Testimony of

Charles H. Romine, Ph.D.

Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Oversight and
Subcommittee on Research and Technology

“Bolstering Government Cybersecurity Lessons Learned from WannaCry”

June 15, 2017

Introduction

Chairman LaHood, Chairwoman Comstock, Ranking Member Beyer, and Ranking Member Lipinski, and members of the Subcommittees, I am Dr. Charles Romine, the Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss NIST's key roles in cybersecurity. Specifically, today I will discuss NIST's activities that help strengthen the Nation's cybersecurity capabilities.

The Role of NIST in Cybersecurity

With programs focused on national priorities from advanced manufacturing and the digital economy to precision metrology, quantum science, biosciences, and more, NIST's overall mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

In the area of cybersecurity, NIST has worked with federal agencies, industry, and academia since 1972, starting with the development of the Data Encryption Standard, when the potential commercial benefit of this technology became clear. NIST's role, to research, develop and deploy information security standards and technology to protect the Federal Government's information systems against threats to the confidentiality, integrity, and availability of information and services, was strengthened through the Computer Security Act of 1987 (Public Law 100-235), broadened through the Federal Information Security Management Act of 2002 (FISMA; 44 U.S.C. § 3541[1]) and reaffirmed in the Federal Information Security Modernization Act of 2014 (Public Law 113-283). In addition, the Cybersecurity Enhancement Act of 2014 (Public Law 113-274) authorizes NIST to facilitate and support the development of voluntary, industry-led cybersecurity standards and best practices for critical infrastructure.

NIST standards and guidelines are developed in an open, transparent, and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are often voluntarily adopted by other organizations, including small and medium-sized businesses, educational institutions, and state, local, and tribal governments, because NIST's standards and guidelines are effective and accepted globally. NIST disseminates its resources through a variety of means that encourage the broad sharing of information security standards, guidelines, and practices, including outreach to stakeholders, participation in government and industry events, and online mechanisms.

[1] FISMA was enacted as Title III of the E-Government Act of 2002 (Public Law 107-347; 116 Stat. 2899).

Recent Malware Attack

Since May 12, a cyberattack impacted more than 230,000 computers in over 150 countries, including the United Kingdom, Russia, and India. Major health systems, telecommunications providers, and railway companies across Europe felt the impact of the attack.

The cause of the attack is reported to be a ransomware called WannaCry. This type of malicious software blocks access to systems and data until a ransom is paid. In this case, the ransomware targets computers running Microsoft Windows operating system by exploiting a vulnerability specific to this system.

WannaCry has spread across local networks and the Internet automatically and has infected systems that have not been secured with recent software updates or are using an older and unsupported operating system. Most of the systems that were infected by the ransomware were running these unsupported operating systems. On March 14, Microsoft had issued a patch to remove the underlying vulnerability for its supported systems. Later, Microsoft also took the unusual step of providing security updates for those unsupported systems, as well.[2]

NIST provides resources to assist organizations in preventing or, at least, quickly recovering from ransomware attacks with trust that the recovered data is accurate, complete, and free of malware and that the recovered system is trustworthy and capable.

To address the issue of cybersecurity in general, and malware in particular, NIST has long worked effectively with industry and federal agencies to help protect the confidentiality, integrity, and availability of information systems. Some of our most significant efforts are addressed below.

Resources to Help Address Malware Incidents

NIST provides standards, best practices, tools, reference implementations, and other resources to help organizations protect assets and detect, respond to, and recover from incidents to minimize the impact of an incident to an organization's mission. The WannaCry incident was new and disruptive, and NIST intends to review the event and its aftermath to ensure that our resources sufficiently address these types of events. Based on our initial review, we believe that many of our past recommendations are applicable to these events, most notably recommendations that can be found in the NIST *Guide for Cybersecurity Event Recovery* and the *Framework for Improving Critical Infrastructure Cybersecurity*, among others.

[2] https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Cybersecurity Event Recovery
Effective planning is a critical component of an organization's preparedness for cyber event recovery. As part of an organization's ongoing information security program, recovery planning enables participants to understand system dependencies; critical roles such as crisis management and incident management; arrangements for alternate communication channels, services, and facilities; and many other elements of business continuity. NIST's *Guide for Cybersecurity Event Recovery* (NIST Special Publication 800-184) provides guidance to help organizations plan and prepare recovery from a cyber-event and integrate the processes and procedures into their enterprise risk management plan.[3] The guide discusses hypothetical cyber-attack scenarios, including a scenario focused on ransomware, and the steps taken to recover from the attack. It provides a detailed description of the pre-conditions required for effective recovery, the activities of the recovery team in the tactical recovery phase, and, after the cyber-attack has been eradicated, the activities performed during the strategic recovery phase.

