WOLF
& COMPANY, P.C.

Cybersecurity Threats & Challenges

January 22, 2020

WOLF
& COMPANY, P.C.

Today’s Agenda

- Where we’ve been
- Where we’re going
- Tools and frameworks to help
- Advanced testing

Guidance and Resources

NATIONAL EXAM PROGRAM
OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

- OCIE Cybersecurity Initiatives (2014 and 2016)
- Cybersecurity Sweep 2019
- 2020 Examination Priorities

FINRA

- Report on Cybersecurity Practices (2015 and 2018)
- Checklist for a Small Firm's Cybersecurity Program

NIST

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- Special Publication 800-53

Center for Internet Security

- Critical Security Controls ("SANS Top 20")

Insights from OCIE Exams

2014 OCIE Focus Areas

- Governance and risk management
- Protection of networks and data
- Remote customer access and fund transfer requests
- Third-party risk management
- Detection of unauthorized activity

2014 OCIE Results

- **Many BCPs don't address cyber resilience**
  - Very few address liability for client losses
- **Most perform cyber risk assessments, but few include third-party service providers**
- **Overall, vendor management practices are inconsistent**
- **Social Engineering:**
  - Over half of the firms examined reported receiving phishing email(s) that asked the recipient to transfer funds out fraudulently
  - 26% Reported loss(es) over $5,000 to social engineering
  - Often resulting from employee error
- **Only 30% of IAs have a designated CISO**
- **Only 21% of IAs have cybercrime insurance**

2016 OCIE Focus Areas

Governance and risk management

Access rights and controls

Data loss prevention

Vendor management

Security awareness training

Incident response

2016 OCIE Results

- **Most firms had governance, formal policies, and a risk assessment program in place**
- **Most performed vulnerability assessments and/or penetration testing**
  - However, many did not effectively remediate problems
  - Some had significant missing patches
- **40% of investment advisors' IRPs did NOT include customer data breach response procedures**
- **Almost all had vendor management programs**

2016 OCIE Results (continued)

- **Majority of firms' policies were generic and/or not adequately implemented**
  - Vague, general, "not reasonably tailored"
  - Contradictory requirements
  - Lack of implementation, monitoring, and enforcement
- **Almost all had policies, procedures, and standards for transferring customer funds to third parties**
  - Included customer identification and verification

2020 OCIE Focus Areas

Governance and risk management

Access controls

Data loss prevention

Vendor management

Security awareness training

Incident response and resiliency

Online/mobile customer access

Hardware disposal

Overseeing network/cloud vendors

FINRA Report on Cybersecurity Practices

FINRA Report on Cybersecurity

- **Released December 2018**
  - First edition was February 2015
  - 2018 update is incremental
- **Intended to be an instructive resource**
- **Largely mirrors SEC OCIE areas of focus**

FINRA Report on Cybersecurity

Branch Controls

- Ensure home office controls extend to all offices/locations
- Written security policies
- Asset inventory
  - Hardware, software, appliances
- Technical controls
  - Network and application security
  - Access rights management/least privilege
  - Disposal of physical media
- Internal audit program to monitor branch compliance

WOLF & COMPANY, P.C.

FINRA Report on Cybersecurity

Phishing

- Attacks increasing in quality and sophistication
- Be careful of spear phishing and whaling
- Train employees to recognize and report phishing emails
- Implement technical email controls to limit phishing exposure
- Establish manual confirmation procedures for transaction requests
- Conduct simulated phishing tests regularly
  - Provide remedial training to employees who fail
- Segment customer data
- Use multi-factor authentication (MFA) and Data Loss Prevention (DLP)

WOLF & COMPANY, P.C.

