Designing and Building a Cybersecurity Program

Based on NIST Cybersecurity Framework

Larry Wilson
lwilson@umassp.edu
May, 2017

Part 1: Background and Introduction

Part 1: Background & Introduction	**Lesson 1: Framing the Problem** **Lesson 2: The Controls Factory Model**
Part 2: The Controls Factory The Engineering Office	**Lesson 3: The Threats and Vulnerabilities** **Lesson 4: Digital Assets, Identities and Business Impact** **Lesson 5: The NIST Cybersecurity Framework (CSF) Design & Build**
Part 2: The Controls Factory The Technology Office	**Lesson 6: The Technology Program Design and Build** **Lesson 7: The Security Operations Center** **Lesson 8: The Technology Program Test and Assurance**
Part 2: The Controls Factory The Business Office	**Lesson 9: The Business Program Design and Build** **Lesson 10: The Cyber Workforce Skills Development** **Lesson 11: The Cyber Risk Program Design and Build**
Part 3: The Program Deliverables	**Lesson 12: The Cybersecurity Program Details** **Lesson 13: The Cyber Risk Program Details**

About the Instructor

Larry Wilson, CISA, CISSP, PCI-ISA
University of Massachusetts
Chief Information Security Officer (CISO)

Primary Role
- Design, implement, operate, maintain the UMass Written Information Security Program (WISP)
- Based on the NIST (National Institute of Science and Technology) Cybersecurity Framework (CSF)
- Technical Controls: The CIS (Center for Internet Security) 20 Critical Security Controls
- Business Controls: The ISO 27002 Code of Practice for Information Security Management

Day to Day Responsibilities
- Manage program implementation and compliance reporting
- Communicate security program deliverables and implementation status
- Establish cybersecurity consulting practice and deliver consulting services
- Design and deliver training in cybersecurity program design, cybersecurity operations

Team Accomplishments
- 2016 ISE (Information Security Executive) Program Award Finalist
- 2013 ISE Program Award Winner

Individual Accomplishments
- 2016 Security Magazine Most Influential People in Security
- 2016 ISACA New England Achievement Award
- 2013 SANS Person Who Made a Difference Award in Cybersecurity
- 2013 ISE Individual Award Finalist

Why is Cybersecurity Important

The Why: The Innovation Economy

To reach the full potential of technology and the associated economic benefits, we need to ensure our computing assets (applications, networks, systems, endpoints , etc.) and our information assets are secure, and our digital identities are trusted.

The What: Effective Cybersecurity Program and Cyber Risk Program

- Establish engineering, technical and business requirements
- Establish a Cybersecurity Program based on the NIST Cybersecurity Framework
  - Build and maintain a comprehensive technical solution – 20 Critical Security Controls
  - Build and maintain a comprehensive business solution – ISO 27002:2013 Controls
  - Build and maintain an executive solution - Cyber Risk Program based on the 2017 AICPA Description Criteria

The Who and the How: People, Process and Technology

- Technology: Design, implement, manage a set of technologies that automate the technical controls
- People: Establish a skilled cyber-workforce to manage our technical, business and executive solutions
- Process: Establish roles / responsibilities and best practices at the technical / operational level, the business / management level and the executive / risk level

Today's Innovation Economy

The Business Model

Where the economy is based on knowledge, technology, entrepreneurship, innovation.

Job & Wage Growth

Where job growth and wage growth exceeds the rest of the economy.

Demand for Knowledge

Demand for STEM-capable workforce (computer science, technology engineering, math)

Technology Enablement

Where technology enables innovation and creates economic prosperity.

Entrepreneurship

Individuals and teams create value via determination, leadership, enthusiasm.

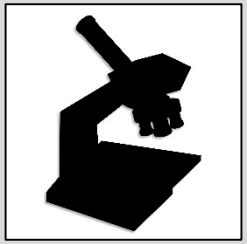
Innovation

Better solutions that meet new requirements, unarticulated needs, existing market needs

Talent

Set of personal characteristics that enhance one's ability to excel in in a certain endeavor..

