NEW YORK STATE | Homeland Security and Emergency Services

Five Steps to Jump Start Your Cybersecurity Program

Tug Hill Commission Virtual Conference

April 28, 2021

Agenda

- ➢ **Introductions**
- ▪ Real Risks
- ▪ Five Steps
- ▪ Helpful Resources
- ▪ Questions?

Team Composition and Mission Objectives

Multi-Unit Collaborative Approach

- OCT Cyber Incident Response Team
- OCT Critical Infrastructure Unit
- Partnership with New York Division of Military and Naval Affairs

Identify / Prevent / Protect

- Training and exercises
- Proactive outreach and assessments

Respond / Recover

- Incident response and digital forensics
- Remediation assistance and guidance

Agenda

- ✓ Introductions
- ➢ **Real Risks**
- ▪ Five Steps
- ▪ Helpful Resources
- ▪ Questions?

NEW YORK STATE | Homeland Security and Emergency Services

Real Risks - Education

- Threat Actors: students, information brokers
- Objectives: disrupt schedules, sell “personally identifiable information” (PII) on the dark web
- Tactics: “denial of service”, ransomware, phishing
- Factors to Consider:
  - Insider threat
  - Availability of attack “services”
  - Value of student PII

Real Risks – Local Government

- Threat Actors: nation states, “hacktivists”
- Objectives: disrupt elections, disrupt critical infrastructure
- Tactics: disinformation, ransomware, system penetration
- Factors to Consider:
  - Counties’ role in voter registration and polling
  - Heightened public and media focus on elections
  - Municipal control over water systems and other CI

Real Risks – Healthcare

- Threat Actors: nation states, anarchists
- Objectives: promote nationalism, “watch the world burn”
- Tactics: disinformation, ransomware, system penetration
- Factors to Consider:
  - Prominence of health care facilities in pandemic response
  - Automated detection of vulnerable systems
  - Risk associated with older medical devices

Agenda

- ✓ Introductions
- ✓ Real Risks
- ➢ **Five Steps**
- ▪ Helpful Resources
- ▪ Questions?

Step 1: Introduce Cyber to Leadership

- Who is your “cyber sponsor” on the leadership team?
- How can you relate business risks to cyber risks?
- What are your organizations “crown jewels”?
- When and how should leadership be engaged?
- Replace “FUD” with facts whenever you can.
- Establish a realistic charter for your cyber-efforts.