FINRA Report on Cybersecurity

Insider Threats

- Culture/tone at the top
- Strict enforcement of access rights restrictions
  - Rule of least privilege
  - Segregation of duties
  - Periodic review of access rights
  - Limitation of administrative rights
  - Monitoring admin account usage
- Security Information and Event Management (SIEM) tools
- User and Entity Behavioral Analytic (UEBA) tools
- DLP tools
- Identify potentially malicious insiders

FINRA Report on Cybersecurity

Penetration Testing

- Vet a third-party provider
- Risk-based scope and approach
  - Internal, external, web applications
- Annual test performance
- Remediation of issues

Mobile Devices

- Acceptable Use Agreements
- MDM software
  - Strong authentication/MFA
  - Encryption
  - Remote wipe
- MFA for customer access to app

WOLF & COMPANY, P.C.

“Core” Cybersecurity for Small Firms

- **Smaller list of must-haves**
- **Links to external resources for implementation**
- **“Small Firm Cybersecurity Checklist”**
  - Companion workbook for the FINRA guide
  - Provides templates for basic risk assessments and controls identification

NIST Cybersecurity Framework

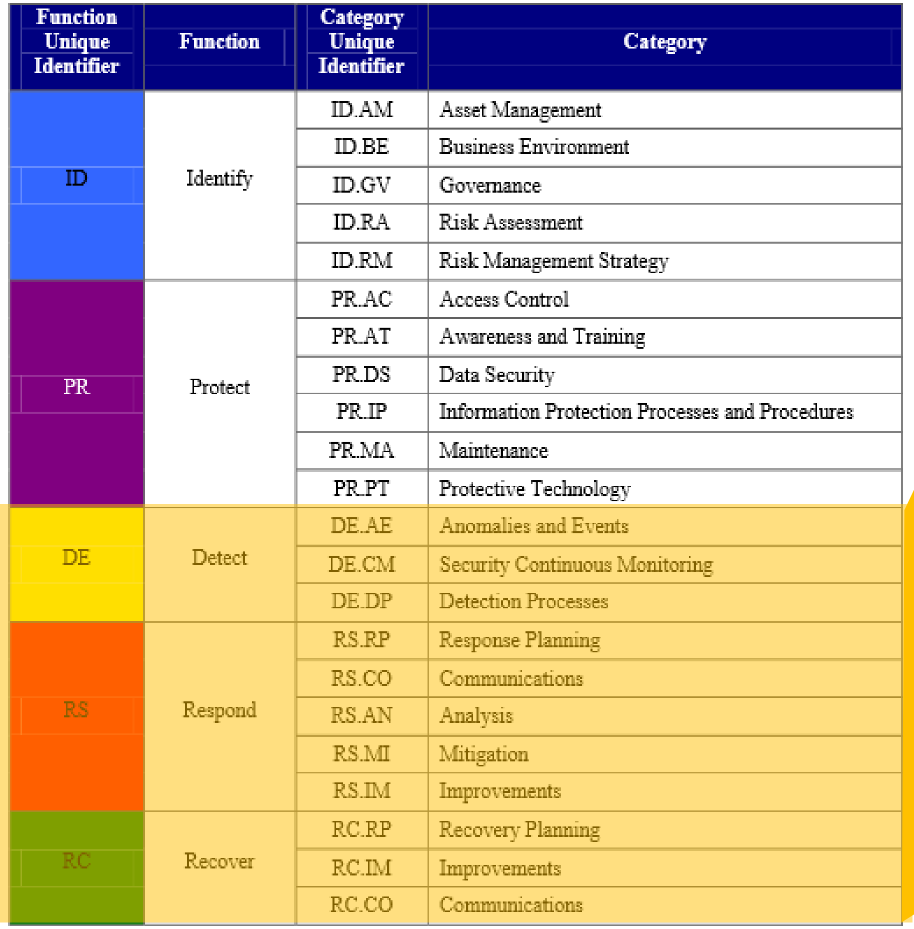
Framework Core

- **Functions**
  - Identify
  - Protect
  - Detect
  - Respond
  - Recover
- **Categories (e.g. access control)**
- **Subcategories (e.g. remote access is managed)**
- **Informative References**
  - CIS Critical Security Controls
  - COBIT 5
  - ISO 27001
  - NIST SP 800-53 (FISMA)

