromised networks fill the headlines, and governments, the private sector, and citizens all recognize the need for action to improve cybersecurity. Governments worldwide are struggling with questions around how to do this while balancing privacy, civil liberties, and cost.

Over the past decade, national governments have been developing strategies to address emerging security issues associated with the rapidly expanding use of information and communications technology (ICT). These "cybersecurity" issues have developed into significant national-level problems that require government consideration, including the protection of assets, systems, and networks vital to the operation and stability of a nation and the livelihood of its people. Threats against these vital assets target corporations and citizens, and include cybercrime such as identity theft and fraud, politically motivated "hacktivism,"and sophisticated economic and military espionage.

What is "cybersecurity"?

There are many terms associated with cybersecurity: information security, critical infrastructure, information assurance, standards, security baselines, security risk management, information systems, and more. Understanding the relationships between these terms and disciplines is essential.

Unlike legal regimes covering privacy, which have evolved over time to include strong laws aimed at protecting consumer information and preventing online fraud, cybersecurity has not evolved a corresponding legal regime over the past decade. In the absence of regulation, ICT companies have developed standards and best practices to help establish strong security protections for products and services.

As governments around the world begin to consider the appropriate legal framework for cybersecurity regulation, it is Microsoft's view that such a framework should be based upon a principled national strategy that sets a clear direction to establish and improve cybersecurity for government, academia, enterprises, consumers, and the ICT companies who serve those communities.

Microsoft strongly supports governments taking steps to protect their most essential information and ICT systems—those needed to support national security, the economy, and public safety. A national cybersecurity strategy is critical for managing national-level cyber risks and developing appropriate legislation or regulation to support those efforts. As a global software 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.

This document contains recommendations for policymakers for developing or improving a national security strategy.

What Is a National Strategy for Cybersecurity?

A national cybersecurity strategy outlines a vision and articulates priorities, principles, and approaches to understanding and managing risks at the national level. 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, and still others may focus on improving the cybersecurity awareness of newly connected citizens.

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 not articulated and integrated as guiding principles. Third, the strategies are based on a risk-management approach where governments and private sector partners agree on the risks that must be managed or mitigated, and even those that must be accepted.

A national strategy, if developed correctly, can meet many needs of government, the private sector, and the citizens of the country. A national strategy can:

National cybersecurity strategy
Educate citizenry about the nature of the problem and mitigation approaches.
Give citizens and organizations an opportunity to provide their input into a national dialogue.
Clearly articulate the national priorities, principles, policies and programs.
Specify the roles and missions of each government agency and non-government organization involved.
Stipulate goals, milestones, and metrics to measure and communicate the extent of progress in addressing the issues.
Ensure appropriate resourcing.

Microsoft believes that every nation should have a national strategy for cybersecurity. Microsoft has a unique view of cyber threats, as each month the company receives cybersecurity threat information from more than 600 million systems in more than 100 countries and regions. In addition, Microsoft works closely with governments, enterprises, and customers around the world to assess, manage, and respond to risks. From this experience, Microsoft has observed four key cyber threats worldwide: cybercrime, economic espionage, military espionage, and cyber conflict. These threats can have serious implications for critical infrastructures, governments, and many other key stakeholders. Understanding the complex threat landscape and grappling with the breadth of cyber attackers, especially those affiliated with nation-states or organized crime, is a challenging proposition. To counter this threat, governments need to design and implement a national strategy for cybersecurity.

A Principled Approach to Cybersecurity

At its foundation, a national strategy must reflect the cultural values and beliefs of the nation. It must have a clear set of principles that help frame decisions about how to identify, manage, or mitigate cybersecurity risks in a way that balances civil rights and liberties, costs, and a range of other possible priorities.

Specifically, Microsoft recommends the following six foundational principles as the basis for a national strategy; it must be:

Cybersecurity Strategy Principles	
	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 Fair Information Practice Principles and other 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.

Each of these principles is reflected in the sections below, and, taken together, can form the basis of a national strategy to secure cyberspace.

Building a Risk-Based Approach to National Cybersecurity

Once a nation has set its cybersecurity priorities, a national strategy should focus on the risks that must be identified, managed, mitigated, or accepted. National cyber risks are typically thought of as risks to information systems, that, if exploited, could negatively impact national security, economic well-being, or public safety to a significant degree. Governments must now confront more complex challenges, including attacks that seek to exfiltrate sensitive data or intellectual property, or even destroy machines critical to business or government operations. Governments must also manage risks caused by critical dependencies across infrastructures, such as ICT's dependence on electrical power.