Research & Development



Discovering and applying knowledge to create new and improved products and services.

Areas of growth of an Innovation Economy

Growth in Information

Growth in Devices

Growth in Software

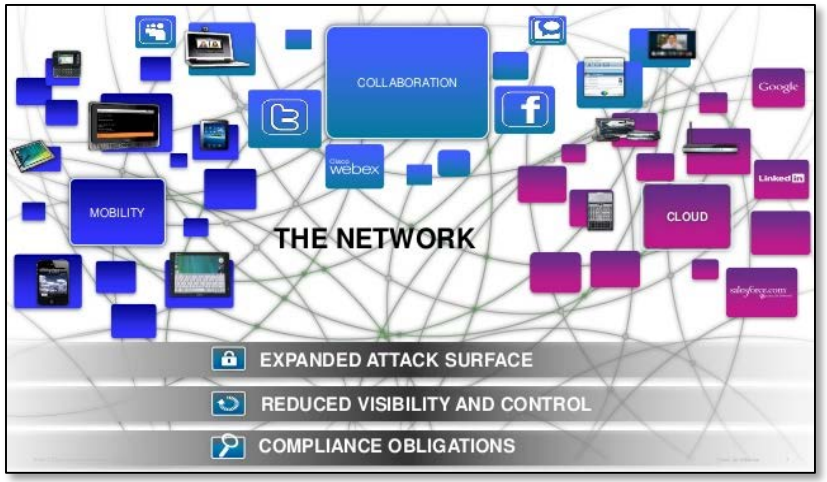
Growth in Cloud

Growth in Outsourcing

Growth in Threats

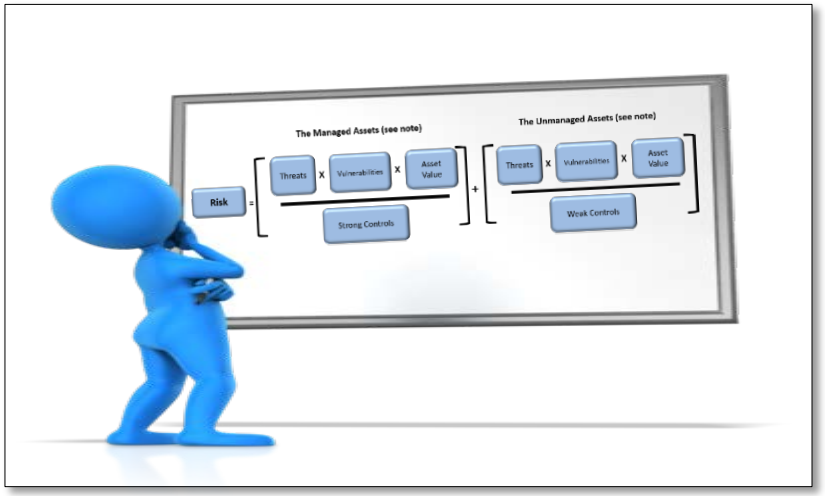
The Key Challenges of an Innovation Economy