Implementation Tiers

- **PARTIAL (Tier 1)**
  - Controls are ad hoc / reactive
  - Limited awareness and integration
- **RISK INFORMED (Tier 2)**
  - Controls are known and enforced, but may be unofficial
  - Risks inform control processes
- **REPEATABLE (Tier 3)**
  - Formal policies define controls
  - Organization-wide risk management function
- **ADAPTIVE (Tier 4)**
  - Continuous improvement process to adapt controls
  - Organization-wide risk management function
  - Active in Information Sharing and Analysis Centers

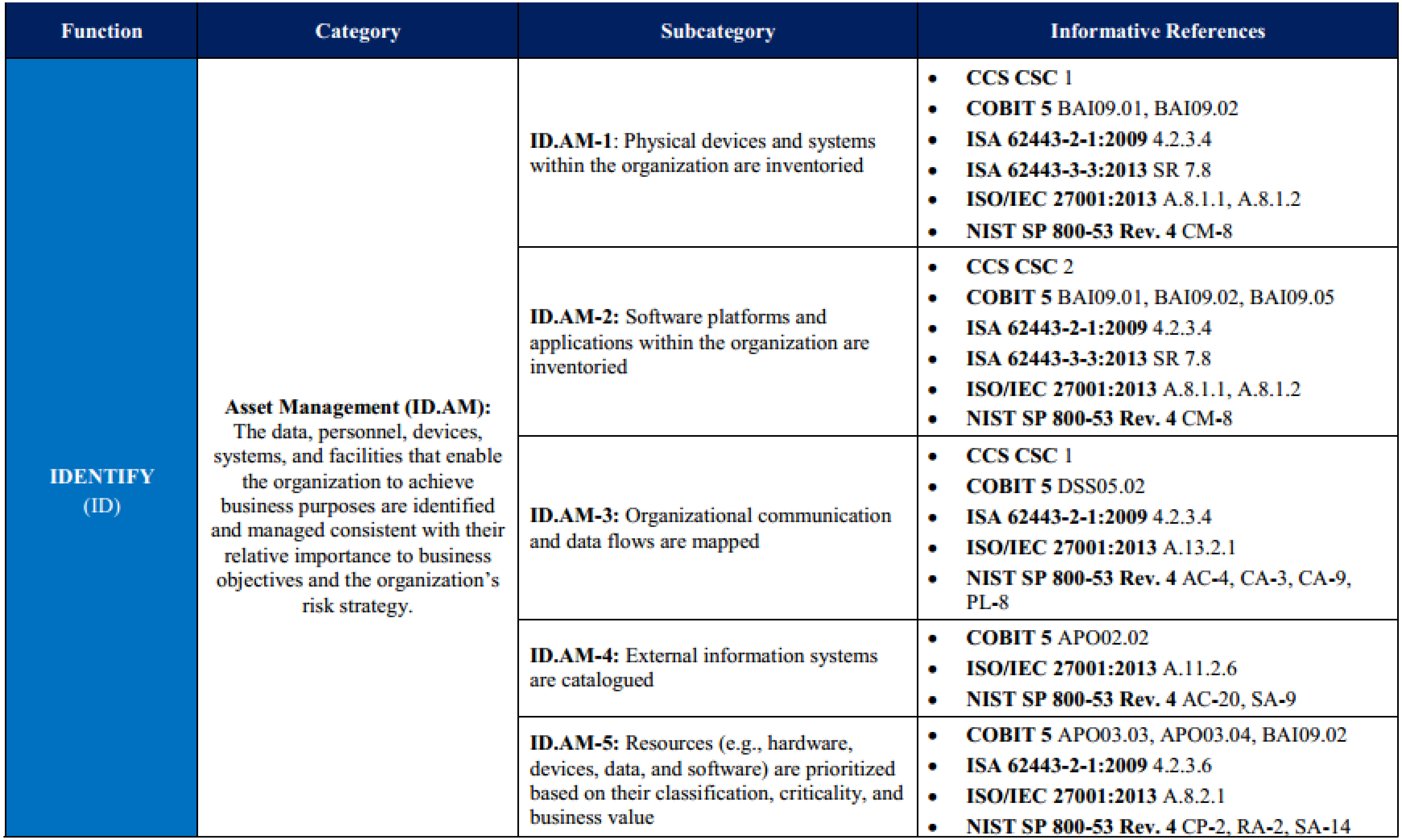
Incident Response Focus



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements
- Recovery Planning
- Improvements
- Communications