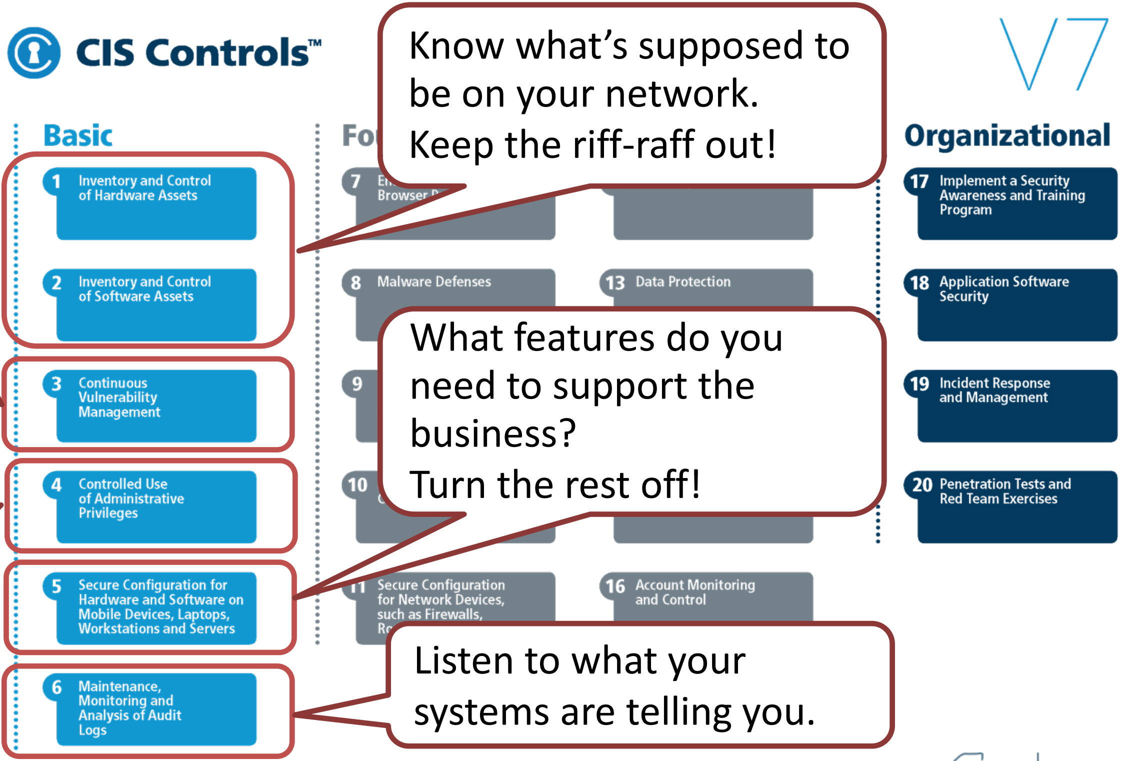
Step 2: Start With the Basics

- There's a lot you *could* do. What should you do first?
- The right framework can help make sense of your options.
- The CIS Top 20 Critical Security Controls are one option.
- Temper the recommendations of the controls with your organization's own experiences and those of your peers.
  - Past incidents
  - Regulatory requirements

A framework to guide you

Keep your systems up-to-date.

Be careful with your “super users”



CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Fo

7 En Browser P

8 Malware Defenses

9

10

11 Secure Configuration for Network Devices, such as Firewalls, Ro

13 Data Protection

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

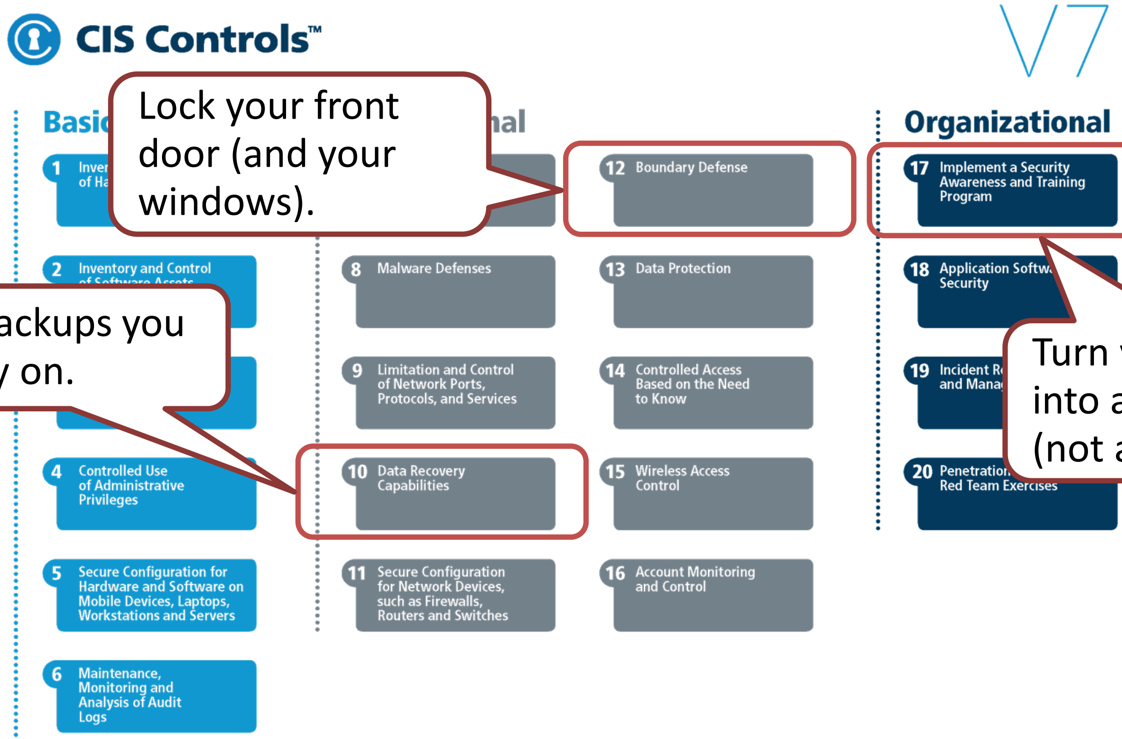
Know what’s supposed to be on your network.
Keep the riff-raff out!

