LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing 2019 Threats Posed to Healthcare Sector by Use of Third-Party Services

OVERALL CLASSIFICATION IS

TLP:WHITE

4/2/2020

Report #: 202004021030

Agenda

- Overview
- MSPs and MSSPs
- “Business Associates”
- Mitigation: NIST Cyber Security Framework
- Mitigation: Health Industry Cybersecurity Practices
- Mitigation: Communicate Requirements
- Assessment
- HHS 405(d) Mitigation Practices: Third-Party Risks
- References
- Questions

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

Players

- Managed Service Providers (MSP) and Managed Security Service Providers (MSSP)
- Third-party companies, also called “business associates” (BA)
- Third-parties provide various services to include IT, consulting, and administration services for healthcare facilities

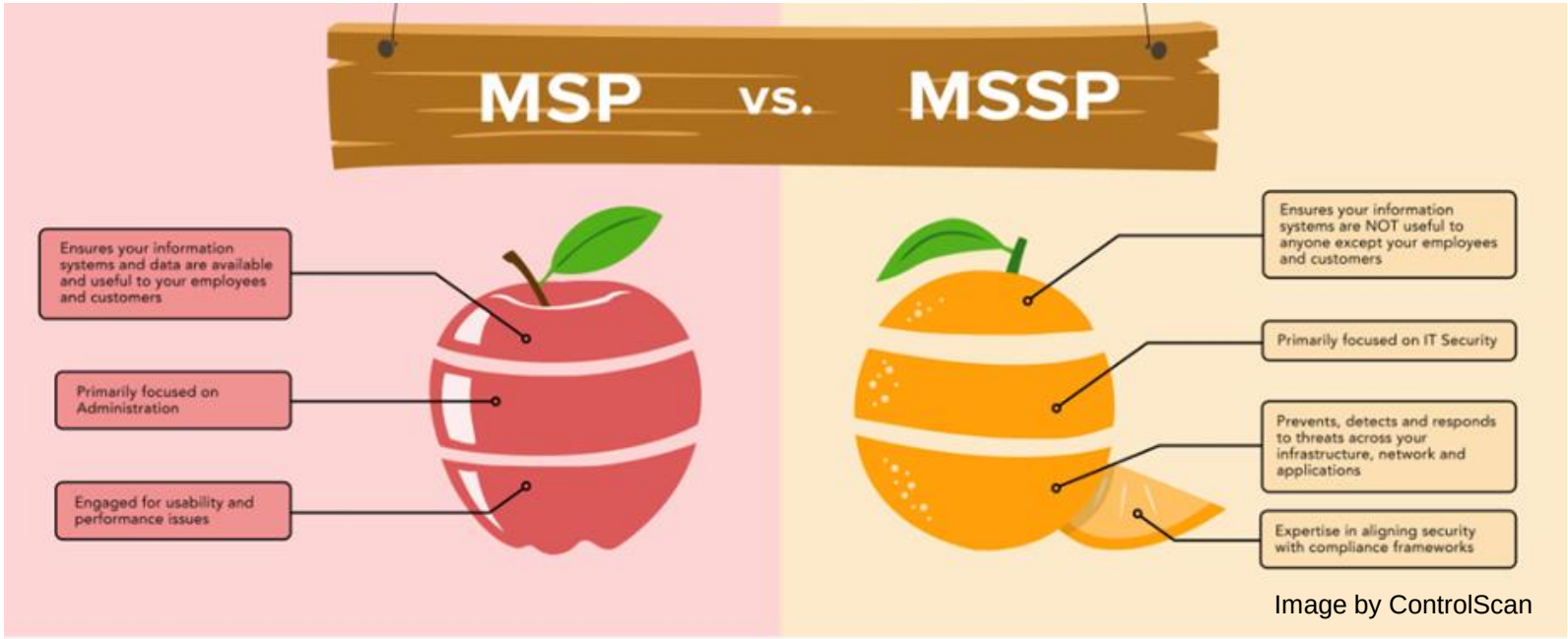
Mitigations

- **A comprehensive evaluation of the organizations that a healthcare entity intends to do business with.**
- Policies adopted by a healthcare entity may be desirable for those that they intend to do business with to adopt as well.

Assessment – High Risk

- The more third-parties in an environment the more uncontrolled entry points to your network you may have
- Reputational harm to the healthcare entity could occur because of their association with a compromised third-party victim.