The Key Business Challenges



The Key Technology Challenges

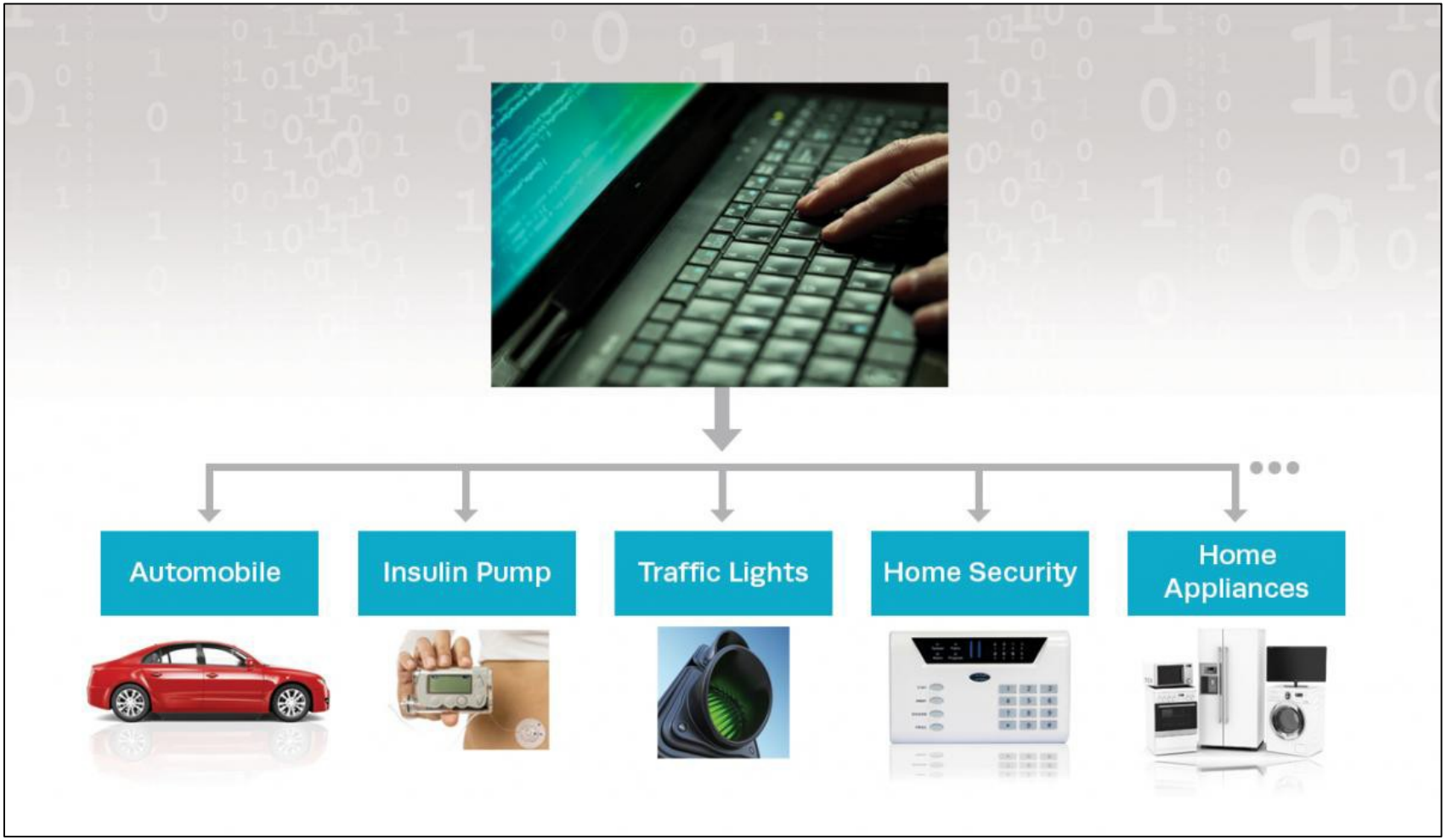
The Key Risk Management Challenges



The Key Workforce Challenges

What is Vulnerable?

