NIST's ROLE IN IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: PUBLIC/PRIVATE TEAMWORK

By William Barker, Cybersecurity Standards and Technology Advisor, Information Technology Laboratory at the National Institute of Standards and Technology (NIST).

National and global economic security depends on the reliable functioning of critical infrastructures. The threat to these infrastructures from threat actors with varying motivations and degrees of capability is severe and is increasing. The roles of public and private institutions in the management and operation of critical infrastructures varies from nation to nation and from sector to sector, but the majority of targets and response capabilities are found in the private sector. However, the ability to foster and coordinate multi-institutional and cross sector responses rests primarily in the public sector. The National Institute of Standards and Technology (NIST) is working in and with national agencies, consensus standards bodies, industry consortia, academia, and individual corporations to accelerate the adoption of emerging technologies and support the effective use of these technologies to protect critical infrastructures.

Recognising that the national and economic security of the United States depends on the reliable functioning of its critical infrastructures, the President of the United States issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The Executive Order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for reducing cyber risks to the critical infrastructure. The framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of the nation's critical infrastructures. The prioritised, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure elements to manage cybersecurity-related risk. NIST also issued a companion Roadmap that discusses NIST's next

steps with the framework and identifies key areas of cybersecurity development, alignment, and collaboration.

NIST is also working directly with both public sector and private sector institutions to develop standards-based security automation platforms and platform implementation guidance to support the rapid adoption of those security controls necessary to reduce cyber risks to critical infrastructures and to economic development. The National Cybersecurity Center of Excellence (NCCoE) was established in 2012 through a partnership among NIST, the State of Maryland and Maryland's Montgomery County to further innovation through the rapid identification, integration and adoption of practical, standards-based cybersecurity solutions, using commercially available technologies. The NCCoE aims to foster the development, acquisition, implementation, and use of comprehensive cybersecurity platforms that support automated and fully trusted government and industry business operations and e-commerce. The ultimate vision for the NCCoE is to advance cybersecurity by enabling a secure cyber infrastructure that inspires technological innovation and fosters economic growth. Its stated mission is to accelerate adoption of secure technologies through collaboration with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs. In order to achieve this mission, the NCCoE

1. provides practical cybersecurity by helping people secure their data and digital infrastructures, equipping them with practical ways to implement cost-effective, repeatable and scalable cybersecurity solutions;
2. increases the rate of adoption by enabling companies to rapidly acquire and implement commercially available cybersecurity technologies; and
3. accelerate effective innovation by empowering innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment.

The improved trust in cyber systems resulting from the NCCoE's efforts supports the development and actual use of innovative automated industry processes that serve to improve operational efficiency, generate significant financial benefits for operators of critical infrastructures and for other public and private sector institutions, promote entrepreneurship, and create new employment and career opportunities.

The NCCoE is working across the private sector and Federal, State, and Local governments to:

- Foster the transfer and broad adoption of existing cybersecurity capabilities and practices from the laboratory to practical, affordable, and useful business use cases and applications across the full range of commercial and government sectors;
- Research and develop new principles and mechanisms underlying security standards, metrics, and technologies;
- Establish a comprehensive library of practical and effective standards, guidelines, metrics, and best practices for secure and privacy-preserving information technologies;
- Develop and test methods for composing, discovering, monitoring, and measuring the mechanisms, configurations, and practices that affect the security posture of systems and enterprises; and
- Communicate cybersecurity principles and technologies to cyber systems developers, providers, and users through effective advertising campaigns, training materials and programs, and formal education.

... THE ULTIMATE VISION FOR THE NCCOE IS TO ADVANCE CYBERSECURITY BY ENABLING A SECURE CYBER INFRASTRUCTURE THAT INSPIRES TECHNOLOGICAL INNOVATION AND FOSTERS ECONOMIC GROWTH ...

The NCCoE is located in a non-Federal facility and represents a true partnership of governments, private corporations and academic institutions. The NCCoE coordinates directly with technologists at Federal and non-Federal institutions and also coordinates closely with National cybersecurity initiatives and with international standards bodies and organisations. Some of these organisations and initiatives include U.S. Federal agencies responsible for implementing Executive Order 13636, the National Strategy for Trusted Identities in Cyberspace (NSTIC), the international ISO/IEC Joint Technical Committee 1's information security initiatives, International Organisation for Standards and International Telecommunications Union Cloud Computing standards initiatives, and the Federal Cybersecurity R&D Strategic Plan. The Federal staff component of the NCCoE is small and relies heavily on private sector participation for the implementation of its programs.