MSPs and MSSPs

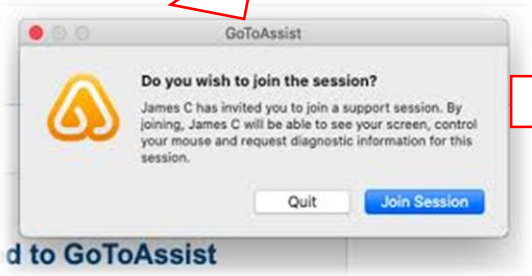


Managed Service Providers (MSP) and Managed Security Service Providers (MSSP) are “high-value targets” for threat actors

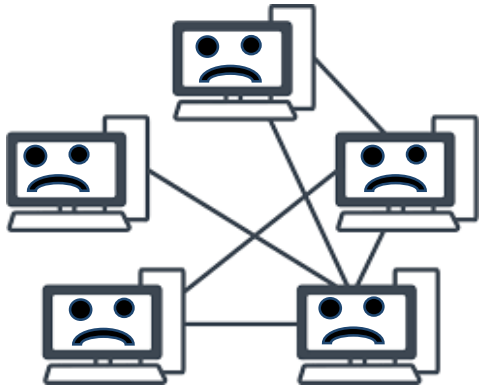
- MSPs and MSSPs as entry points to their true intended target—the MSP and MSSPs’ customers (you)
- Once access to the target is gained the attackers will disable security tools on the victim’s network and expand their presence within the network.

MSPs and MSSPs (cont.)

Attacker



Customer Network



RDP

Symantec
A Division of Broadcom

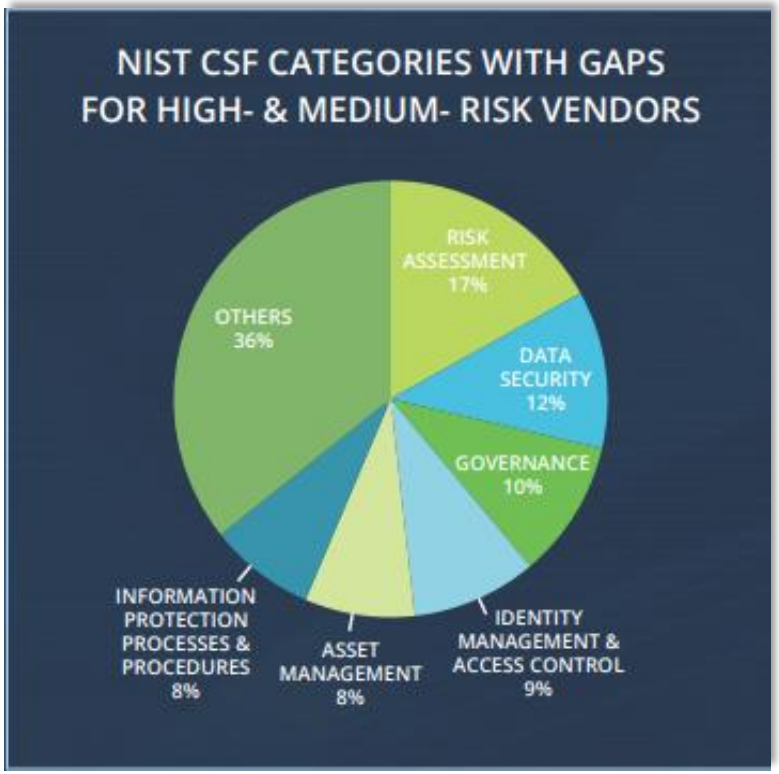
Business Associates

Third-party companies—also called “business associates” (BA) that support operations such as billing, outstanding bill collections, and healthcare records management.

- In 2019 BAs accounted for more than 20% of healthcare breaches.
- The two largest healthcare data breaches of 2019 impacting over 37,500,000 victims were caused by BAs.
- Healthcare records breaches are another high-profile risk area that has more than doubled since 2017 with, 27.5 million records exposed in 2019 costing the healthcare industry an average of $429 per record.

The threats faced by healthcare industry are the same threats that MSPs, MSSPs and BAs face as well. In 2019 those threats were:

- Phishing
- Insider Threats
- Ransomware



Graph by Cynergistek

Mitigation: NIST Cyber Security Framework

A comprehensive evaluation of the organizations that a healthcare entity intends to do business with.

The National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) provides strategies to conduct vendor selection and management. NIST recommends an evaluation of potential vendors against the following criteria:

Risks Associated with the Suppliers

- Evaluation process that focuses on product delivery and condition
- Financial, location, operational, business continuity, and time to recovery

Cyber Supply Chain Risks

- Evaluation process that focuses on security
- Vetting of personnel, their service providers, products and software

kaspersky

HUAWEI

Adversary Country?

Who do they do business with?
Where is their infrastructure?

Where is production?

Mitigation: NIST Cyber Security Framework

A comprehensive evaluation of the organizations that a healthcare entity intends to do business with.