What features do you need to support the business?
Turn the rest off!

Listen to what your systems are telling you.

NEW YORK STATE | Homeland Security and Emergency Services

A framework to guide you



CIS Controls™ V7

Basic

1 Inver of Ha

2 Inventory and Control of Software Assets

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

nal

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Softw Security

19 Incident R and Manag

20 Penetration Red Team Exercises

Lock your front door (and your windows).

Have backups you can rely on.

Turn your workforce into a cyber-asset (not a risk).

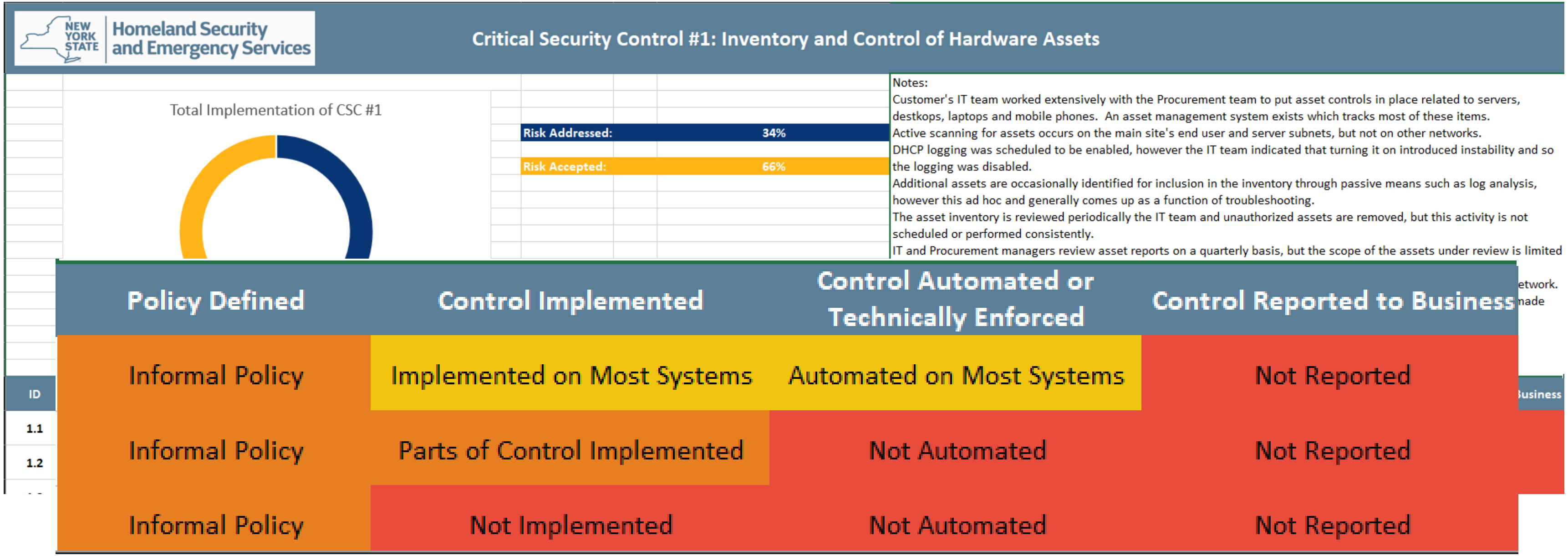
Step 3: Introduce Cyber to Your Workforce

- “Tone at the top” is crucial to success here.
- Phishing exercises can provide a dual benefit:
  - Assessing your workforce’s proficiency
  - Providing “in the moment” training
- Awareness training – and not just “the usual”.
  - Lunch and learns, departmental cyber-Q&A, etc.

Step 4: Measure So You Can Improve

- Remember that framework? It’s about to do double duty.
- Get some help from people in your organization who can remove barriers and provide resources.
- Brief leadership on progress and needs.