Cyber Attacks Could Put Humans and Infrastructure at Risk



Programmable Logic Control (PLC) Vulnerabilities

Automotive Vulnerabilities (Electronic Control Unit)

Traffic Light Vulnerabilities (Malfunction Management Unit)

Industrial Control Vulnerabilities (Programmable Control Unit)

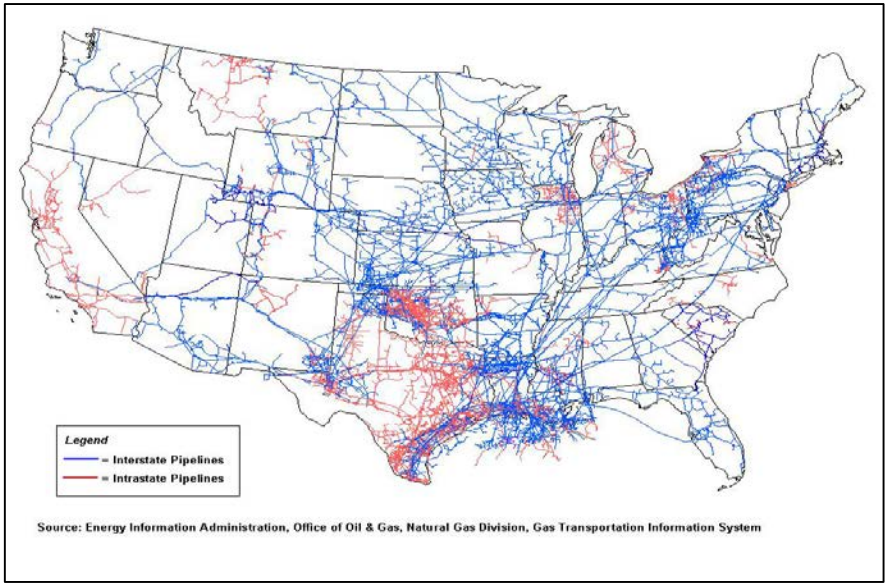
Medical Device Vulnerabilities (Electronic Control Unit)

What Has Happened Already?

The Cyberattack in Turkey: Against gas pipeline

- A recently disclosed 2008 targeted attack on the majority BP-owned Baku-Tbilisi-Ceyhan pipeline in Turkey caused an explosion with flames as high as 150 feet.
- At the time, Baku-Tbilisi-Ceyhan was thought to be one of the most secure pipelines in the world.
- Hackers had shut down alarms, cut off communications and super-pressurized the crude oil in the line. The main weapon at valve station 30 on Aug. 5, 2008, was a keyboard..