Traditionally, government organisations have attempted to cause improvements in cybersecurity by generating and imposing cybersecurity requirements within the government, and encouraging critical private-sector organisations to implement those same requirements. Budget limitations, difficulty in making security improvements to current information technology and operational technology (ICS/SCADA) infrastructures, and general inertia have limited reducing the cyber threats to government systems, but cybersecurity improvement programs have generally been more effective in government organisations than in the private sector. The encouragement to private sector organisations generally includes sharing information concerning cyber threat technologies, incidents of cybercrime, vulnerabilities, available security technologies, and best practices. Usability and cost issues inhibit private sector adoption of security controls, but another significant inhibiting factor is that the requirements are too often generated by government and security product vendors, and are stated in terms familiar to government security practitioners rather than being generated by private sector users and stated in terms familiar to business' decision makers.

The requirements determination approach employed by the NCCoE is to meet with representatives from specific industrial and economic sectors to identify, from a business perspective, cybersecurity problems specific to individual businesses and sectors. Problems examined include lack of regulatory alignment, competing/conflicting compliance requirements, organisational threats, recognised vulnerabilities, and customer confidence concerns. In a collaborative process, the NCCoE and the business participants derive security and operational requirements from the identified business problems and the relevant systems and business environments. The requirements and problems they are intended to address are stated using terminology employed by the business participants. The NCCoE staff then meets with cybersecurity technology providers in order to identify cybersecurity products and components that can employ automation to address identified business problems and derived requirements.

The NCCoE team analyses the derived requirements and characteristics of component products that may be useful in meeting the requirements of the most current versions of government and industry risk management guidelines and recommendations. Proposed mechanisms for satisfying requirements are typically compositions of a number of products, each of which addresses some aspect of the business security requirement(s). Consistent with the

... CYBERSECURITY IMPROVEMENT PROGRAMS HAVE GENERALLY BEEN MORE EFFECTIVE IN GOVERNMENT ORGANISATIONS THAN IN THE PRIVATE SECTOR ...

... BOTH THE TECHNOLOGY COMPONENTS AND EXPERT ASSISTANCE NEEDED IN COMPOSING AN EFFECTIVE SECURITY PLATFORM FROM THE COMPONENTS ARE PROVIDED WITHOUT FINANCIAL COMPENSATION BY THE GOVERNMENT …

results of the analysis, use case definitions are generated. The use case definition identifies a proposed use case, the business problem(s) addressed by the use case, cybersecurity risks associated with the business problem(s), cybersecurity requirements derived from the business problem and risk assessment, cybersecurity technology potentially available to address the derived requirements, potential sources for the security technologies identified, and any technology gaps that leave any identified requirements unaddressed. Use case descriptions are subjected to public review in order to identify erroneous assumptions, potential additional solutions and sources, and potential additional business applications for proposed solutions.

Once the use case is defined, the technology provider community is invited to participate in the development and demonstration of a proof-of-concept prototype security platform that satisfies the use case requirements. Both the technology components and expert assistance needed in composing an effective security platform from the components are provided without financial compensation by the government. The interested parties must formally agree that, though some details of the components they provide are protected intellectual property, any hardware or software harnesses necessary to making the components work effectively in the composed security platform will be freely available to the public. The team formed for each use case then develops the demonstration security platform and demonstrates the platform to potential users, including those who were involved in the development of the requirements that the platform is intended to address. Finally, the team documents the security platform, including the harnesses and applications programming interfaces, and documents how the platform may be effectively employed to satisfy the use case requirements in applicable environments. The documentation is structured in a manner that permits other technology providers to compose platforms that also satisfy the same or similar use case requirements. Where appropriate, the NCCoE develops and publishes applications guides and best practices for standardised employment of the platforms to satisfy government, critical infrastructure, and other economically significant information and automation security requirements. It is important to note that the platform documentation does not constitute a NIST endorsement of the security platform described or of any technology provider.

A similar process is also employed by the NCCoE to develop building blocks that may be employed in the development of security platforms that have cross-sector applications.