Cybersecurity Risk Assessment Process



Homeland Security and Emergency Services

Critical Security Control #1: Inventory and Control of Hardware Assets

Total Implementation of CSC #1

Risk Addressed:	34%
Risk Accepted:	66%

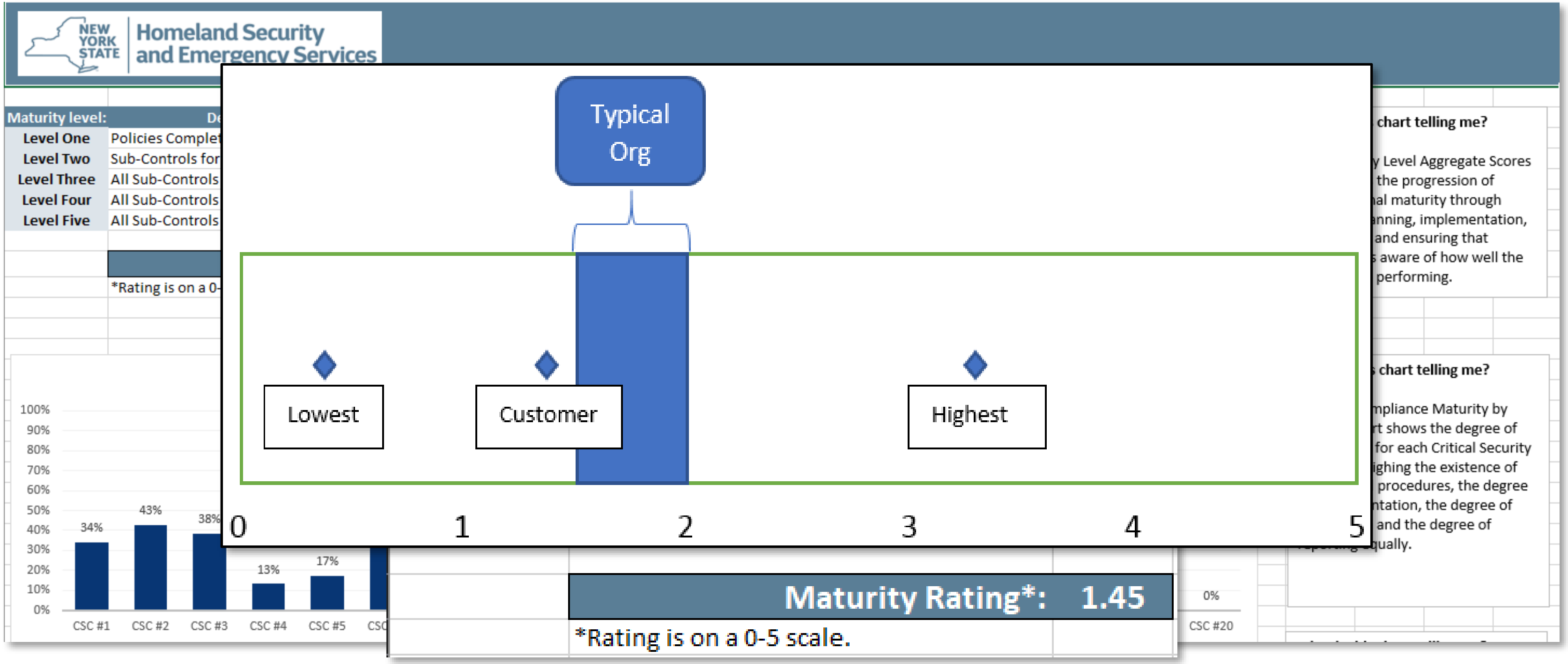
Notes:
Customer's IT team worked extensively with the Procurement team to put asset controls in place related to servers, destkops, laptops and mobile phones. An asset management system exists which tracks most of these items.
Active scanning for assets occurs on the main site's end user and server subnets, but not on other networks.
DHCP logging was scheduled to be enabled, however the IT team indicated that turning it on introduced instability and so the logging was disabled.
Additional assets are occasionally identified for inclusion in the inventory through passive means such as log analysis, however this ad hoc and generally comes up as a function of troubleshooting.
The asset inventory is reviewed periodically the IT team and unauthorized assets are removed, but this activity is not scheduled or performed consistently.
IT and Procurement managers review asset reports on a quarterly basis, but the scope of the assets under review is limited

etwork.
nade

ID
1.1
1.2

Policy Defined	Control Implemented	Control Automated or Technically Enforced	Control Reported to Business
Informal Policy	Implemented on Most Systems	Automated on Most Systems	Not Reported
Informal Policy	Parts of Control Implemented	Not Automated	Not Reported
Informal Policy	Not Implemented	Not Automated	Not Reported

Cybersecurity Risk Assessment Process



NEW YORK STATE | Homeland Security and Emergency Services

Maturity level:	De
Level One	Policies Complet
Level Two	Sub-Controls for
Level Three	All Sub-Controls
Level Four	All Sub-Controls
Level Five	All Sub-Controls

*Rating is on a 0-

chart telling me?

y Level Aggregate Scores the progression of al maturity through nning, implementation, and ensuring that s aware of how well the performing.