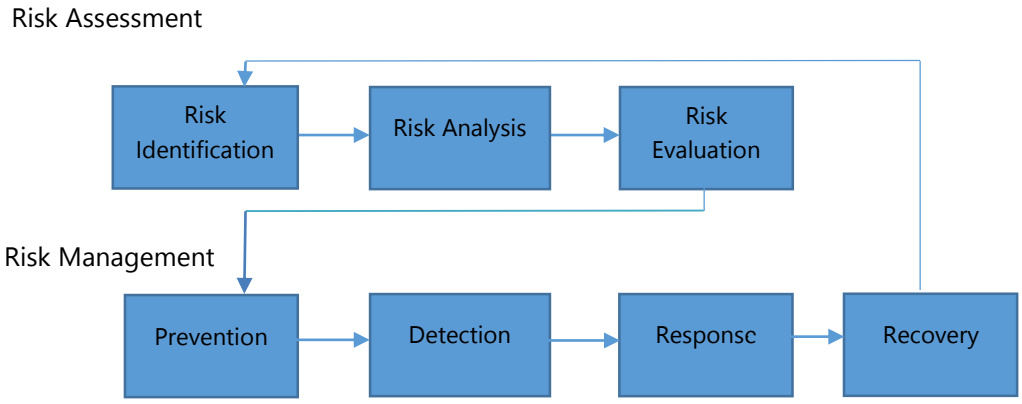
Governments face four principal challenges in establishing risk-based approaches to national cybersecurity: (1) articulating and understanding the relationship between security and resiliency; (2) developing national-level capabilities for risk assessment, risk management, information sharing, incident response, and strategic analysis and warning; (3) establishing policies that reduce national cybersecurity risks while encouraging technological innovation; and (4) identifying and mitigating key interdependencies on other sectors.

Recommendations for a National Strategy

In order to develop a risk-based approach to managing national cybersecurity risks, countries must first create and articulate a framework for assessing national cyber risk and prioritizing protections. This all starts with a clear focus on risk: assessment, management, acceptance, and review.

Develop a clear structure for assessing and managing risk across the strategy

When choosing a national approach to managing risk, international standards and best practices can help governments in the process. In order to simplify the approach to risk for the purpose of a national strategy, it is helpful to use the following taxonomy.



This structure enables the broad application of process rather than a set of prescriptive controls. It is important that any national strategy lay out the principles of risk assessment and management, but stop short of requiring specific controls. Controls should be identified by the infrastructure owners and operators, who best understand the specific needs and dependencies of their systems.

Understanding national threats through threat modeling

In order to establish national cybersecurity priorities, a risk framework must reflect an understanding of the motives of threat actors; potential avenues for attack or exploitation; and the key assets or functions that could be targeted by criminals, non-state actors, and state-sponsored organizations. When developing national threat models, governments should seek input from a variety of sources, including government and law enforcement agencies, the private sector, and academia. Consulting a wide range of stakeholders equips national governments to prioritize their defensive efforts. The prioritization of threats will differ between countries, given factors such as ICT penetration, levels of economic development, and geopolitical considerations.

Microsoft has identified four major categories of cyber threats to simplify the threat model used in the assessment process.[1] Categorizing the threats in this manner makes it easier to assess them more clearly and then develop preventive and reactive strategies. Categorization can also help reduce the paralysis that may occur when governments attempts to design a single strategy for the myriad of threats that involve information technology.

The four major categories of cyber threats:

- **Conventional cybercrimes.** These crimes include cases in which computers are targeted for traditional criminal purposes, or used as tools to commit traditional offenses including fraud, theft of intellectual property or financial instruments, abuse or damage of protected information technology systems, and even damage of critical infrastructure. These crimes span those committed by individual hackers through those committed by organized crime entities.
- **Military and political espionage.** These attacks include instances in which nation-states intrude into and attempt or succeed to exfiltrate large amounts of sensitive military data from government agencies or the military-industrial base, or use third parties to do so on their behalf.
- **Economic espionage.** This category applies to governments (or third parties that are acting on their behalf) stealing intellectual property that was created in other nations, or tolerating domestic companies stealing information from foreign competitors.

[1] http://www.microsoft.com/en-us/download/details.aspx?id=747

- **Cyber conflict or cyber warfare.** Asymmetric warfare has significant implications for cyberattacks, since the Internet makes it possible for anonymous and difficult-to-trace individuals or organizations with slight resources to engage a nation-state in cyber conflict. Recently, 15 governments including China, Russia, and the United States agreed that the United Nation charter applies in cyberspace and affirmed the applicability of international law to cyberspace. [2]

The threats described above can have serious implications for critical infrastructures, including the theft of sensitive data, damage to business or operational systems, disruption of services, and other scenarios that could result in substantial financial loss and compromise public safety or national security. Each of these four areas should be included in the threat model for the national strategy.