The process described above recognises that the cybersecurity platforms needed to support use cases depend on effectively composed sets of security policies, tools, and practices. For example, in Cloud Computing, there is a notional set of components, including components responsible for identity management and cryptography; however, the underlying standards and metrics needed to create a strong cloud platform that supports identity, authentication, authorization, and access control are not well understood. Composing a cryptographic platform for a cloud with cross enterprise key management, confidentiality for information in transit to and from the cloud, and confidentiality or integrity for information within the cloud is not well understood, even though systems rely on strong cryptographic mechanisms today. The security of the whole is dependent on the security and collective composition of a number of components. In this context, the NCCoE fosters the availability and accelerates the adoption of standards, metrics, test methods, technical solutions, operational practices, service-level agreement components, and training for a range of business use cases employing the Cloud Computing model. Recognising that different use cases are at differing levels of maturity and have different needs, the Center works with all parties to support the composition of security measures in a manner that integrates the pieces to create robust and usable security platforms that protect critical infrastructures and enable the expansion of, and economic and operational effectiveness of, electronic commerce.

Examples of early NCCoE development and demonstration projects include:

- Secure Exchange of Electronic Health Information (a mobile devices use case),
- Securing Assets for the Financial Services Sector (an access rights management use case and IT asset management use case),
- Securing Networked Infrastructure for the Energy Sector (an identity and access management use case and a situational awareness use case),
- Software Asset Management (a building block), and
- Trusted Geolocation in the Cloud (a building block).

The NCCoE supports and complements the broader NIST cybersecurity program. In addition to the NCCoE and NSTIC initiatives, NIST cybersecurity programs include:

1. work in cryptographic mechanisms that address topics such as hash algorithms, symmetric and asymmetric cryptographic techniques, key management, authentication, and random number generation;
2. security research focused on the development and management of foundational building-block security mechanisms and techniques that can be integrated into a wide variety of mission-critical U.S. information systems;
3. security research focused on identifying emerging and high-priority technologies, and on developing security solutions that will have a high impact on the U.S. critical information infrastructure;
4. the development, integration, and promotion of security standards, guidelines, tools, technologies, methodologies, tests, and measurements to address critical cybersecurity needs;
5. validating cryptographic algorithm implementations, cryptographic modules, and Security Content Automation Protocol (SCAP)-compliant products; and
6. developing test suites and test methods. In turn, many of these NIST cybersecurity programs provide standardised technological foundations and applications frameworks to support the NCCoE's role in accelerating the adoption of cybersecurity mechanisms and other controls needed to improve the cybersecurity of critical infrastructures.

The degree of automation and interconnection in the world today invalidates many of the distinctions that have been prevalent in past cybersecurity activities. Government and the private sector interconnect through the internet and various wireless media. Various critical infrastructures are themselves interconnected. Many of the interconnections are designed, while a few are the unforeseen consequences of the pursuit of efficiency (e.g., undocumented system administration and maintenance connections and permission sets). Networks not intended to connect to each other connect to common internetworks. All of this greatly complicates threat environments, access to points of vulnerability, and consequences of malicious exploits and simple system failures. The expertise required to recognise, diagnose, and prioritise threats, vulnerabilities, and countermeasures is distributed broadly but unevenly across public, private, and academic sectors. As stated at the beginning of this article, much of the expertise rests in the private sector, but the ability to coordinate prevention and response measures more often rests in the public sector. Recognising these factors, NIST is adapting its role to leverage private sector expertise and resources to develop security mechanisms that will be recognised in the private sector as relevant and useful to satisfy security problems that are relevant in business terms. The goal is to not just foster the creation of effective cybersecurity technology but to also encourage markets for technical solutions and understanding of how to most effectively employ those solutions. Security mechanisms and controls that are not adopted just aren't very useful, so NIST is working closely with the private sector to accelerate the adoption of useable and affordable mechanisms that address private sector-recognised problems. Ultimately, these private sector-developed products can be adopted to mitigate vulnerabilities in both public and private sector components of our critical infrastructure. ■

ABOUT THE AUTHOR

William Barker is Cybersecurity Standards and Technology Advisor for the Information Technology Laboratory at the National Institute of Standards and Technology. Before joining NIST, Mr. Barker worked in Department of Defense cybersecurity organisations, and subsequently in private sector R&D and business development. He has been involved in cybersecurity since 1966.