“Supplier Security Requirements” could be implemented into agreements and contract language:

- Security Governance
- Manufacturing/Operational Security
- Software Engineering and Architecture
- Asset Management
- Incident Management
- Transportation Security
- Physical and Environmental Security
- Personnel Security
- Information Protection
- Sub-tier partner security (lower tiers, service providers, cloud)

Mitigation: Health Industry Cybersecurity Practices

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) Technical Volumes 1 and 2 outline cybersecurity policies that organizations—based on their size—may want to implement to improve their cybersecurity posture.

These types of policies if adopted by the healthcare entity may be desirable for those that they intend to do business with to adopt as well. The policies in HICP are linked to the NIST CSF to further the integration of an overall cybersecurity framework at a healthcare organization.

Small, Medium, & Large

- Roles and Responsibilities
- Education and Awareness
- Acceptable Use / Email Use
- Data Classification
- Personal Devices
- Laptop, Portable Device, and Remote Use
- Incident Reporting and Checklist

Medium & Large

- Disaster Recovery Plan
- IT Controls Policies
- IT Acquisition Policy

Mitigation: Communicate Requirements

A comprehensive evaluation of the organizations that a healthcare entity intends to do business with.

NIST “common language” to communicate requirements:

Framework - enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices as well as reflecting risk management priorities.

- Current Profile - indicates the cybersecurity outcomes that are currently being achieved.
- Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals.

Implementation Tiers - provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.

Flowchart from NIST CSF

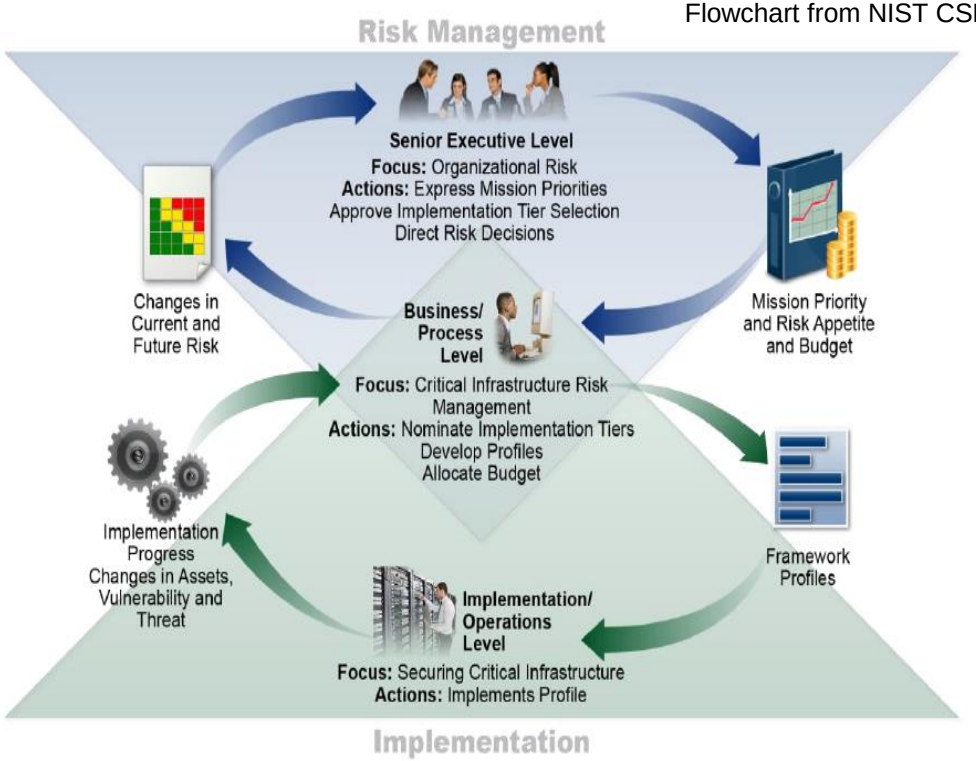
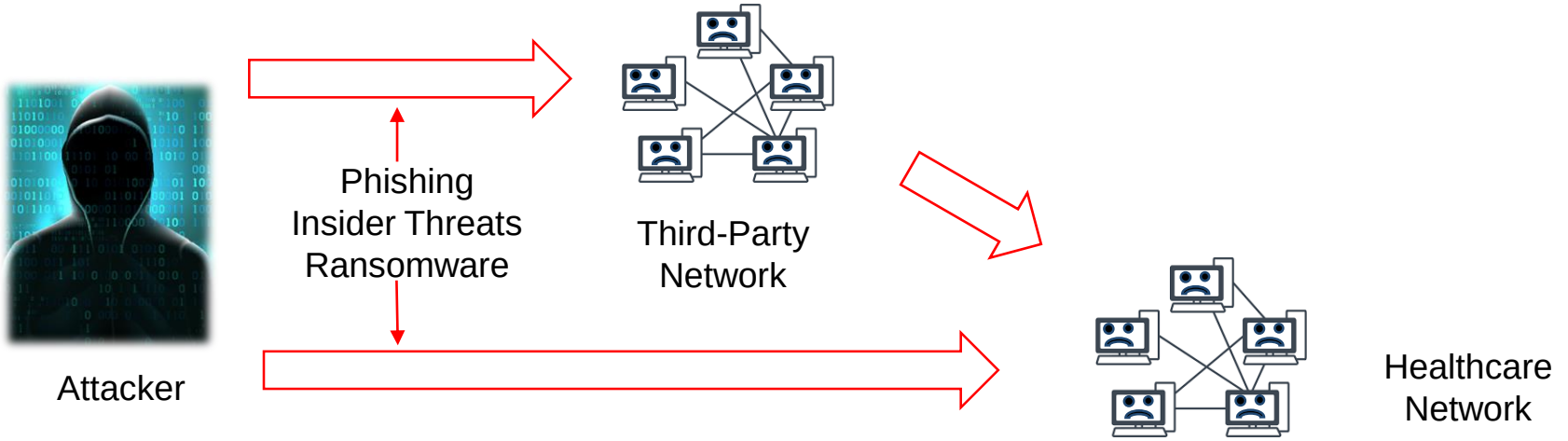