Document and review risk acceptance and exceptions

When implementing a risk-based national cybersecurity strategy, governments will likely find that some risks will need to be accepted, resulting in exceptions to standards in order for government or critical infrastructure to deliver services. Since it is impossible to mitigate all risk, frameworks for national risk developed under the parameters of the national strategy should include clear guidelines governing how risks are accepted and documented. Guidelines should also articulate when an asset or system (such as digital trust infrastructure) is so vital that it must be protected at a higher standard. They should assign responsibility for accepted risks to pertinent personnel and, as discussed more fully below, develop appropriate incident response plans to manage these risks in times of crisis. Registries of accepted risks should be reviewed on an ongoing basis to ensure that critical government and privately owned systems are not needlessly exposed.

Make national cyber risk assessment and management an ongoing process

As noted above, a national strategy is intended to be a living document that continues to evolve to meet the security needs of the nation and the technology capabilities of its infrastructure. Risk assessment and risk management should be a continual process, not an end state. As technology evolves and threat actors grow more sophisticated, risk assessments and evaluations will have to adapt and consider if current control are still sufficient. Additionally, technologies may become available that will allow for effective mitigation of previously accepted risks. Due to the dynamic nature of cybersecurity, risk-management initiatives should be regularly updated as an ongoing process. Any national strategy must continue to prioritize this review as a part of its principles.

[2] http://cnsnews.com/news/article/us-china-among-15-countries-agreeing-un-charter-applies-cyberspace#sthash.y9G5beB4.dpuf

Establishing Clear Priorities and Security Baselines

Threat models and risk assessments help define the priorities of a national strategy. In turn, these priorities should provide guidance to regulators and infrastructure owners and operators managing the most significant risks to a nation's ICT infrastructure. In setting clear priorities and establishing a security baseline for a national strategy, there are four principles that should remain "front of mind" for governments: the strategy should be outcome-focused; prioritized; practicable; and globally relevant.

A national strategy should establish a process to create a "critical security baseline" for ICT systems that are determined to be nationally significant. Achieving a security baseline will significantly reduce the risk facing a nationally significant entity. Some governments have adopted well-known security approaches to help manage risk, such as the ISO/IEC 27000 family of standards or the U.S. National Institute of Standards and Technology (NIST) Special Publication series, while others have adopted a "Top 20" approach to prioritize mitigations. Microsoft recommends the use of international standards–based frameworks where possible. In many instances, cybersecurity risks evolve too fast to be addressed by international standards alone. Additional, risk management activities and innovation will be needed to augment the foundational efforts from standards and respond to changing risks.

In addition, the national strategy must also take into consideration the broad security needs of the nation, and not just the most nationally significant assets or infrastructures. The unfortunate reality is that many organizations, including government agencies and enterprises that may be considered nationally significant, have largely failed to implement even the most basic, minimum cybersecurity practices. A recent report published by Verizon found that 97 percent of investigated network breach incidents in 2012 could have been prevented by using simple or intermediate security controls.[3] The strategy should therefore also establish "minimum security baselines" for all users of ICT, regardless of criticality. These minimum acceptable levels of security should be based on international standards and best practices, and should also be tailored by sector as appropriate. This approach recognizes the role that non-critical government, enterprise, and individual end users play in enhancing national cybersecurity.

[3] Verizon RISK Team, *2012 Data Breach Investigations Report*. <http://aka.ms/Verizon-Breach-Report-2012>, March 22, 2012.

Recommendations for a National Strategy

Set clear security priorities consistent with the strategy's principles

Government and industry provide certain critical services and functions whose compromise, damage, or destruction through a cybersecurity incident could have national significance. Additionally, governments maintain sensitive national security information and systems that must also be protected from compromise, destruction, or disruption. However, the challenge of prioritizing these systems involves difficult trade-offs between the many roles that government must serve in protecting citizens and providing national security. Having a clear process to ensure that not all assets, systems, networks, or data are identified as "high priority" is critical to the successful implementation of the framework within the federal government enterprise.

Establish both critical and minimum security baselines

A national strategy can set the context for establishing a cybersecurity baseline for government systems and elements of critical infrastructure. Subsequently, there may be other appropriate security measures recommended for use more broadly in a range of government systems, critical infrastructures, enterprises, and consumers. The security baselines and appropriate security measures establish a flexible foundation upon which the nation can drive security enhancements for citizens. The strategy should recognize the need to include:

1. Securing Government Systems

The government is responsible for participating in cybersecurity standards development, as well as establishing and meeting security baselines for critical and non-critical information and government systems. Strategies should task states and localities with doing the same for their own systems. In order to meet these security baselines, government should hire or train cybersecurity and forensics experts to manage and defend networks. Finally, governments should establish and enforce procurement policies that result in the purchase of ICT products and services that are developed using a secure development process, and then configured and deployed commensurate with risk.