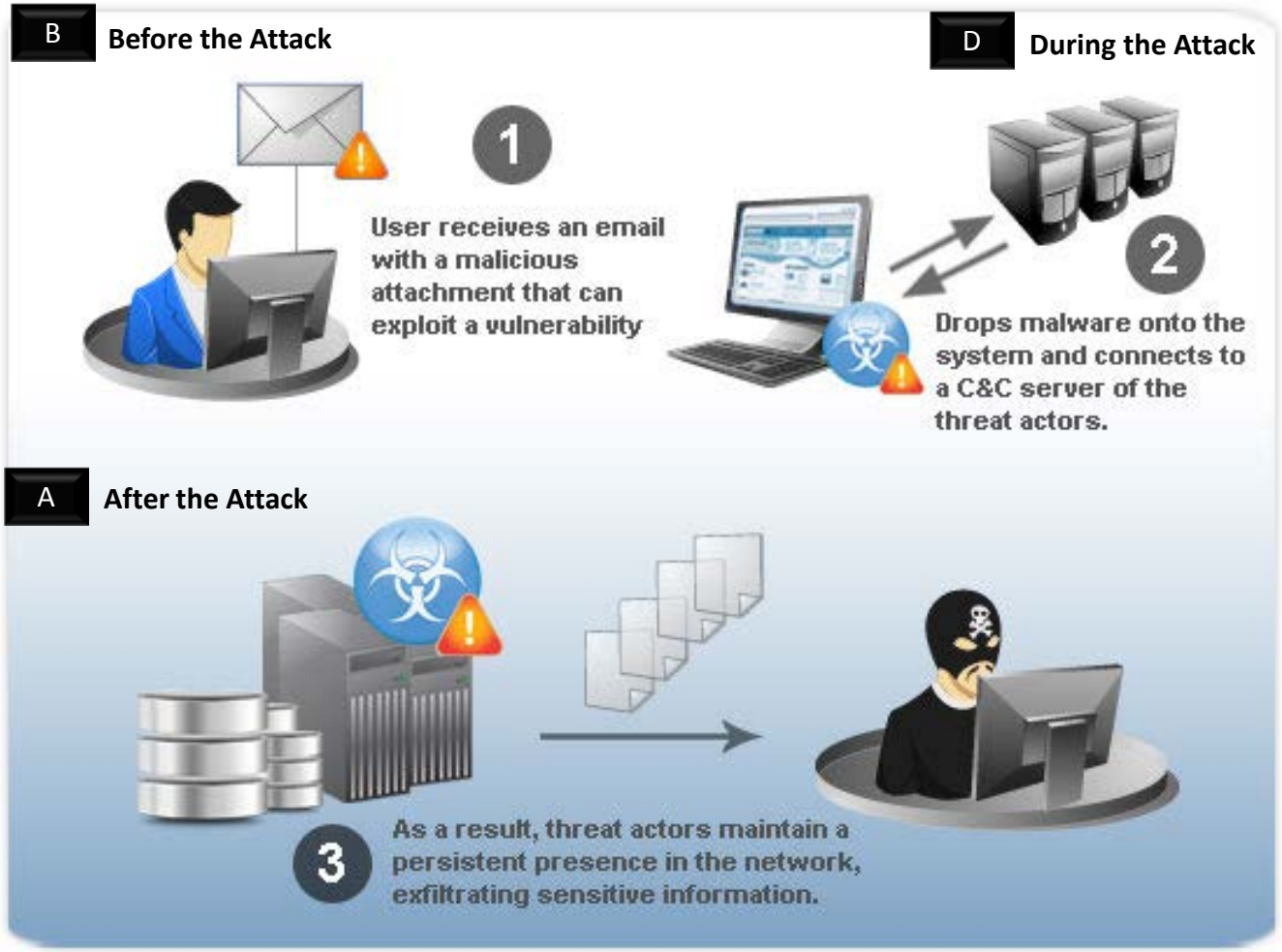
Could that happen here: U.S. Natural Gas Pipelines



- In the U.S., there are millions of miles of pipelines that distribute everything from oil, hazardous liquids, natural gas and chemicals.
- Many of them are approachable above ground, calling their physical security into question.
- These same pipelines are unquestionably vulnerable to cyberattacks that can inflict the same kind of serious damage as physical attacks.