Figure 2: Notional Information and Decision Flows within an Organization

Assessment

Assessment – High Risk

- Threat actors potentially have two avenues of attack against the healthcare sector, the healthcare entity and the third-parties that the healthcare entity uses to support their operations
- These avenues of attack potentially impact the healthcare entities directly or indirectly
- Even if, a healthcare entity is not targeted directly but a MSP, MSSP, or BA that they do business with is, the health care entity could have reputational harm through association with that third-party victim
- Healthcare entities are increasing their exposure to phishing, insider threats, and ransomware with the integration and use of MSPs, MSSPs, and BAs



HHS 405(d) Mitigation Practices: Third-Party Risks

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate ….

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Encrypt sensitive data, especially when transmitting data to other devices or organizations	(4.S.B, 4.M.C)
Acquire and use data loss prevention tools	(9.M.A)
Implement a safeguards policy for mobile devices supplemented with ongoing user awareness training on securing these devices	[9.M.B]
Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device	(4.M.C)
Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors	(1.S.B, 1.M.D)
Implement and use privileged access management tools to report access to critical technology infrastructure and systems	(3.M.C)

For more information on the risks posed by third-party business associates reference HC3 white paper “Cyber Third-Party Service Threat Mitigation” from February 25, 2019.

For more information on the risks posed by MSP and MSSPs reference HC3 Intelligence Brief “Risks of Outsourcing” from March 1, 2018.

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

References

- BlackBerry | Cylance 2020 Threat Report Highlights
  - https://www.cylance.com/en-us/resources/knowledge-center/2020-threat-report.html
- MSP versus MSSP: Like Apples & Oranges
  - https://www.controlscan.com/msp-versus-mssp-infographic/
- Top 15 Best Managed Security Service Providers (MSSPs) In 2020
  - https://www.softwaretestinghelp.com/managed-security-service-providers/
- Sodinokibi Ransomware Still Very Relevant for MSSPS
  - https://www.msspalert.com/cybersecurity-guests/sodinokibi-ransomware-still-very-relevant-for-mssps/
- GoToAssist is now RescueAssist with 2x faster Remote Support.
  - http://sur.ly/o/go2assist.com/AA000014
- Identity Theft Attacks to MSPs in 2019…
  - https://www.msspalert.com/cybersecurity-guests/identity-theft-attacks-to-msps-in-2019-why-mfa-is-critical-in-protecting-managed-service-providers/
- 2019 Healthcare Data Breach Report
  - https://www.hipaajournal.com/2019-healthcare-data-breach-report/

References (cont.)

- The 20 Most Popular EMR Software Solutions
  - https://www.capterra.com/infographics/top-emr-software
- Measuring Progress: Expanding the Horizon | 2019 Annual Report
  - https://insights.cynergistek.com/reports/2019-healthcare-cybersecurity-privacy-report
- Number of records exposed in healthcare breaches doubled from 2018 to 2019
  - https://www.helpnetsecurity.com/2020/02/20/records-exposed-healthcare-breaches/
- Cyber Threats Behind the Biggest Healthcare Data Breaches of 2019
  - https://healthitsecurity.com/news/cyber-threats-behind-the-biggest-healthcare-data-breaches-of-2019
- Best Practices in Cyber Supply Chain Risk Management
  - https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-SCRM-Vendor-Selection-and-Management.pdf
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  - https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

Questions

Upcoming Briefs

- Access Control on Health Information Systems
- State of the HPH: Cybersecurity Edition

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**