2. Critical Information and Information Systems Baselines

The strategy should also call for government, in concert with private industry, to establish security baselines for government information and information systems deemed to be critical. These baselines should also consider broad cross-sector interdependencies and promote means to reduce these risks. Once those government baselines are set, it is useful to assess the state of critical infrastructure, and consider the extension of those government baselines to certain critical infrastructures if enterprise approaches outlined below are insufficient to meet a clearly articulated threat or risk.

3. **Enterprise Baselines**

   Unlike critical information and infrastructure, where attacks can create immediate national security concerns, attacks against enterprises can create serious economic impacts for the individual company. But attacks on enterprises are less likely to create national-level economic or security risks. However, over time, the theft of intellectual property, business secrets, personally identifiable information, or funds can create risks to the competitiveness of the nation. Government can encourage enterprises to implement minimum security baselines to protect their most valuable data and operations by sharing best practices, and lessons learned from their own government agencies.

4. **Individual Baselines**

   Threats against individual Internet users are unlikely to create situations of national importance, but in the aggregate, and over time, they can be concerning. For example, with the increasing profitability of cybercrime and utility of botnets to cybercriminals, attacks against individuals in the aggregate can eventually become significant at the national level. Setting a baseline that includes consumers will help service providers and consumers alike to migrate toward a more secure environment, which is consistent with the needs of the strategy.

Set clear roles and responsibilities

The national strategy should call for the creation of clear roles and responsibilities that support the essential functions of a security baseline, and, if necessary, appropriate authorities to support those functions. Often, roles and responsibilities are varied, and distributed across an organization. If there is no agency in a country with clear authority over ICT and security, the national strategy should call for regulation or legislation to establish an agency with appropriate skills, authority, and resources to develop an ICT security baseline and implement the other requirements of the national strategy. The development and implementation of security baselines can advance the development of cybersecurity capabilities in both governments and private sector entities.

Ensure operational security and resiliency

ICT infrastructure is of little value if it does not meet its core function of being available to meet a particular user's need. When the national strategy sets the parameters for creating a security baseline, it should also consider the operational security of assets and networks, as well as the requirement to identify and set appropriate resiliency requirements. It is essential that the relevant agencies have the requisite resources and skills to meet the operational security needs set forth in the national strategy. Moreover, the strategy should also consider what level of resources, standards, and organizational support is needed for private sector ownership and operation of essential ICT functions, and encourage regulators and legislators to consider appropriate incentives, training, and support in order to facilitate private sector capabilities.

Recognize a role for continuous monitoring of systems and protection of data

In an increasingly sophisticated threat environment, a national strategy should recognize the need for continuously monitoring the security of national security, military, and civilian government systems, rather than focusing on "point-in-time" audits and paper-based compliance checks. This is also an important capability for critical infrastructures and enterprises, and should grow into a key component of entities' information security plans. Continuous monitoring of systems involves using automation to collect and analyze data from a variety of sources in order to maintain an accurate description of an organization's security posture to support organizational risk-management decisions.[4] With the appropriate monitoring capabilities in place, adequate amounts of information will be available to determine whether a compromise has occurred. Monitoring services should be divided into four high-level categories:

- Baseline security monitoring for broad detection of malicious or anomalous network activity.
- Specialized security monitoring for critical assets and critical processes.
- Data analysis and reporting to provide telemetry to other key internal security detection and response partners across the enterprise.
- Policy enforcement and measurement of control effectiveness.

Establishing a national approach for continuous monitoring of the highest-priority systems (and appropriate analytics to understand and act on the data) will allow operators and auditors of government systems to be more responsive to changes in the threat landscape and to meet the specific challenges of their respective enterprises with greater speed.

Establish technology-neutral software assurance and supply chain security policies

Ensuring adequate protection of a nation's information technology supply chain is a widely debated topic, given the global and diverse nature of ICT development today. As the national strategy considers the broader implication of the end-to-end needs of the country's ICT infrastructure and its supply chain, it is important that the strategy remain focused on the principle of global relevance and on recommending principles of technology neutrality and supply chain security that are rooted in international standards.

---

[4] The U.S. National Institute of Standards and Technology (NIST) See, e.g., National Institute of Standards and Technology (NIST), "NIST Guide for Applying the Risk Management Framework to Information Systems (NIST Special Publication 800-37)"; ISO/IEC 31010:2009 - Risk management – Risk Assessment Techniques; and ISO/IEC 31000:2009 – Risk Management Techniques, defines continuous monitoring as "a risk management approach to Cybersecurity that maintains a picture of an organization's security posture, provides visibility into assets, leverages use of automated data feeds, monitors effectiveness of security controls, and enables prioritization of remedies." Available at http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf.

