PROJECT DESCRIPTION

IMPROVING CYBERSECURITY OF MANAGED SERVICE PROVIDERS

(Supporting Small-and Medium-Size Businesses)

Karen Waltermire
NIST National Cybersecurity Center of Excellence

Harry Perper
The MITRE Corporation

DRAFT

October 2019

smb_nccoe@nist.gov

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

This document describes how managed service providers (MSPs) can improve the cybersecurity of their information technology (IT) infrastructure. NCCoE cybersecurity experts will address this challenge through collaboration with a Community of Interest, including vendors of cybersecurity solutions. The resulting reference design will detail an approach that can be incorporated across multiple sectors.

Abstract

MSPs have become an attractive target for cyber criminals. As a result, an MSP could benefit from improving its own cybersecurity through implementing a secure IT architecture that reduces vulnerabilities to attacks such as ransomware. When an MSP is vulnerable to a cyber attack, it also increases the vulnerability to the small-and medium-size businesses (SMBs) that it supports. SMBs rely on MSPs as trusted partners for their cybersecurity needs and to help them address challenges in implementing cybersecurity technologies, including cost and staff expertise. Unfortunately, many MSPs face challenges similar to those of SMBs, including a cybersecurity talent shortage and a lack of cybersecurity technology integration experience. To address these challenges, this project will provide MSPs with informed guidance that will enable them to adopt cybersecurity technologies and techniques that result in better security for themselves and their SMB customers. The goal of this project is to provide a cybersecurity reference model that MSPs can customize to fit their cybersecurity program needs.

Publication of this project description begins a process that will further identify project requirements, scope, and hardware and software components for use in a laboratory environment. In the laboratory, the NCCoE will build a standards-based, modular, and end-to-end example solution(s) that will address a set of cybersecurity challenges aligned to the NIST Cybersecurity Framework v1.1, listed in Table 2 in the Scope section. The approach may include architectural model definition, logical design, build development, test and evaluation, and security control mapping.

This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Keywords

cybersecurity; managed service provider; MSP; risk management; SMB; small business

Disclaimer

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

Comments on NCCoE Documents

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://www.nccoe.nist.gov.

45 Comments on this publication may be submitted to smb_nccoe@nist.gov.

46 Public comment period: October 8, 2019 to November 8, 2019

Table of Contents

List of Figures

List of Tables

1 Executive Summary

Purpose

The National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) is interested in helping managed service providers (MSPs) support the cybersecurity needs of small-and medium-size businesses (SMBs). MSPs provide information technology (IT) and cybersecurity products and services to the majority of SMBs in the nation. Therefore, providing cybersecurity guidance to MSPs to improve their own cybersecurity will result in improved cybersecurity for their customers, SMBs. The goal of the project is to provide MSPs with guidance for implementing cybersecurity techniques that will help them secure their IT architecture. This guidance should allow MSPs to adapt techniques to best fit their environment and needs by using current technologies, off-the-shelf technologies, or open-source technologies. To ensure that the project best addresses MSPs' cybersecurity needs, the NCCoE is requesting feedback on this project idea.

The NCCoE intends for the project to provide MSPs who adopt the guidance with the following potential benefits:

- improved cybersecurity awareness
- improved hardware and software asset management
- improved system and data access control
- improved cybersecurity of an MSP's IT infrastructure
- improved design, acquisition, and integration of secure technologies

Each MSP's design must be based on its cybersecurity needs evaluation.

This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement a cybersecurity reference design that addresses this challenge.

Scope

The scope of this project includes the Cybersecurity Framework Subcategories noted in Table 2. The Subcategories were chosen based on discussion with cybersecurity experts and MSP representatives. The project will address the Cybersecurity Framework Functions (i.e., Identify, Protect, and Detect) and the Subcategories of those Functions identified as the most pertinent to securing an MSP IT infrastructure based on those discussions. Future projects may cover other Functions (i.e., Respond, Recover) and Subcategories that are not included here.

Guidance will include a reference architecture model and example implementation (proof of concept) details to enable an MSP's decision makers or technologists to understand and implement any part or all of the proposed approach to improve the cybersecurity of its IT infrastructure.

Assumptions

The following assumptions and dependencies will help shape the scope of the project:

- MSPs recognized that improving their own cybersecurity program is important to their success and the success of the SMBs they support.
- MSPs consider themselves trusted partners of their customers.
- Applicable secure technologies are available.
- The Cybersecurity Framework Subcategories listed in Table 2 are applicable to a broad segment of MSPs.
- MSPs understand that the proposed architecture model is modular and that the example solution(s) will enable MSPs to adopt applicable portions of the proposed approach that best fit their needs.
- MSP organizations will perform a risk assessment to determine the value of an investment in one or more of the secure technologies included in the architecture.