Sample Framework Core



Function	Category	Subcategory	Informative References
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 business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6 • **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• **COBIT 5** APO03.03, APO03.04, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.6 • **ISO/IEC 27001:2013** A.8.2.1 • **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14

Identify

Function	Category
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 business objectives and the organization's risk strategy.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Protect

Function	Category
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	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.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Detect

Function	Category
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Respond

Function	Category
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Recover

Function	Category
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

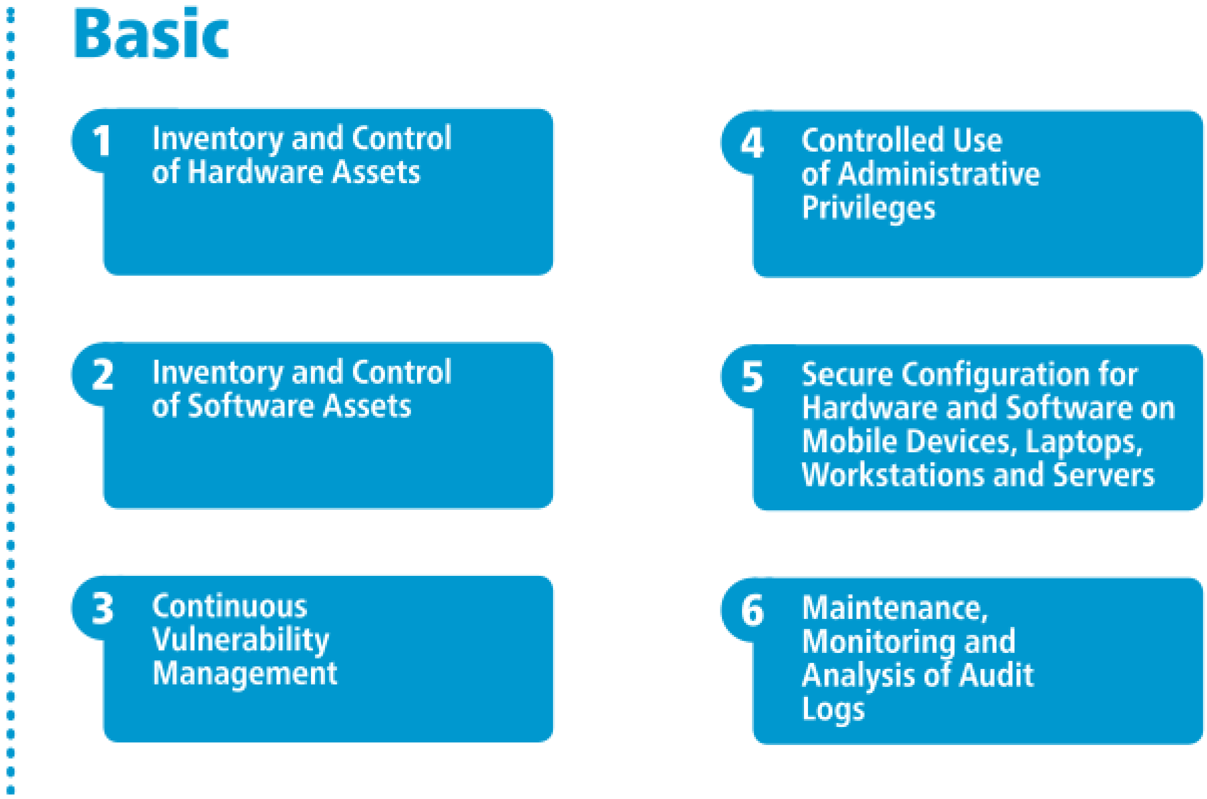
CIS Critical Security Controls

WOLF & COMPANY, P.C.