1. Software Assurance and International Standards

When governments choose to base their software assurance and supply chain policies on international standards and globally recognized best practices, they create flexibility for vendors and suppliers and increase the range of available potential solutions. International standards such as ISO 27034 for secure software development and emerging international standards for supply chain risk management are useful references for developing such policies. Countries should be cautious in their call for national standards, however, as these can reduce the scale, scope, and character of available solutions. Moreover, national standards that are too stringent or narrowly focused can distort incentives for domestic producers that may result in development of products with limited international appeal.

2. Supporting Supply Chain Security

Exerting influence over supply chain practices can be an effective way for countries to reduce the risk in the development, procurement, and operation of government systems. Governments should include an overarching strategy for managing supply chain risk in the national strategy, as opposed to requiring individual agencies to tackle this complicated issue on their own. The core elements of a national strategy for reducing supply chain risk should include:

- An overall threat model for supply chain risk developed by the government and shared with its ICT vendors and suppliers.
- Policies and controls to ensure that the government is buying genuine products from trusted sources, as well as capabilities that can identify and remove counterfeit or gray-market systems that can create risks to the integrity of government information, services, and assets.
- A lifecycle approach to government systems that extends beyond the procurement phase and addresses the controls needed to ensure that the process for updating systems and retiring systems does not introduce risk into organizations.
- Mechanisms to ensure that suppliers have demonstrable processes for: (1) managing employee identity, including tying identity to role-based access for system development and production; (2) a secure development process, such as the Microsoft Security Development Lifecycle and ISO 27034:1; (3) code integrity practices that prevent or remediate potential risks associated with intentional or unintentional insertion of malware; (4) digitally signing code; and (5) swift recognition of counterfeit products.

Coordinating Threat and Vulnerability Warnings

Threats and vulnerabilities are the currency of security responders and those who would seek to exploit infrastructures or assets. Security responders need information about new threats or vulnerabilities to continue to protect against the evolving threat environment. The strategy should recommend that government and the private sector partner to create a threat-and-vulnerability warning model focused principally on the most significant national-level cyber threats, and include requirements to ensure that information can be actionable.

In essence, coordinating threat and vulnerability warnings should be about sharing information between and among the parties that can act on the data. This should be a collaborative model where the strategy can help create a culture where information is shared, and those who are best positioned to act on it, can.

Recommendations for a National Strategy

Setting expectations for sharing threat information

Sharing threat-based information such as vulnerabilities, hacking trend data, new threat identification, or even unexplained anomalies impacting a product or service can enable the ICT sector and government to better protect critical systems and respond to emerging issues. This can also help lead to new protections or mitigations, sometimes even before any impact. If done widely and efficiently, threat sharing removes the head start afforded to an early discoverer and prevents exploitation of security vulnerabilities, either by outside groups or even participants in the program. However, in order for threat-information sharing to be successful, it must be focused on new and novel threats, and not just known issues that already have remediations available. A threat-information sharing program must also be coordinated by a strong and competent national computer emergency readiness team with authority to share threat information with key stakeholders in the government, private sector, and in some instances the broader public. They also need to be able to involve law enforcement where needed (for example, to help seize a machine controlling a botnet), while simultaneously being respectful of privacy and civil liberties with adequate judicial oversight and enforcement of privacy protections.

Novel and unique threats are the most important information to share

A national strategy should commit the government to provide information on novel threats, including the tools and practices it has observed or the possible indicators of compromise. Sharing this threat information empowers enterprises to identify, manage, and potentially mitigate vulnerabilities that could impact national security, national economic security, or public safety, or any combination thereof. Notifications from the government should be targeted to nationally critical industries and to major hardware, software, and application developers who have the ability to respond, including the ability to develop and disseminate updates to their customers in nationally critical industries. If governments are willing to share this unique information, it will demonstrate to private sector entities that the government is indeed a partner in threat-information sharing, and ensure that responders are focused on essential threats.

Focus on developing a strong national computer emergency readiness team (CERT)

The national strategy must call for a functioning and capable national-level CERT, the primary focus of which should be the protection of government systems in times of need, and secondly the sharing of actionable information about new threats and vulnerabilities with private sector partners. CERTs with strong technical capacity should put their primary focus on remediating and disseminating information on risks that can have national security or public safety consequences. They should analyze incidents from government agency networks and assess potential implications for national impact and share the resulting analysis. In addition to having the ability to find new and novel vulnerabilities, the national CERT should have strong connections to other national CERTs and work collaboratively to address multinational or regional issues.

