CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Executive Summary: A Cybersecurity Agenda for the 45th President

This report lays out practical steps for policy, resources and organization that the next Administration can use to build better cybersecurity. The goals for a national approach to better cybersecurity remain the same: to create a secure and stable digital environment that supports continued economic growth while protecting personal freedoms and national security. The requirements for implementation also remain the same: central direction and leadership from the White House to create and implement a comprehensive and coordinated approach to cybersecurity. Much has been done since 2008 and the next Administration should build on and improve on this. The 45th Presidency should:

- Develop a new international strategy based on partnerships with like-minded nations, and improve the ability to deter attackers by developing a full range of response and countermeasures that go beyond the threat of military action.

- Make a serious effort to reduce cybercrime, with consistent Cabinet level support to build international cooperation to fight botnets and sophisticated financial crime. Part of this effort must be to penalize countries that won't cooperate in the effort to reduce and control cybercrime.

- Prepare critical infrastructures and services for attack and improve "cyber hygiene." The new Administration should use incentives when possible, but be ready to regulate if incentives don't work. Greater use of managed services can make government agencies more secure.

- Identify where Federal action in resource issues such as research or workforce development is necessary, since most such efforts are best left to the private sector. We don't need a cyber "Manhattan Project."

- Streamline White House bureaucracy, increase oversight of Federal cybersecurity by creating a special GAO office, and clarify the roles of DOD and other agencies. A stronger DHS is crucial, and the new Administration must either strengthen DHS move the cybersecurity mission.

Two principles should guide the next administration: creating consequences for foreign actors and incentivizing domestic actors. Creating consequences for cybercrime, espionage and cyber-attack is the most effect way to reduce risk (especially if done in partnerships with like-minded nations). Since risk cannot be completely eliminated, better cybersecurity also requires holding key critical infrastructures to high standards while incentivizing improvements in the general population of online actors through jawboning, tax policy, regulation, and investment. These tasks will require some additional resources, but resources are not the major obstacle to better cybersecurity. The major obstacles have been and remain disorganization, confusion over the role of government, and a lack of will.

Recommendations for the Next Administration

Teams in Washington and Silicon Valley generated fourteen working papers and two hundred and twenty specific recommendations. An overview of the recommendations follows below:

I. Policy

The environment for cybersecurity has changed. There has been an erosion of American influence and the arrival of assertive challengers. Russia's use of cyber as an instrument state power is impressive and worrying. Significant incidents – such as North Korea's and Iran's hacks against Sony and the Sands Casino, the Chinese hack of the Office of Personnel Management (OPM) – reflect a growing willingness to use cyber tools against us. A deteriorating situation for international security means that the next administration faces continued cybercrime and espionage, threats to personal information and company data, the possibility of politically coercive cyber acts, and the risk of disruption or attack on critical infrastructure. This means that there is greater risk that requires both international and domestic action in response.

International Strategy

It has been apparent for years that a global approach faces limitations. We are only going to get limited agreement from authoritarian states on cyber norms. Their interests lie in the protection of their sovereignty and in reducing the political and military threat of information technology. This limits the scope for agreement with them to pursing risk reduction. In contrast, the next President has an opportunity to build a robust international structure by seeking agreement with likeminded, democratic states. Part of any reconsideration must look at whether it is time to consider a more formal approach, perhaps including institutions or regimes, to building security and stability in cyberspace

The experience with China shows that opponent behavior can be changed and the risk environment reshaped by U.S. actions. The search for an effective deterrent policy has dogged the last two administrations. Their problem is that they sought to use military. The most effective deterrent actions did not involve the military and were the threat of sanctions or indictments, retaliatory actions that do not involve the use of force. The U.S. would benefit from "populating all the rungs of the deterrence ladder" with the appropriate non-military responses and then communicating them to opponents. Declaratory policy is a crucial part of a deterrent strategy. The current declaratory policy is verbose and confusing and a lack of clarity diminishes its effectiveness in deterring threat. It needs to be rewritten. One caveat here is that even with an improved deterrent policy, including a clearer declaratory policy and a broader range of response options, some opponents will not be deterred. This argues for more work to improve our cyber defenses, but it also raises the larger problem of relations with Russia and China

A More Assertive Response to Cybercrime

Cybercrime has become an epidemic. It is transnational, making international cooperation the only effective response. But some countries don't even pretend to cooperate. The next administration needs to develop ways to penalize them. Existing mechanisms for this cooperation are outdated. The Budapest Convention on Cybercrime is stalemated by opposition from countries that use cybercrime as a political tool and by new powers who object to signing a treaty that they did not negotiate. We need to break the stalemate on the Budapest Convention by offering a new negotiating vehicle that preserves the benefits of the Convention but is more attractive to Brazil, India and others. There will be objections that any reopening will undercut the Convention, but the alternative is continued sluggishness.