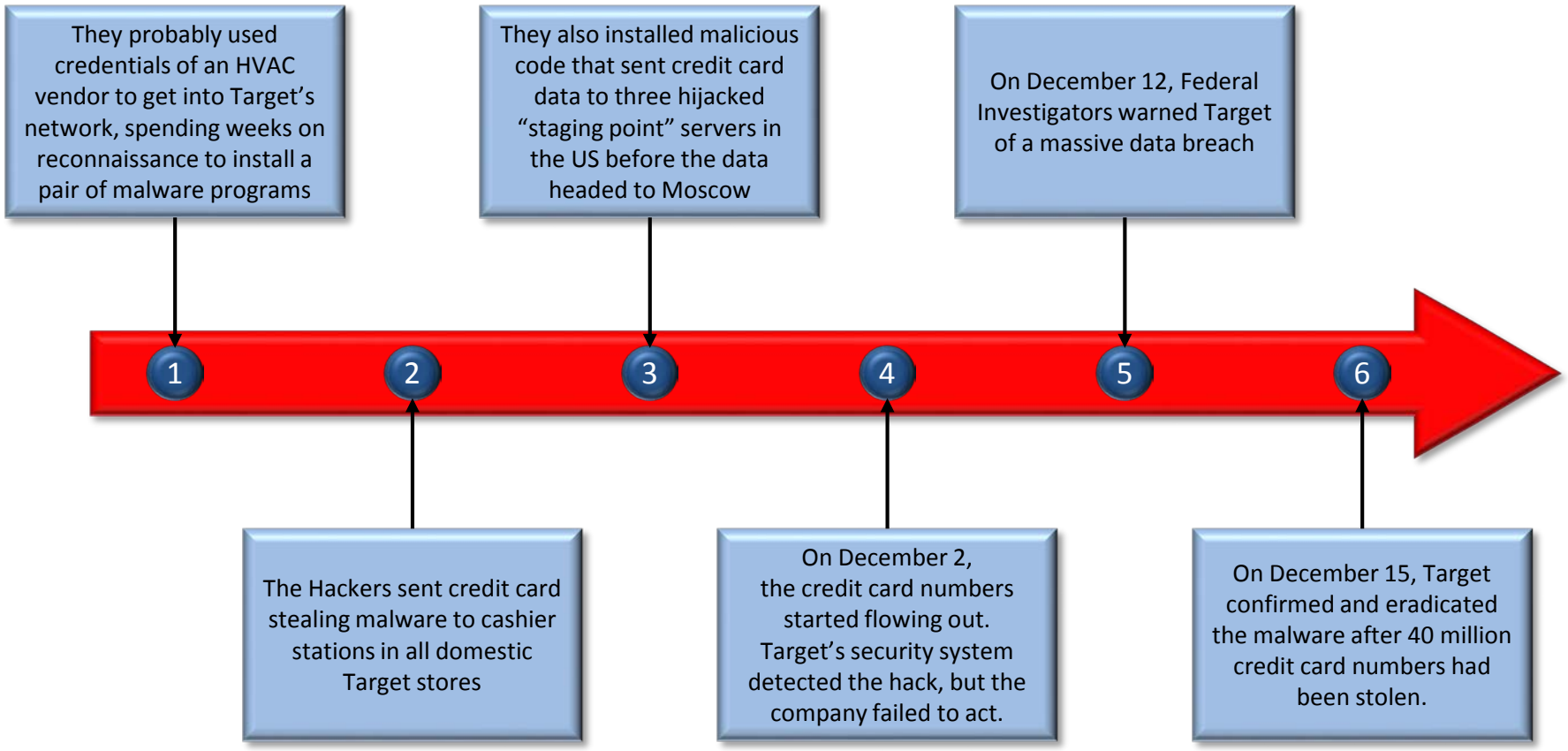
What are the Consequences?

