cyber GRX

Fixing Cyber Security

Mike McConnell, Patrick Gorman

Today's headlines are depressingly familiar – another massive loss of personal data, ransomware locks out access to vital medical records, social media is exploited by hostile nation states to influence our political system, electrical grids are compromised, another company loses critical intellectual property to a foreign a competitor. Despite spending over $80b a year on cybersecurity, progress in securing our digital business systems, protecting our critical infrastructure, and ensuring consumer data is safe appears to be halting. Of more concern is the unrelenting pace of new digital technologies: the internet-of-things where almost every object we use becomes digitized and made more autonomous through artificial intelligence, further blurring the world between physical and cyber systems. This tightening interconnected web of digital ecosystems is rendering mute the traditional definition of critical and non-critical infrastructure.

Clearly, we are at an inflection point- the digital infrastructure that supports our $20 trillion economy, protects our national security, and empowers our society must be made more secure, more trusted and more reliable. We propose the following items that the government and business leaders should take immediately: 1) rethink the distinction between critical and non-critical infrastructure and our risk models; 2) harden our digital ecosystem using clearly defined standards and market incentives; 3) improve public-private sector collaboration and information sharing through a National Cyber Security Center; 4) create a "Manhattan Project" approach to improving research and development on next generation security technologies that brings together academia, the private sector and government research labs; and 5) create a "Cyber GI Bill" to develop our cybersecurity and information technology human resource pool.

First, rethink the distinction between critical and non-critical infrastructure. The economy runs on data and digital networks and platforms, from hospitals reliant on electronic medical records to serve patients to sophisticated payment networks that power small businesses. These ecosystems include the private business sector, the government and consumers. The proliferation of these digital ecosystems across all facets of our economy and society make it very difficult to differentiate between critical and non-critical systems, limiting the power of the regulators and large companies to understand and secure these ecosystems through traditional mechanisms of industry standards, regulatory oversight, and audits. We need new risk assessment approaches to understand and address threats to a broader digital ecosystem.

Second, we need to make more use of market and legal incentives to drive adoption of best practices and harden our digital ecosystems across all industries.

The key to securing and making more resilient the broader digital ecosystem is the greater use of market incentives, not relying solely on regulation. Currently, most businesses spend enormous resources and energy trying to develop programs that address the requirements of dozens of cyber security frameworks, standards, criteria, and audit regimes, to satisfy both regulatory and industry compliance mandates. This "compliance-based" approach adds to the cost and complexity of security with questionable reduction in risk. A case in point, most of the large data breaches over the last several years occurred at organizations who were "compliant" with government and industry control standards.

The US Federal Government should take the lead and create and promulgate one framework with associated controls standards, measurable performance criteria, assessment and audit approaches, and breach disclosure criteria to replace the myriad of federal and state regulatory and industry models that only add to the cost and complexity of security. Liability protection should be extended to those entities that adopt these standards and best practices. This approach should be accompanied by a clear risk management framework to allows organizations to better tailor security controls and architecture to their actual risk; this would ensure that we have minimum cybersecurity protection standards while encouraging innovation in the application of those standards. The work the National Institute for Standard and Technology (NIST) on frameworks, measurable standards and risk management should cascade to the regulatory agencies to provide a uniform approach and reduce the overhead associated with compliance.   These standards and best practices can then be translated into action by the purchasing power of the private sector, government, and consumers.

Private Sector. The adoption of these standards and risk models can be accomplished by an array of market incentives. First, businesses need to hold their vendors and suppliers to a better standard in terms of protecting sensitive data, and ensure that digital services are safe from disruption, destruction or tampering; they can leverage their tremendous purchasing power to demand a higher level of cybersecurity and resilience in the same manner they currently screen vendors for financial soundness and their ability to deliver goods and services.

Government. The US Federal government spends hundreds of billions on suppliers and vendors as well. This purchasing power should be translated into contract language requiring basic levels of digital security. NIST's creation of a common standard for controlled unclassified information is a good start but needs to fully be implemented into the federal government's acquisition and procurement systems to be effective.

Consumer. Consumers in the United States spend over $600b a year on information technology and telecommunication services. In order to improve consumer awareness of the level of security of digital products and services, the government should create the cyber equivalent of ENERGY STAR- a rating system to inform customers of the level of security when they purchase these services and products; this would compel the companies that offer these to the consumer market to invest in and compete against each other in order to improve the security of digital services and products using market mechanisms. Collectively, these three efforts will raise the bar on security across the private sector and government using more risk-based, market-driven incentives.

Third, while hardening the infrastructure is important, to stay ahead of the threat and remain agile, we must improve information sharing and collaboration. One of the lessons learned from our war on terror is not only need to share information between government agencies and between the private and public sectors, but the need to greater collaboration – people-to-people efforts working jointly to tackle cross cutting cybersecurity issues. We propose the creation of National Cybersecurity Center that would include the various federal government cybercenters, the private sector information sharing and analysis centers (ISACs), and non-profit entities as well. The goal of the center is to co-locate - as much as possible - a diverse group of stakeholders to work collaboratively to better prepare for, prevent, detect, respond and recover to cyber threats.

Fourth, while leveraging a set of minimum risk-based standards to improve security and resilience will lift all boats and advance our current security posture, we still need a concerted private-public effort to improve research and development and implementation of next generation technologies for some of the most sensitive systems that drive our modern economy. This would require the White House Office of Science and Technology to lead of efforts to ramp of our R&D working with the private sector and academia in a "Manhattan Project" approach with particular focus on securing internet-of-things technologies and architectures, addressing challenges like quantum computing and cryptography, and improving security and resilience on autonomous systems (e.g., self-driving cars).

Fifth, we are woefully unprepared in terms of our human capital case in cyber, both in terms of security specialists and engineers. Currently, there are almost a half million unfilled jobs in cyber, resulting in substantial gaps in key industries and bidding wars for talent. We as a country need the equivalent of National Defense Education Act passed after the Soviet launch of Sputnik in 1957 for cyber to produce the tens of thousands of specialists we need each year, ranging from better high school programs, community colleges, vocational schools, and universities. Not only would this produce high paying jobs, but it would ensure the United States maintains its competitive advantage in cyberspace for decades to come.

What we are proposing here is not new; in fact, it is been part of recommendations from dozens of previous studies and task forces over the last 25 years. What has been missing is the leadership and commitment to translate these recommendations into action.

About the Authors

Mike McConnell *is the former Director of the NSA and Director of National Intelligence.*
Patrick Gorman *is chairman of the advisory board of CyberGRX, and previously served in several chief information security officer roles in financial services and government.*