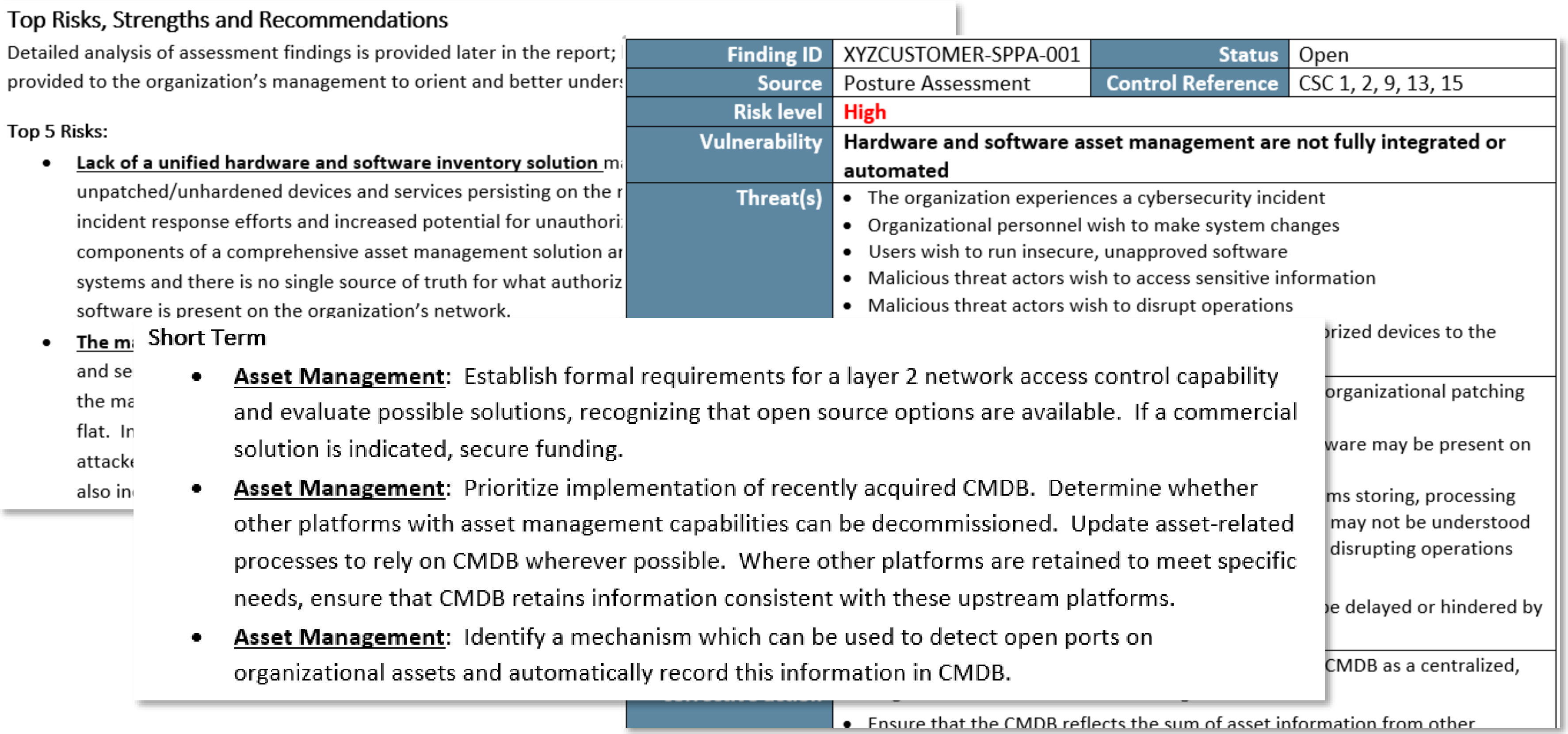
s chart telling me?

mpliance Maturity by rt shows the degree of for each Critical Security ighing the existence of procedures, the degree ntation, the degree of and the degree of qually.