What is the CIS CSC?

- **Non-profit consortium for internet security**
- **Spun off from SANS (formerly the “SANS Top 20”)**
- **Not regulatory, not governmental**
- **Intended for all industries**
- **Many leaders are from Homeland Security, NSA, etc.**
- **Makes available the Critical Security Controls (CSC)**
  - Based on community experience
  - CSCs “prioritize and focus on a smaller number of actionable controls with high-payoff”
  - Cybersecurity focused
  - Tactical and actionable

Critical Security Controls



Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

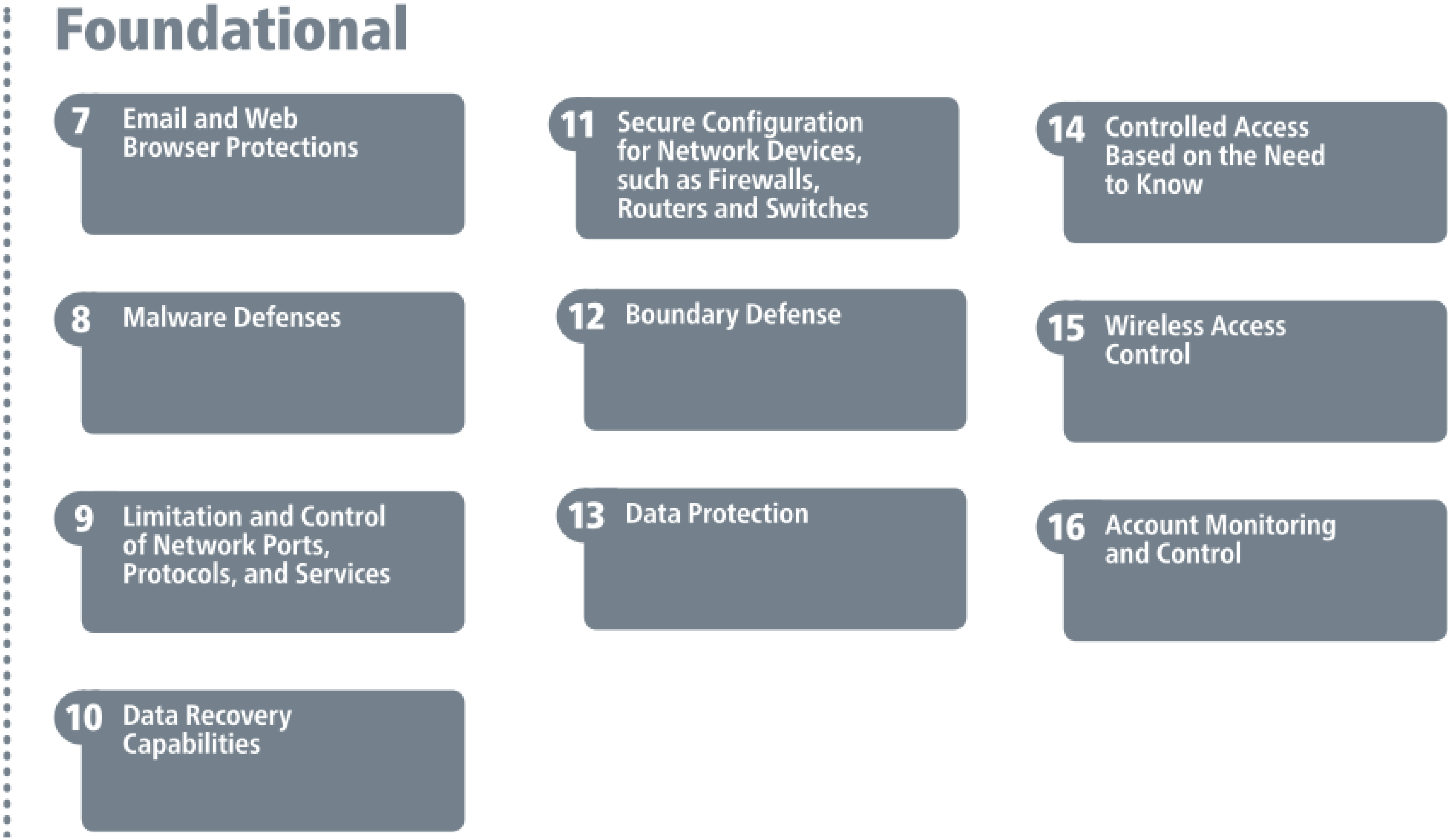
3 Continuous Vulnerability Management

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

Critical Security Controls



Foundational

7 Email and Web Browser Protections

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

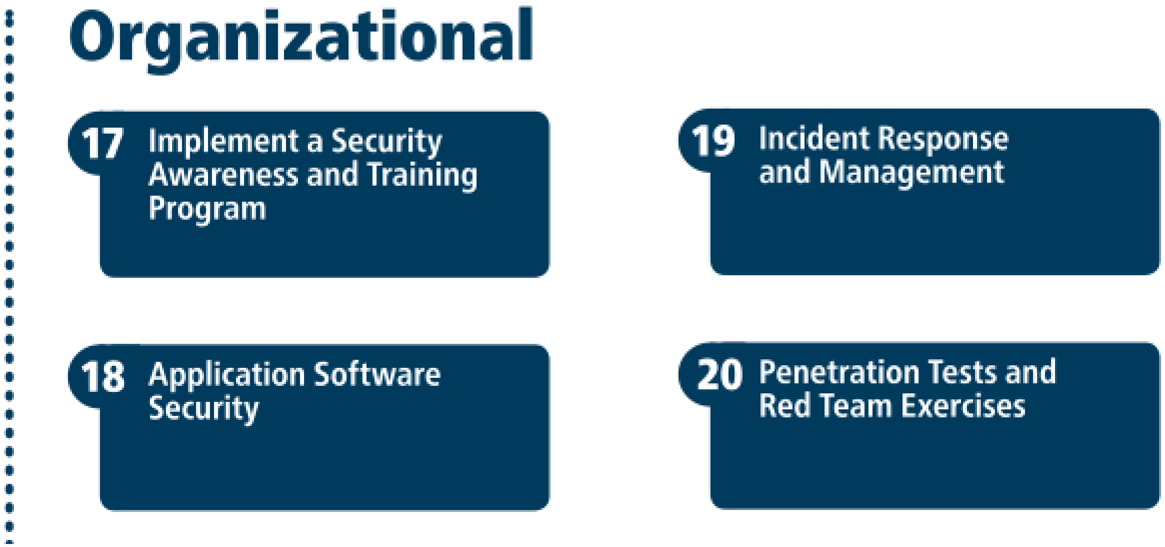
13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Critical Security Controls



Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

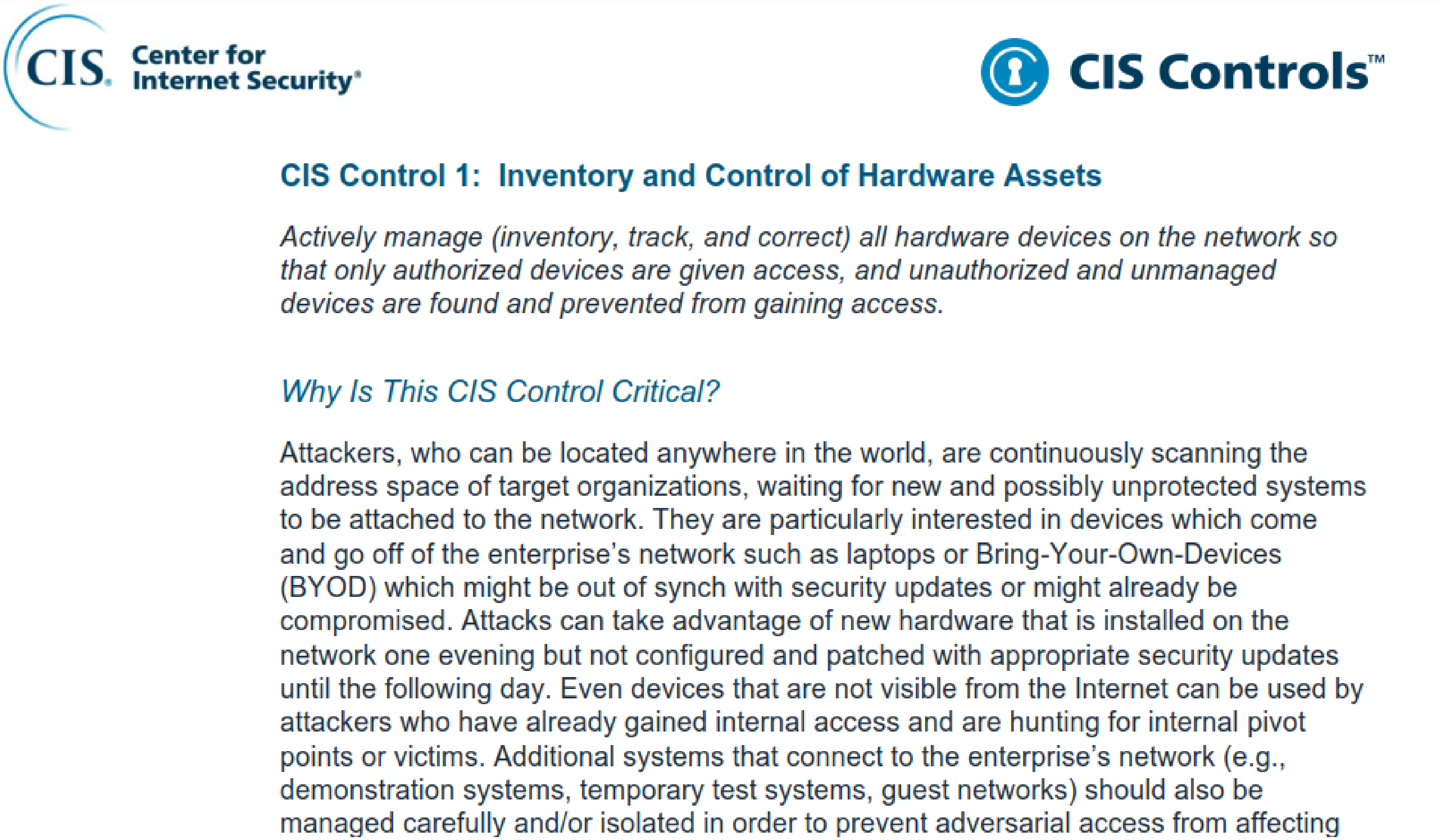
19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

CSC Details

- **Why is this control critical?**
- **How to implement this control**
  - Specific, actionable sub-controls
- **Procedures and tools**
- **Implementation diagrams**