Protect Global Data Flows

One way to think about cybersecurity is that we are building the structure for a secure digital economy. Data flows are the "currency" of this economy and the next administration needs cooperative approaches with other nations to ensure the free, secure flow of data. This will require a discussion of rules (and perhaps institutions) for international cybersecurity, privacy, and digital trade. An effort should include agreement with like-minded countries on baseline standards for privacy and civil liberties. Efforts to improve the Mutual Legal Assistance Treaty process are an important part of this.

"Baseline" Cybersecurity, Critical Infrastructure and the NIST Framework

All organizations have an obligation to strengthen cybersecurity, not only to secure their businesses and data of their customers, but also for the sake of our interconnected digital society itself. Progress on cybersecurity requires organizations to improve baseline cybersecurity, the simple measures and best practices that are surprisingly effective in reducing risk. The keys are better corporate governance for cybersecurity, strengthening cyber "hygiene," adopting a faster technology "refresh" cycle, improving authentication of identity (no important data should be protected with only a password), and incentivizing measures for breach disclosure.

The February 2013 Executive Order for critical infrastructure protection adopted a voluntary, sector-specific approach, based on the NIST Cybersecurity Framework, with individual regulatory agencies responsible for their sector. It's not perfect, but the politics of cybersecurity mean it is the best we can get. The next President should promote and when appropriate, compel implementation. One improvement would be to create measurements on adoption and effectiveness. NIST working with the private sector, should be tasked to develop these metrics.

Data protection, privacy and cybersecurity

Protecting the nation's cyber assets includes safeguarding sensitive personal information. Given the vulnerabilities and threats that exist in cyberspace, those who collect and hold data have greater responsibilities for cybersecurity. Additionally, with the increased global focus on data protection, the U.S. needs to clarify the measures it will take to protect it. The next administration should include data protection in its larger approach to cybersecurity, starting with the principle that "data belongs to the user." One improvement would be for the President to request the Federal Trade Commission (FTC) to establish a Division of Data Protection. Another would be passage of national data breach legislation. A single standard would focus corporate data protection efforts on a single, well-understood regime and provide a legislative vehicle for other major reforms.

Increased Transparency for Cyber Incidents

Much of the cybersecurity debate after 2012 was preoccupied with Information sharing. The passage of in 2015 of the Cybersecurity Act of 2015 ended this debate, but there was a sense that more needs to be done in two areas. The first is to break the gridlock over the release of classified information on cyber threats and attacks. Much of this information does not pose a risk to sources and methods if released.

The second is increase liability protection for victims of a cyber-attack if they share details. This was part of the 2015 legislation, but protect need to be expanded. Those who have been hacked are often unwilling to share information. Publicity about being hacked can damage revenue, stock price, and reputation. Effective post incident reporting requires anonymity and liability protection. A new approach could be modeled on the National Transportation Safety Board, which investigates air crashes, or the Federal Aviation Authority's Aviation Safety Reporting System, where there is a blanket prohibition against using submitted information for enforcement purposes. DHS or the Cyber Threat Information Integration Center could manage the new effort.

Preparing for The Internet of Things (IoT)

The growth of the Internet of Things means there will be unavoidable failures of hardware and software, and an unavoidable increase in opportunities for hackers. Increased liability for IoT products is also inevitable. Absent Federal intervention, standards will develop in divergent and potentially disruptive ways. We recommend that the next administration (1) task NIST, with consumer and business groups, to develop standards and principles for IOT security, (2) take a "sector specific" approach, and (3) use Federal procurement standards to drive improvement and safeguard government functions. A publicly available IOT security rating scheme could be modeled on National Highway Traffic Safety Administration crash tests.