Maturity Rating*: 1.45

*Rating is on a 0-5 scale.

Cybersecurity Risk Assessment Process



Top Risks, Strengths and Recommendations

Detailed analysis of assessment findings is provided later in the report;
provided to the organization's management to orient and better unders

Top 5 Risks:

- **Lack of a unified hardware and software inventory solution** m
  unpatched/unhardened devices and services persisting on the r
  incident response efforts and increased potential for unauthori
  components of a comprehensive asset management solution ar
  systems and there is no single source of truth for what authoriz
  software is present on the organization's network.
- **The m**
  and se
  the ma
  flat. In
  attack
  also in

Finding ID	XYZCUSTOMER-SPPA-001	**Status**	Open
Source	Posture Assessment	**Control Reference**	CSC 1, 2, 9, 13, 15
Risk level	High		
Vulnerability	**Hardware and software asset management are not fully integrated or automated**		
Threat(s)	- The organization experiences a cybersecurity incident - Organizational personnel wish to make system changes - Users wish to run insecure, unapproved software - Malicious threat actors wish to access sensitive information - Malicious threat actors wish to disrupt operations		

rized devices to the

organizational patching

ware may be present on

ms storing, processing
may not be understood
disrupting operations

e delayed or hindered by

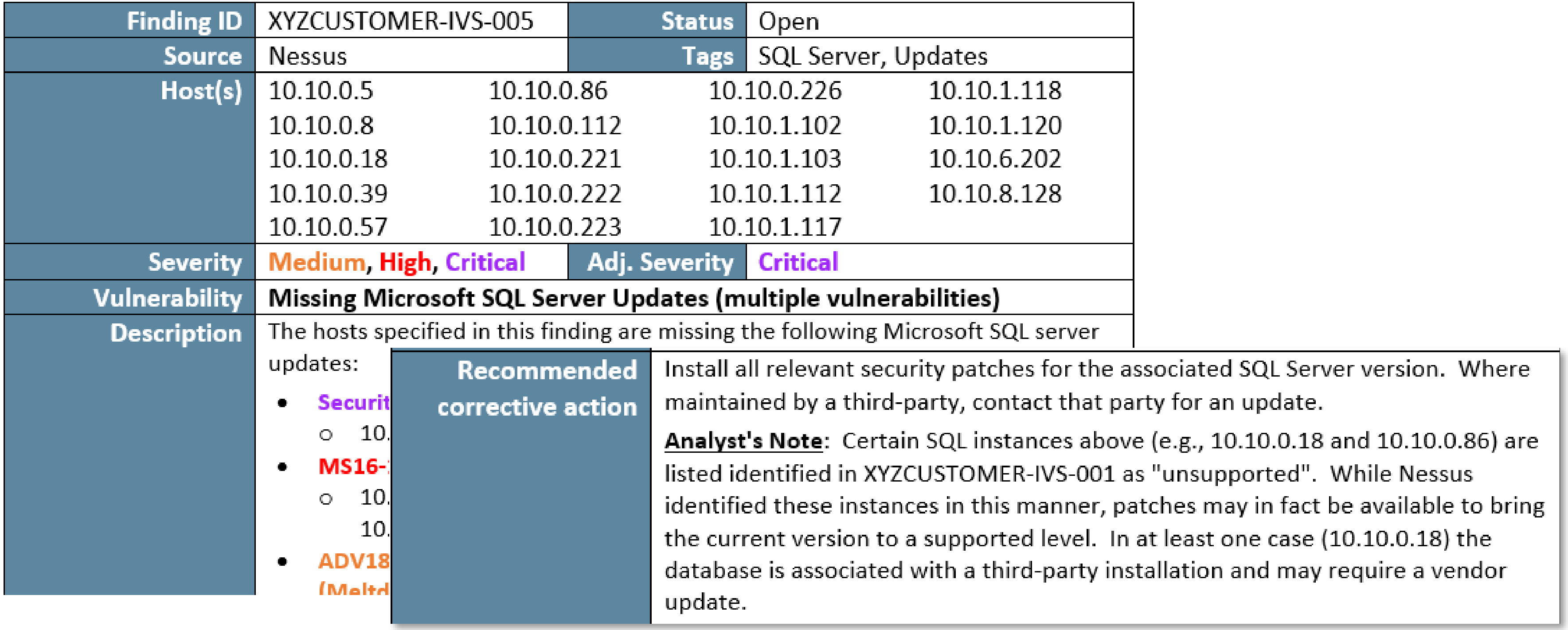
CMDB as a centralized,

- Ensure that the CMDB reflects the sum of asset information from other

Short Term

- **Asset Management**: Establish formal requirements for a layer 2 network access control capability and evaluate possible solutions, recognizing that open source options are available. If a commercial solution is indicated, secure funding.
- **Asset Management**: Prioritize implementation of recently acquired CMDB. Determine whether other platforms with asset management capabilities can be decommissioned. Update asset-related processes to rely on CMDB wherever possible. Where other platforms are retained to meet specific needs, ensure that CMDB retains information consistent with these upstream platforms.
- **Asset Management**: Identify a mechanism which can be used to detect open ports on organizational assets and automatically record this information in CMDB.

Cybersecurity Risk Assessment Process

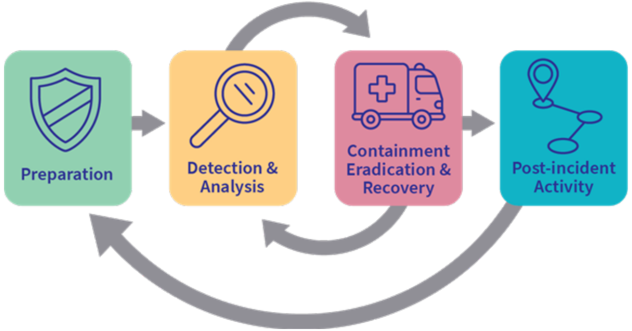