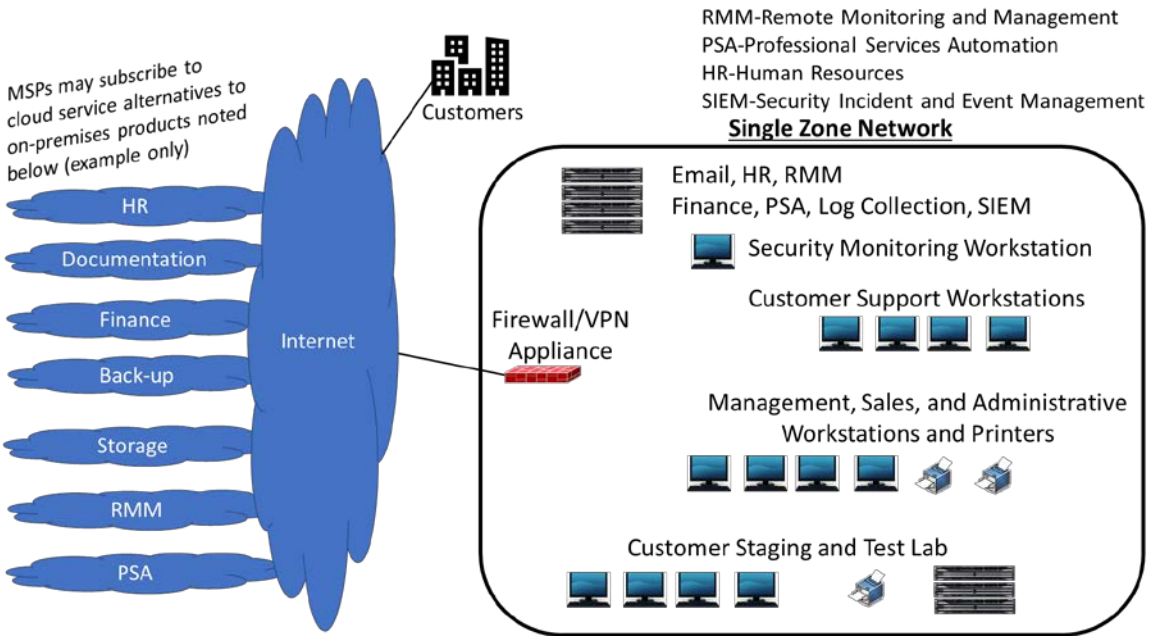
Background

The MSP market has seen tremendous growth over the past six years. This success has resulted in MSPs increasingly becoming targets of cybersecurity attacks that can impact their business and their customers' overall trust in MSPs and jeopardize their customers' security. For example, a recent attack on MSPs, commonly referred to as Cloud Hopper, may have exposed the information that MSPs held describing their customers' IT infrastructures and account information.

The research conducted for this project indicates that a typical MSP focuses primarily on ensuring that it can provide the best options for remotely managing SMBs' IT and end-user systems and that cybersecurity of their own IT infrastructure may be a secondary concern. The research was informed by discussions with subject matter experts (SMEs) in the MSP market and included interviews, correspondence with MSPs, summaries from MSP-focused conferences, and vendors for back-office and customer technical support such as remote monitoring and management, professional service automation, and automated backup tools. The research led the NCCoE SMEs to identify the list of Cybersecurity Framework Subcategories listed in the Scope section of this document.

For example, after discussions with SMEs within the MSP market, the NCCoE's technical experts concluded that many MSP IT infrastructures are implemented on nonsegmented networks. These networks are generally undesirable because they enable equal network access to all assets on the network. If the network were compromised, nonsegmented networking enables the spread of malware by creating a corporate-wide horizontal network. Nonsegmented networking also allows user access to all corporate assets by default, which greatly increases the potential for unwanted user activity. Figure 1 depicts an example of a nonsegmented network to illustrate this research finding.

139 **Figure 1: Example MSP Nonsegmented Network**



140 ## 2 SCENARIOS

141 The NCCoE, in collaboration with MSP organizations, identified three scenarios that capture a broad
142 range of the most pressing cybersecurity challenges facing MSPs. To demonstrate how cybersecurity
143 challenges can be addressed within these scenarios, the NCCoE will create a realistic MSP IT
144 environment, including common MSP applications. Within that environment, multiple standards-based
145 cybersecurity techniques and technologies will be implemented. The technologies used will address
146 each scenario's cybersecurity challenges.