CSC Example



CIS Center for Internet Security®

CIS Controls™

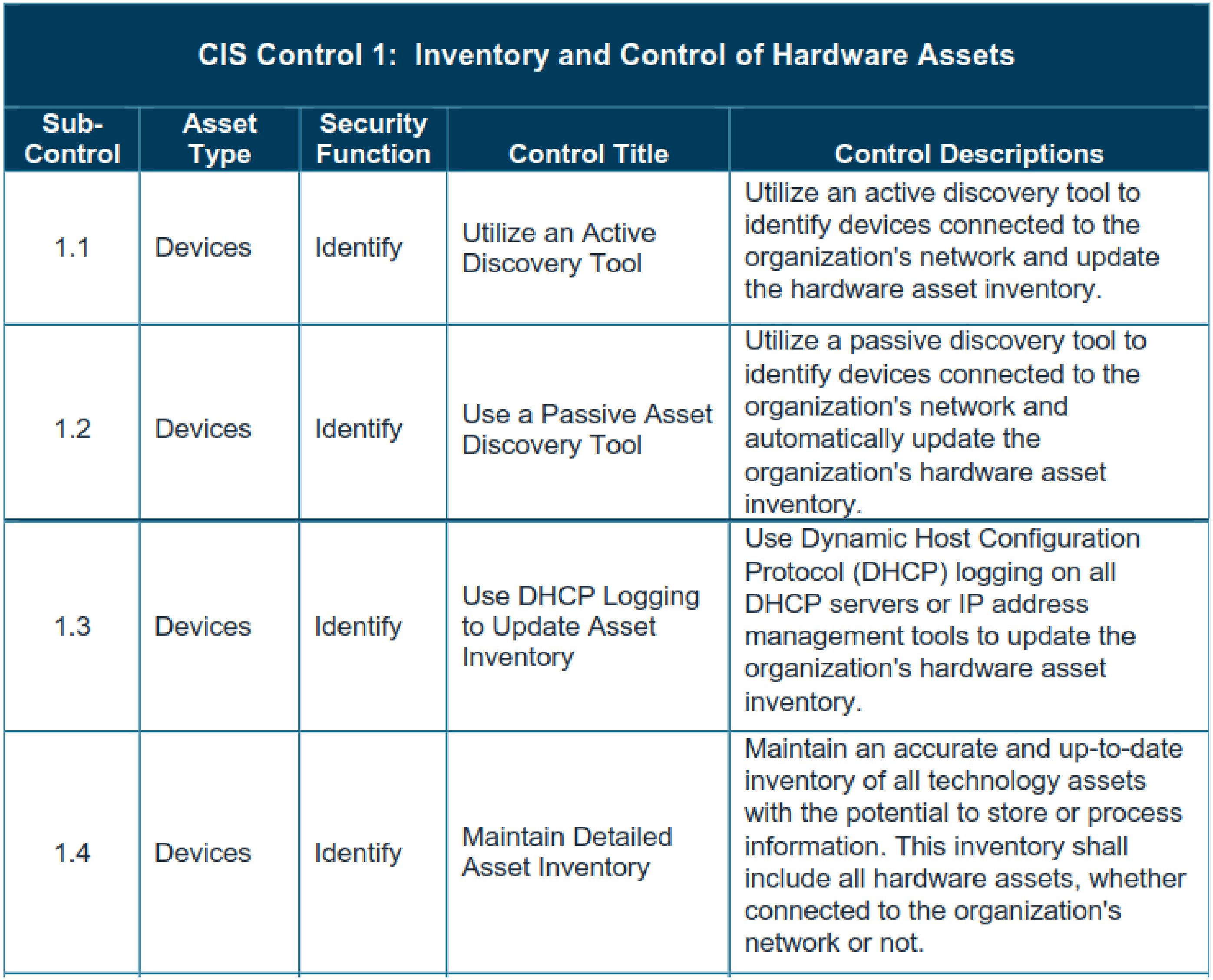
CIS Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Why Is This CIS Control Critical?

Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and possibly unprotected systems to be attached to the network. They are particularly interested in devices which come and go off of the enterprise's network such as laptops or Bring-Your-Own-Devices (BYOD) which might be out of synch with security updates or might already be compromised. Attacks can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Even devices that are not visible from the Internet can be used by attackers who have already gained internal access and are hunting for internal pivot points or victims. Additional systems that connect to the enterprise's network (e.g., demonstration systems, temporary test systems, guest networks) should also be managed carefully and/or isolated in order to prevent adversarial access from affecting

CSC Example



CIS Control 1: Inventory and Control of Hardware Assets				
Sub-Control	**Asset Type**	**Security Function**	**Control Title**	**Control Descriptions**
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.

Penetration Testing

- **Understanding the terms**
  - Vulnerability assessment vs. penetration test
  - Internal vs. external
  - Credentialed vs. uncredentialed
  - Black box vs. grey box vs. white box
  - Red team/blue team/purple team
- **Understanding the scope**
  - Internal network
  - Web applications
  - Hosted/cloud systems
  - Incorporate social engineering?
- **Make it an ongoing program – not an event**

Questions?

Ryan J. Rodrigue, CISSP, CISA

Principal, IT Assurance Services

Wolf & Company, P.C.

Phone: 617-428-5443

Email: rrodrigue@wolfandco.com