CERTs must also recognize and address lower-level threats and vulnerabilities that often affect individuals and small and medium-sized businesses (SMBs), or that could be aggregated to have national-level impacts. They should therefore continue to share information related to lower-level threats and vulnerabilities relevant to all actors in order to reduce the likelihood that risks for which remedies exist accumulate to threaten national security or public safety.

Develop and apply relevant international standards

Relevant standards can bolster readiness in government agencies, as well as private enterprises. Encouraging more common approaches to vulnerability management and information sharing should be incorporated into a national strategy. For example, the strategy can encourage those responsible for information sharing and threat and vulnerability assessment to reflect the draft ISO/IEC standards on vulnerability handling within an enterprise (ISO/IEC 30111) and vulnerability disclosure external to an enterprise (ISO/IEC 29147). These standards greatly improve the ability to handle complicated issues related to response. Also, encouraging greater use of Common Vulnerabilities and Exposures (CVE) identifiers, and taking steps to assess the severity and exploitability of a vulnerability can increase capacity and readiness for complex response events.

Emphasizing privacy and civil liberty protections in threat information sharing

There have been many discussions about the appropriate level of information that can and should be shared between private sector entities looking to respond to vulnerabilities or threats, and between those private sector entities and government agencies. It is important that a national strategy emphasize that regardless of whether the threat information is passing between private sector partners or to a government agency, steps should be taken to ensure that the system is designed such that privacy considerations are included at the outset and privacy-by-design principles are leveraged to help ensure that, regardless of the type of data shared, privacy risks are mitigated across the data lifecycle. Ensuring adequate judicial oversight and enforcement of privacy protections becomes increasingly important in connected societies. In addition, threat and vulnerability warning procedures and practices must fit within the existing privacy protections within individual countries, but also recognize that at times warnings and alerts must be sent across borders, so a clear understanding of privacy requirements is essential to a strong threat information sharing capability.

Building Incident Response Capabilities

Incident response capabilities should be established to manage the most critical and significant events that threaten the confidentiality, integrity, or availability of nationally significant information and systems. Effective incident response capabilities can help brunt the disruption or exploitation of information and systems that could threaten national security, economic stability, or public safety. In order for such a paradigm to function, the public and private sectors must clearly articulate and understand what constitutes a national-level incident, and which entities have responsibility for certain actions in responding to such incidents.[5]

In addition, the strategy should review whether law enforcement should have a role in supporting the response to a particular incident. In some circumstances, there may be interest in reviewing whether the perpetrator of an attack can be identified, or law enforcement authorities may have additional capabilities that may enhance the private sector's ability to respond to an incident.

Microsoft's incident response approach has been well publicized, and some of the company's principles are directly applicable to the national context. Microsoft security tools help protect almost a billion computers. The Microsoft Security Response Center (MSRC) receives over 300,000 reports of potential incidents a year, the overwhelming majority of which are known issues for which an update is already available. Having a strong triage process to identify advanced and emerging threats from known and resolved issues is critical. Once an issue is addressed, having a consistent, repeatable response process is essential; it aids the responders, and assists those who are consuming the output of the response, whether updates, guidance, or other mitigation tools.

Recommendations for a National Strategy

Set clear definitions and procedures for incident response

A national strategy must clearly define what constitutes a national-level cyber incident that will require government involvement and the triggering of incident response plans and procedures. National cyber incidents will likely, and reasonably, focus on disruptive, exploitative, or destructive attacks against nationally significant information and information systems in the government and private sector. The strategy should also consider supporting Coordinated Vulnerability Disclosure, a cooperative collaboration between vulnerability reporters and vendors that is designed to help mitigate cybersecurity risks. Organizations may differ on disclosure policies, but one international standard, ISO/IEC 29147, can help prevent conflict and maintain consistency in communication.

[5] For incidents that exploit already known vulnerabilities for which a mitigation is available, the information-sharing capability addressed above should support that need, rather than an incident response function.

Create a clear role for a national CERT

The strategy should recognize a national CERT to lead coordination between the public and private sectors responding to a national incident, or call for the appropriate legislative authority to establish that role. Such a coordinating role will necessitate the close participation of numerous private sector actors, and terms of participation should be developed with their cooperation. It will also require a CERT with the technical and managerial capabilities to effectively assist government and critical private actors during crisis situations, including national and international events.

Enable consistent incident classification

In creating a strategy that includes incident response, it will be necessary for those entities delegated the responsibility of building out this capability to clearly distinguish between national incidents and events that do not rise to that level, and use that to delineate what government can and cannot offer. Because privately owned critical information and systems are likely targets for serious, national-level cyber events, the government must be sure that those owners and operators have a clear understanding of the role of government, including law enforcement, in such a situation. Government's role, whether in providing direct defense or more indirect support, may vary based on the domestic relationship between private critical infrastructure and the government.