147 ### Scenario 1: Managing the assets of the MSP

148 **Asset Management:** This scenario will address the challenge of asset management. The project will
149 provide a reference architecture and example solution for improving asset management, including
150 hardware, software, vulnerability management, and system patching within the MSP environment.

151 ### Scenario 2: Managing employee access to data and systems

152 **Access Management:** This scenario will address the challenges with access management. The project
153 will provide a reference architecture and example solution for improving access management to MSP
154 data, MSP customer data, and MSP applications/tools, including multifactor authentication, role-based
155 access control, password management, remote access, and privileged account management.

156 ### Scenario 3: Event data is logged, and anomalous events are detected.

157 **Tracking Events Data and Incidents:** This scenario will address the challenges associated with various
158 aspects of event logging and correlation within the MSP environment. The project will provide a
159 reference architecture and example solution for improving event logging and correlation, including user
160 activity and network activity.

3 High-Level Architecture Model

The proposed high-level architecture model for an MSP includes components that address 10 of the 108 Cybersecurity Framework Subcategories as listed in Table 2. Figure 2 depicts a proposed network segmentation architecture model, separating the various corporate assets into sub-networks with common uses or access-control requirements. Figure 2 also aligns to Subcategory PR.AC-5 that recommends network segmentation. Table 1 addresses the remaining Subcategories listed in Table 2.

Figure 2: High-Level Architecture for MSP IT Infrastructure

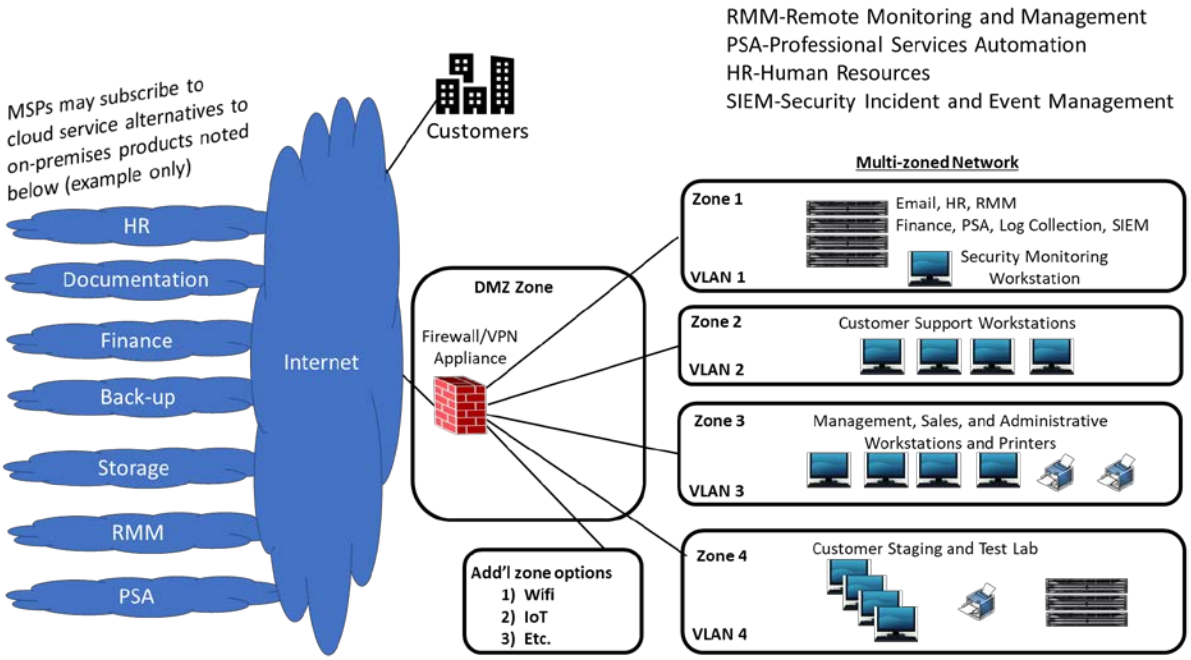


Table 1: Additional High-Level Architecture Security Components

Identify	Protect	Detect
Asset scanning and detection	Directories (Active Directory)	Event logging and collection
Automated update management	Role-based access control	Event log analysis
Update testing	Physical access control	Analysis to detect unauthorized (out of policy) users, user activity, devices, and software
User resource access policies	Multifactor authentication	Network monitoring
User role policies	VPN	
	Disk encryption	
	Backup systems (auto and manual)	

The proposed high-level architecture model components are expected to be included in the project and documented in the practice guide. These components will combine to raise an MSP's cybersecurity posture and address the Cybersecurity Framework Subcategories listed in Table 2.