NIST's *Guide for Cybersecurity Event Recovery* assists organizations in developing an actionable set of steps, or a playbook, the organization can follow to successfully recover from a cyber-event. A playbook can focus on a unique type of cyber-event and can be organization-specific, tailored to fit the dependencies of its people, processes, and technologies. If an active cyber-event is discovered, organizations that do not have in-house expertise to execute a playbook can seek assistance from a trustworthy external party with experience in incident response and recovery, such as the Department of Homeland Security (DHS), an Information Sharing and Analysis Organization (ISAO), or a reputable commercially managed security services provider.

Cybersecurity Framework
Three years ago, NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework) in accordance with Section 7 of Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The Framework, created through collaboration between industry and government, consists of voluntary standards, guidelines, and practices to promote the protection of critical infrastructure. The voluntary, risk-based prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. Although the Framework was originally designed to help protect critical infrastructure, numerous business of all sizes and from many economic sectors use the Framework to manage their cybersecurity risks.

Since the release of the Framework, NIST has strengthened its collaborations with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders to raise awareness about the Framework, encourage use by organizations across and supporting the critical infrastructure, and develop implementation guides and resources.

The Framework is a valuable tool to help organizations understand and manage cybersecurity risk. It focuses on identifying and protecting key systems and assets and

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

on implementing capabilities to detect the occurrence of a cybersecurity event. The Framework also reinforces the importance of capabilities necessary to respond to, and recover from, cybersecurity attacks, including ransomware.

In the case of WannaCry and similar ransomware, the Framework prompts decisions affecting infection by the ransomware, propagation of the ransomware, and recovery from it. For example, the Framework encourages users to understand "data flows"[4] and configure systems minimally to reduce potential vulnerabilities.[5] The Framework identifies network monitoring to "detect potential cybersecurity events,"[6] including the presence of "malicious code,"[7] and to compare them to "expected data flows"[8] in the network to help organizations quickly detect and contain the malicious code and to determine the effectiveness of eradication measures.

WannaCry propagated using a specific operating system vulnerability. The operating system vendor had released a patch nearly two months prior to the first observed instance of WannaCry. The Framework states, "maintenance and repair of organizational assets is performed and logged in a timely manner."[9] Organizations that performed "maintenance and repair" of their operating systems within a two-month window would not have been subject to the spread of WannaCry. Using the Framework, each organization determines its own definition of "timely" to align with its risk tolerance. WannaCry and similar circumstances inform our perspectives on what "timely" means.

An organization's ability to prevent WannaCry from spreading is hinged on identifying systems that are vulnerable and potentially infected and the incident response plans and actions to stop the spread. Recovery is hinged on adequate backups,[10] high-priority system patching,[11] and improvements made to user education and system-patching timelines based on lessons learned.[12]

While the Framework allows an organization to determine its priorities based on its risk tolerance, it also prompts a sequence of interrelated cybersecurity risk management decisions, which should prevent virus infection and propagation and support expeditious response and recovery activities.

On May 11, President Trump signed Executive Order 13800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* that mandated Federal

---

[4] Identify, Asset Management, Subcategory 3 (ID.AM-3)

[5] Protect, Protective Technology, Subcategory 3 (PR.PT-3)

[6] Detect, Security Continuous Monitoring, Subcategory 1 (DE.CM-1)

[7] Detect, Security Continuous Monitoring, Subcategory 4 (DE.CM-4)

[8] Detect, Anomalies and Events, Subcategory 1 (DE.AE-1)

[9] Protect, Maintenance, Subcategory 1 (PR.MA-1)

[10] Protect, Information Protection Processes and Procedures (PR.IP)

[11] Protect, Maintenance (PR.MA)

[12] Recovery, Improvements (RC.IM)

agencies to use the Framework. Under the Executive Order, every Federal agency or department will need to manage their cybersecurity risk by using the Framework and provide a risk management report to the Director of the Office of Management and Budget and to the Secretary of Homeland Security.[13]

On May 12, NIST released a draft interagency report (NISTIR 8170), *The Cybersecurity Framework: Implementation Guidance for Federal Agencies,* which provides guidance on how the Framework can be used in the U.S. Federal government in conjunction with the current and planned suite of NIST security and privacy risk-management standards, guidelines, and practices developed pursuant to the Federal Information Security Management Act, as amended (FISMA).