Test incident response capabilities and processes

A national strategy should also include exercises to test those processes created to communicate, collaborate, and restore services in the event of an incident. With the importance of private sector actors in cyber incident response, the government should delineate the expectations for private actors in such exercises. While collaboration in test exercises may not be enforced by regulatory mandates, it is important that the strategy set the expectation that there will be cooperation between private sector entities and with the government during a national-level cyber event. National exercises, involving both government and private sector actors, help stakeholders understand their roles during a crisis and better prepare for incident response scenarios.

Public Awareness, Workforce Training, and Education

Technology and policy considerations can often dominate discussions of cybersecurity, overlooking the fundamental human element of the issue. However, significant compromises can occur because of an event as trivial as an employee clicking on a link thought to be trusted, opening a file from a supposedly trustworthy source, or unknowingly inserting into a computer a USB stick that contains malware. The U.S. Department of Homeland Security conducted an experiment during which "infected" USB drives were spread around agency and contractor parking lots.[6] Of the drives that were picked up, over 60 percent were eventually connected to agency or contractor computers, offering an easy vector for an attack to deliver malware. It takes only a single click for a determined adversary to gain access to a network and to begin to compromise the confidentiality, integrity, or availability of ICT resources. As a result, Microsoft believes that it is crucial that a national strategy recognizes that citizens should receive training to practice smart and safe computing.

Developing a knowledgeable, sophisticated cybersecurity workforce is critical to reducing national cyber risk. Every employee in government or business enterprise—from the chief executive to the information technology staff to the rank and file—has cybersecurity responsibilities. Training and education are critical to effective risk management in order to ensure that systems and networks are adequately protected and that risks are accepted at the right level, which is both an educational and an operational priority. Training and education help ensure that the technology staff is using optimal security tools and techniques to protect their networks. Such tools and techniques include event logging, forensic training, and dynamic network protection as a part of an overall cybersecurity risk management program. Training and education help inform individual end users about technical measures and best practices they can utilize to limit the risk of intrusion. Finally, training and education can help senior executives charged with managing financial and operational risks understand the impact of cyber incidents in their environment and manage those risks appropriately. In sum, it should be central to the strategy that training and education be included in the national approach to improving cybersecurity.

[6] http://gcn.com/articles/2011/06/30/dhs-test-found-thumb-drives-disks-network.aspx

Recommendations for a National Strategy

General public awareness and education

The strategy should identify an agency or entity responsible for raising public awareness of cyber risks and the need for cybersecurity, and provide educational resources to help improve the state of cybersecurity. This should include improving the "human" element of cybersecurity—the impact of individual user actions on security and the personal responsibility of individuals to use data and instruments of communication in a purposeful and appropriate manner. This can also lead to an informed public where users are "digitally literate" and are aware of cybersecurity threats and the measures they can take to ensure the safe use of cyberspace, starting in the classroom when students are first introduced to computers. This can be done through public awareness campaigns or developing appropriate academic programs that reflect the defined public awareness goals set forth in the strategy.

Workforce training

While it is important that the strategy encourage improved cybersecurity skills and awareness in digital life in the home, it must also encourage the development of a strong and cyber-literate workforce. The strategy should support technical cybersecurity training in the public and private sectors by promoting the development of academic cybersecurity and risk management programs in order to build domestic technical expertise, harmonize certifications internationally, and create career paths for security experts in government or private sector roles. A national strategy should also consider support for executive training in the public and private sectors by ensuring that leaders have adequate training to understand risk management and cybersecurity, to make informed policy and business decisions, and to grow technical and executive training partnerships with appropriate private sector actors in order to leverage more developed programs existing outside a country's borders.

Driving Research and Technology Investments

Given the potential national security, economic, and public safety impacts of national cyber incidents, it is imperative that countries increase domestic competence in creating and deploying security technologies. National cybersecurity strategies play a crucial role in developing this national competence by highlighting technology research and development needs. It is important that a national strategy set out a research and technology agenda to promote advances in cybersecurity, cryptography, applied mathematics, and related fields.

As the ICT environment continues to expand, a national strategy should also encourage the development and deployment of new technologies by building security into the technology development process.

Recommendations for a National Strategy

Driving technical research and development

As part of the strategy, countries should seek to establish ties with the international research community in the scientific fields related to cybersecurity, such as computer science, electrical engineering, applied mathematics, and cryptography. International ties can help states build on their own capabilities and leverage the expertise in other states that might be lacking domestically.