Finding ID	XYZCUSTOMER-IVS-005	**Status**	Open
Source	Nessus	**Tags**	SQL Server, Updates
Host(s)	10.10.0.5 10.10.0.8 10.10.0.18 10.10.0.39 10.10.0.57 10.10.0.86 10.10.0.112 10.10.0.221 10.10.0.222 10.10.0.223 10.10.0.226 10.10.1.102 10.10.1.103 10.10.1.112 10.10.1.117 10.10.1.118 10.10.1.120 10.10.6.202 10.10.8.128		
Severity	Medium, High, Critical	**Adj. Severity**	Critical
Vulnerability	**Missing Microsoft SQL Server Updates (multiple vulnerabilities)**		
Description	The hosts specified in this finding are missing the following Microsoft SQL server updates: • Securit ○ 10. • MS16- ○ 10. 10. • ADV18 (Meltd		

Recommended corrective action	Install all relevant security patches for the associated SQL Server version. Where maintained by a third-party, contact that party for an update. **Analyst's Note**: Certain SQL instances above (e.g., 10.10.0.18 and 10.10.0.86) are listed identified in XYZCUSTOMER-IVS-001 as "unsupported". While Nessus identified these instances in this manner, patches may in fact be available to bring the current version to a supported level. In at least one case (10.10.0.18) the database is associated with a third-party installation and may require a vendor update.

Step 5: Prepare for the Inevitable

- Your organization will eventually experience a cyber-incident.
- Lean on your organization’s COOP if you have one.
- Develop a cyber-specific plan that covers:



- Develop relationships with third parties who can help.
- Practice, practice, practice.

Agenda

- ✓ Introductions
- ✓ Real Risks
- ✓ Five Steps
- ➢ **Helpful Resources**
- ▪ Questions?

Resources

- **NYS DHSES CIRT** – proactive and response services for SLTTs
  - http://www.dhses.ny.gov/oct/cirt/index.cfm
- **CIS** – cyber frameworks and benchmarks
  - https://www.cisecurity.org/
- **MS-ISAC** – monitoring and cyber intelligence for SLTTs
  - https://www.cisecurity.org/ms-isac/
- **NIST** – small business cyber planning and training
  - https://www.nist.gov/itl/smallbusinesscyber
- **GCA** – small business cyber toolkit
  - https://gcatoolkit.org/smallbusiness/
- **FBI** – criminal investigation of cyber crime
  - https://www.fbi.gov/investigate/cyber

Contact Information

Contact DHSES Cyber Incident Response Team (CIRT)

- To report a cyber incident please call: 1 (844) OCT-CIRT | 1 (844) 628-2478
- To request DHSES CIRT cyber support please email: CIRT@dhses.ny.gov
- http://www.dhses.ny.gov/oct/cirt