This report illustrates eight cases in which Federal agencies can leverage the Framework to address common cybersecurity-related responsibilities. By doing so, agencies can integrate the Framework with key NIST cybersecurity risk-management standards and guidelines already in wide use at various organizational levels.

The goal of these efforts is to allow Federal agencies to build more robust and mature agency-wide cybersecurity risk-management programs. NIST will engage with agencies to add content based on their implementation of the Framework, refine current guidance, and identify additional guidance to provide information that is most helpful to government agencies.

National Software Reference Library
Another NIST resource that can assist system administrators in protecting against similar future attacks is the most recent release of the NIST National Software Reference Library (NSRL). The NSRL provides a collection of software from various sources and unique file profiles (computed from this software), which is most often used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the system.

To assist system administrators following the WannaCry attack, the most recent NSRL release includes all Microsoft patches for end-of-life operating system software, such as Windows XP, and the current Windows 10 operating system software, which is a patched version of Windows. NIST is adding a standalone data set to the NSRL, which will include patched versions of supported Windows software that are not Windows 10, such as Windows Server 2016.

National Vulnerability Database
NIST maintains a repository of all known and publicly reported IT vulnerabilities, such as the one exploited by the WannaCry malware. The repository, called the National

[13] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

Vulnerability Database (NVD),[14] is an authoritative source of standardized information on security vulnerabilities that NIST updates dozens of times daily. NIST analyzes and provides a common severity metric to each identified security vulnerability.

The NVD is used by security vendors as well as tools and service providers around the world to help them identify whether they have vulnerabilities. For example, the WannaCry malware exploited a vulnerability that was well documented in the NVD database. This vulnerability's impact score, which assesses the severity of a computer system's security vulnerability, ranges between 8.1 and 9.3 (with 10 being the most severe).

Organizations that use the NVD database to identify and address their computer systems' vulnerabilities can better prepare against malware that exploit these vulnerabilities. The patch issued by Microsoft on March 14 was meant to remove such vulnerabilities and allowed computer systems to be protected from the WannaCry malware attack.

Data Integrity
NIST recently initiated a project at our National Cybersecurity Center of Excellence (NCCoE) on data integrity, specifically focused on recovering from cyberattacks. This project will enable organizations to answer questions like what data was corrupted, when was the data corrupted, how was the data corrupted, and who corrupted the data? Organizations will be able to use the results of NCCoE's research to recover trusted backups, rollback data to a known good state, alert administrators when there is a change to a critical system, and restor services quickly after a WannaCry-like cyberattack.

Conclusion

NIST recognizes that it has an essential role to play in helping industry, consumers, and the government to counter cyber-threats, such as those from destructive malware like WannaCry, and enhance the security of the Nation's cyberinfrastructure and capabilities. The outputs from its cybersecurity portfolio allow users to improve their cybersecurity posture, from small and medium businesses to large private and public organizations, including the Federal Government and companies involved with critical infrastructure.

From the NSRL software collection, which includes all Microsoft patches for end-of-life operating system software, to the *Cybersecurity Framework* and the *Guide for Cybersecurity Event Recovery*, which help organizations manage cybersecurity-related risks and prepare for recovery, to the NVD database, which includes all known and publicly reported IT vulnerabilities, NIST provides tools that help various organizations and the Federal Government prepare for future ransomware attacks. By understanding IT vulnerabilities, protecting computer systems against them, and being prepared to

[14] https://nvd.nist.gov/vuln/detail/CVE-2017-0145#vulnDescriptionTitle [Link to NVD reference to the main vulnerability exploited by WannaCry]

carry out plans that counter cyberattacks, we can all significantly reduce harms that can result from such attacks.

NIST is extremely proud of its role in establishing and improving the comprehensive set of cybersecurity technical solutions, standards, and guidelines to address cyber-threats, in general, and ransomware, in particular. Thank you for the opportunity to testify today on NIST's work in cybersecurity and in preventing ransomware attacks. I would be happy to answer any questions you may have.