We need to understand How Cyber Attacks Occur

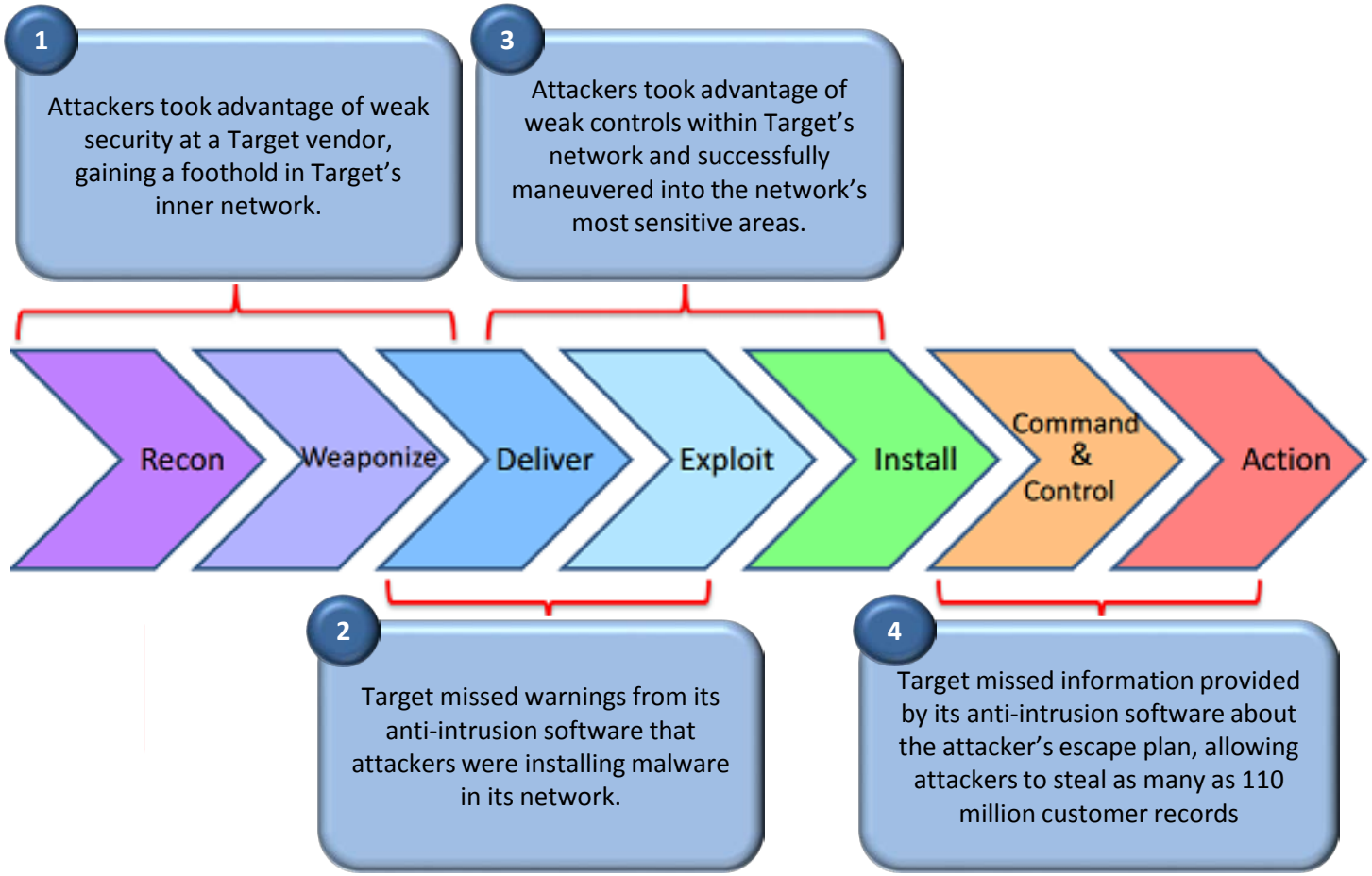


The Target Data Breach Example

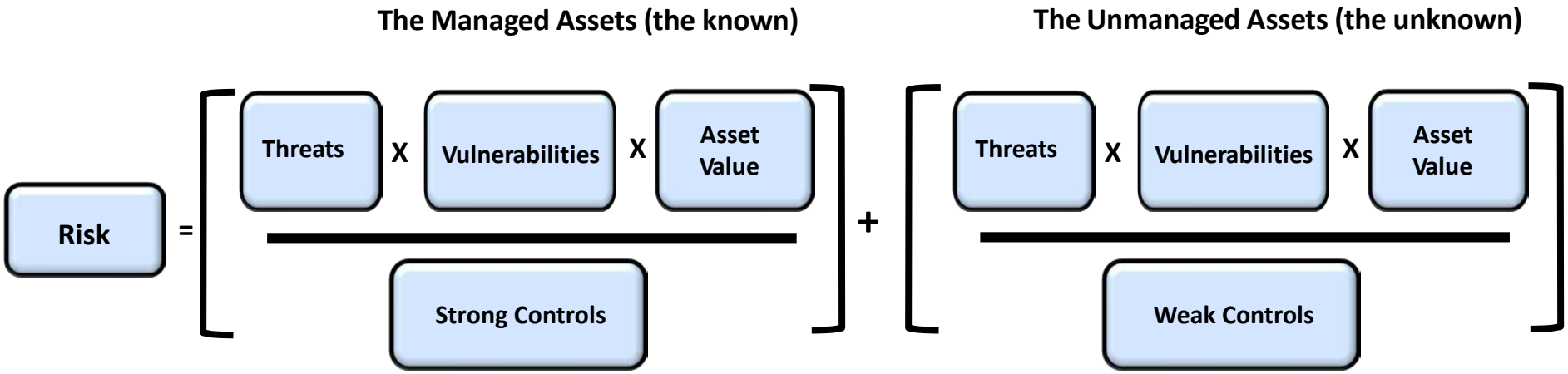
How the Hackers Broke Into Target



Target's Missed Opportunities



The Risk Equation



How do we calculate risk?

1. Threats involve the potential attack against IT resources and information assets
2. Vulnerabilities are weaknesses of IT resources and information that could be exploited by a threat
3. Asset Value is based on criticality of IT resources and information assets
4. Controls are safeguards that protect IT resources and information assets against threats and/or vulnerabilities (see note)
5. Risk is based on the likelihood and impact of a cyber-security incident or data breach

Note: Managed assets imply strong controls; unmanaged assets imply weak controls