Public procurement and grant making

A national strategy should influence future government acquisitions and technology grants to ensure that next-generation technologies are developed more securely, thereby reducing their exploitable attack surface. As ICT continues to expand, it is critical that security be at the heart of the development efforts. Government can play an important role in ensuring that complex systems are built more securely from the outset, including security requirements in public procurements or issuing grants to support technology acquisitions by state and local government entities. Once security begins to play a more recurring role in the procurement process, it will likely have the corollary benefit of driving innovation in the marketplace as service providers continue to look for new products and services for their customers.

Structuring International Engagement

While improving domestic defense and response capabilities is largely the focus of national cybersecurity strategies, there are important international elements that impact domestic defensive efforts: cyber-criminal groups operate across national borders; espionage is carried out remotely; and foreign nation-states have the capability to launch destructive attacks against critical infrastructure. With the advantage of the attacker in cyberspace, these risks cannot be properly managed simply through domestic defense.

Countries can help support their domestic mission of protecting against threats through better cooperation between CERTs and through concerted efforts at international diplomacy. A national strategy should therefore reflect the importance of international cooperation to national cyber efforts, including through support for international law enforcement, expanding it to better combat the most advanced and dangerous attacks. The strategy also needs to articulate the need for international cybersecurity norms, and the principles the country plans to promote on this critical matter in the international environment.

Recommendations for a National Strategy

Fostering international CERT cooperation

National-level CERTs should be tasked with building relationships and agreements with one another in order for each to receive timely information on potential threats and vulnerabilities and be able to respond effectively to incidents as a result. CERT cooperation should include determining clear points of contact and agreed-upon methods and channels for information exchange.

CERT agreements can also allow technical expertise to be exchanged between countries, helping build the ability of CERTs to respond to emerging malware trends and threats.

Promoting law enforcement cooperation

Currently law enforcement cooperation on cybercrime issues can be cumbersome, and agencies around the world have disparate forensic capabilities to respond to incidents. The national strategy should identify a law enforcement entity with primary responsibility for cybersecurity issues, and ensure that the entity has adequate training and resources to help partner with victims and with the relevant entities to promote information sharing of new and novel threats. In addition, law enforcement should also be strongly encouraged to participate in efforts to harmonize global law enforcement forensic capabilities and expedite the ability to share information across borders.

Fostering international standards and harmonizing international certifications

International standards can be used in a national strategy to help establish a stronger security baseline or a clearer approach to risk management. The strategy should also require a continued focus on the creation and adoption of international standards. Governments are well suited to contribute technical expertise and political support for the creation of international cybersecurity standards. Microsoft strongly endorses the identification of the most important international standards (or areas where new standards are needed) and supports a global approach, rather than a domestic one, to setting a security baseline. Given the global nature of the creation of ICT, creating products or services to meet hundreds of national standards of varying degrees on the same issue is both unworkable and unnecessary.

Moreover, Microsoft also supports the use of international standards such as ISO 15408 (Common Criteria) to assist in product certification and evaluation, rather than in the creation of domestic approaches. As noted above, harmonization of individual workforce certification and testing schema can also help facilitate the increased development of a future ICT workforce.

Developing cybersecurity norms

The international implications of cybersecurity are immense. How countries behave in cyberspace from a national security perspective is no longer the private matter of an individual state; it is an international issue. Countries need to articulate a clear policy on how they approach national security in cyberspace, and how they will organize to ensure their respective economic security, national defense, and public safety as it relates to cybersecurity. While development of some of these positions should be led by government, many policies and the confidence-building measures that can enable effective cybersecurity norms are highly dependent upon the cooperation of the private sector. The national strategy should set out principles for cybersecurity norms, appoint a clear leader to coordinate and develop those norms, and establish a process for communicating positions in existing international forums. The development of cybersecurity norms is a long-term commitment for the security and stability of cyberspace, and every country should have a voice in this critical dialogue.

Conclusion

A modern nation-state increasingly depends on cyberspace for its economy, public safety, and even defense. Establishing a national strategy for cybersecurity is now and will continue to be an important element of the overall national and economic security strategy for a government. A national strategy cannot solve all of a nation's cybersecurity challenges. 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, incidents will occur. 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. Without a concerted effort to improve cybersecurity through a strong national strategy, followed by the implementation of an active risk-management framework, those attacks will continue to occur, and will only grow in severity over time.

Through a public-private partnership, government, the private sector, and citizens can achieve a national strategy for cybersecurity that is risk-based, outcome-focused, prioritized, practicable, respectful of privacy and civil liberties, and globally relevant. Only then can the digital ground lost to cyber criminals and attackers be reclaimed.

Microsoft stands ready to partner in this challenge.


Microsoft