Encryption Policy

Greater use of encryption improves cybersecurity across the board, but the kind of encryption and how it is implemented can have serious implications for national security. Any U.S policy and legal framework for encryption must take into account the global environment and the U.S. strategy for international cyber security. U.S. policy should support the use of strong encryption while specifying the conditions under which assistance for lawful access to data can be required. Ultimately, encryption policy requires a decision on risk. Untrammeled use of encryption increases the risk of crime and terrorism, but countries may find this risk acceptable compared to imposing restrictions on encryption use. No one in our groups believed that risk currently justifies new restrictions.

II. Organization

The Obama administration gave DHS the responsibility for cybersecurity. While there has been improvement in the last four years, some experts still believe DHS is inadequate, especially when compared with NSA, and would prefer to see DOD take responsibility for cybersecurity. This idea has little support in the private sector, which prefers a civilian agency. If DHS is to be this agency, it needs to reform its cyber mission. The best solution is to strip extraneous functions from the National Protection and Programs Division, elevate it to an DHS component agency (like Coast Guard or Secret Service). The new agency should avoid intelligence or law enforcement missions and focus on mitigation (helping companies prepare and recover from cyberattack). DHS has been the lead agency for a decade; if these reforms are not implemented or if they do not work, it is time to move the cyber function from DHS.

Early in its tenure, the new administration should issue a clear statement of roles and responsibilities for agencies to minimize internecine struggles. This should define how DOD will support DHS in mitigating incidents, how DHS should support FBI in investigations, and when the "handoff" from DHS to DOD should take place in response to an attack. DOD needs policy and doctrine that define how it can take action in a crisis or emergency, particularly if it involves foreign actors. DOD should not assume regulatory or other peacetime functions. The last administration created a number of White House positions – CTOs, CISOs, etc. These lacked authority and resources and can be eliminated. Similarly, OSTP's role in cybersecurity is unnecessary.

Cybersecurity at federal agencies remains a problem. While the solution is to move to managed services, GAO should be given authority to provide an independent Congressional review, including penetration testing, of federal agency cybersecurity.

III. Resources

Vulnerability Reduction

The U.S. spends billions of dollars on cybersecurity as companies and agencies layer on different technologies to protect networks. This provides a reactive, fragmented approach that attackers can evade. A proactive approach that deserves additional investment and attention "bug bounty" and zero vulnerability programs, where researchers are rewarded for finding vulnerabilities. These programs have a high payoff and the U.S. should support them, emphasizing work to secure Internet infrastructure and widely used open source software. One important step would be to clarify the legality of these programs to provide safe harbor for researchers and support the growing security research industry using a code of conduct for vulnerability research.

Increase the Use of Shared and Cloud Services

Most federal agencies are not in the cybersecurity business. The requirements for adequate cybersecurity distract from the core business. This problem is exacerbated as a result of too few cybersecurity personnel. Better cybersecurity requires rethinking how the U.S. government acquires and manages information technology. It should move to a managed services model, with smaller agencies contracting for email, data storage, and cybersecurity. This move should be part of a larger effort to build cybersecurity into IT acquisitions and programs undertaken by OMB and GSA. Cloud services offer significant security benefits, with lower cost and higher effectiveness than the average enterprise with self-managed IT. Outsourcing basic security functions enables better threat sharing and allows organizations to focus their resources on other critical or uncommon cyber risks that are the most consequential to their organization.

Expanding the Cybersecurity Workforce

Hiring of well-trained cybersecurity candidates is increasingly difficult due to skyrocketing demand. To remedy this, the next administration should implement an ambitious education and workforce plan for cybersecurity, with a system for accrediting training and educational institutions; a taxonomy of cybersecurity roles and the skills that practitioners must demonstrate to claim competence in each specialty; and a robust network of professional credentialing entities.

Moving Ahead

Cybersecurity policy has, with few exceptions, been reactive and fragmented. The response to this is to call for a new strategy, but the experience of national strategies is discouraging. Many are collections of platitudes and in cybersecurity, they can be detailed prescriptions that do not rise to the level of strategy and which often become quickly outdated.

What we have learned in twenty years is that a focus solely on hardening network is inadequate. It must be complemented by understandings and rules for businesses and States on how they will behave in cyberspace. None of the problems we face are insurmountable, but all require continuous, senior level attention and steady effort if we are to make progress.

Cyberspace has become the central global infrastructure. It will only grow in importance. But it is not secure, and the risks we face are unnecessarily great. Our opponents still have the advantage. We can change this if we want, not quickly and not easily, but of necessity if we are to build security for the U.S. and its allies.