Component List

The following components will be needed to create a realistic MSP IT environment and demonstrate capabilities to address the cybersecurity challenges presented in the three scenarios described in Section 2:

- mobile and desktop devices
- cloud application and directory services
- mobile-device manager (cloud service)
- on-premise applications
- on-premise IT infrastructure
- security incident and event management (SIEM)
- identity and access management capabilities
    - identity store
    - access rights management (role-based)
    - authentication and authorization
- network segmentation capabilities
- encryption capabilities–disk level
- network monitoring capabilities
- asset management capabilities
    - vulnerability scanning
    - automated update
    - asset identification
- RMM capabilities
- PSA capabilities

Security Characteristics

This project will develop a reference architecture and example implementation that meets the following requirements:

- is standards-based
- is effective and secure
- addresses the subset of Cybersecurity Framework Subcategories in Table 2
- supports modular implementation such as:
    - multivendor implementations
    - independently implementable security capabilities

4 Relevant Standards and Guidance

Standards, guidance, and open-source activities that may be leveraged for this effort include:

- NIST *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1 [1]
- NIST Interagency or Internal Report (NISTIR) 7621, Revision 1, *Small Business Information Security: The Fundamentals* [2]
- NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [3]

- NIST SP 800-63-3, *Digital Identity Guidelines* [4]
- NIST SP 800-171 Rev. 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [5]
- NIST SP 1800-18, *Privileged Account Management for the Financial Services Sector* [6]
- NIST Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules* [7]
- NIST SP 1800-9, *Access Rights Management for the Financial Services Sector* [8]

5 Security Control Map

Table 2 maps the characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity. This exercise is meant to demonstrate the real-world applicability of standards and best practices but does not imply that products with these characteristics will meet an industry's requirements for regulatory approval or accreditation.

Table 2: Security Control Map

Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.
PROTECT (PR)	**Identity Management, Authentication, and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.
		PR.AC-2: Physical access to assets is managed and protected.
		PR.AC-3: Remote access is managed.
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-5: Network integrity is protected (e.g., network

		segregation, network segmentation).
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-4:** Backups of information are conducted, maintained, and tested.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected, and the potential impact of events is understood.	**DE.AE-3:** Event data are collected and correlated from multiple sources and sensors.

Appendix A References

[1] *Framework for Improving Critical Infrastructure Cybersecurity,* V1.1, National Institute of Standards and Technology (NIST), Gaithersburg, Md., Apr. 2018. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[2] C. Paulsen and P. Toth, *Small Business Information Security: The Fundamentals,* NIST Interagency Report 7621, Revision 1, Gaithersburg, Md., Nov. 2016. Available: https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final.

[3] *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication (SP) 800-53 Revision 4, Gaithersburg, Md., Jan. 2015. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

[4] P. Grassi et al., *Digital Identity Guidelines*, NIST SP 800-63-3, Gaithersburg, Md., June 2017. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[5] R. Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST SP 800-171 Rev. 1, Gaithersburg, Md., December 2016 Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf.

[6] K. Waltermire et al., *Privileged Account Management for the Financial Services Sector,* NIST SP 1800-18, Gaithersburg, Md., Sept. 2018. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-pam-nist-sp1800-18-draft.pdf.

[7] U.S. Department of Commerce. *Security Requirements for Cryptographic Modules,* Federal Information Processing Standards Publication 140-3, March 2019. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf.

[8] J. Banoczi et al., *Access Rights Management for the Financial Services Sector,* NIST SP 1800-9, Gaithersburg, Md., Aug. 2017. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-arm-nist-sp1800-9-draft.pdf.

[9] Gartner IT Glossary. Managed Service Provider (MSP). 2019. Available: https://www.gartner.com/it-glossary/msp-management-service-provider

APPENDIX B ACRONYMS AND ABBREVIATIONS

FIPS	Federal Information Processing Standard
IT	Information Technology
MSP	Managed Service Provider
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency or Internal Report
SMB	Small and Medium Business (or Organization)
PSA	Professional Services Automation
RMM	Resource Monitoring and Management
SIEM	Security Incident and Event Management
SME	Subject Matter Expert
SP	Special Publication

Multifactor Authentication	An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.
Managed Service Provider	A managed service provider (MSP) delivers services, such as network, application, infrastructure and security, via ongoing and regular support and active administration on customers' premises, in their MSP's data center (hosting), or in a third-party data center. The term MSP traditionally was applied to infrastructure or device-centric types of services but has expanded to include any continuous, regular management, maintenance and support. [9]