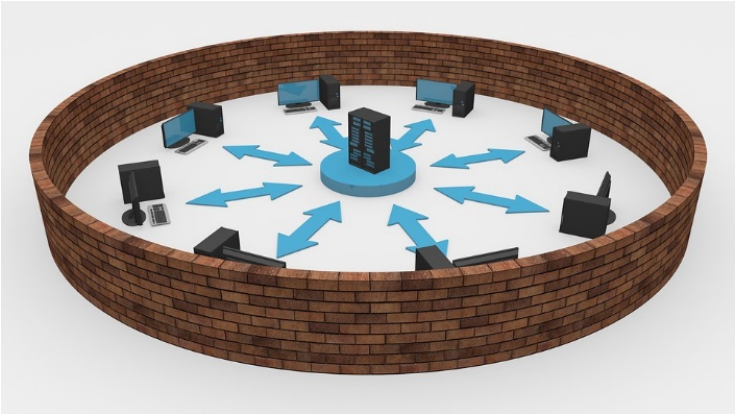
What Are the Risks?

The risks are the unknowns

The Risk of Unknown or Undetected Threats

The Risk of Unknown or Unmitigated Vulnerabilities

The Risk of Unknown or Unprotected Assets



The Risk of Unknown, Missing or Ineffective Controls

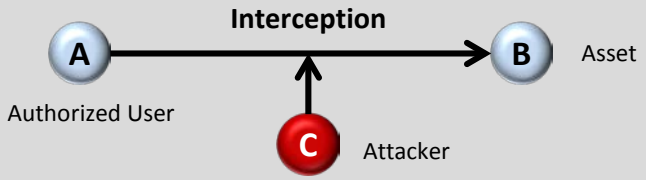
What are the Controls?

The controls are the safeguards

Confidentiality

Attack on Confidentiality (Unauthorized Interception) - An unauthorized individual gains access to an asset

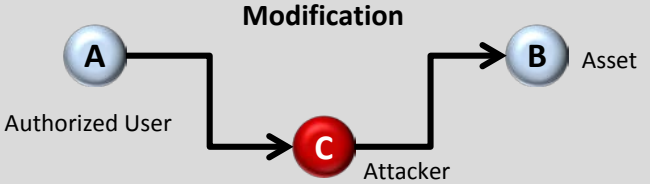
Confidentiality Controls – Ensure only authorized users ***(trusted identities)*** can access the computer resources and information ***(managed assets)***



Integrity

Attack on Integrity (Unauthorized Modification) - An unauthorized individual gains access and tampers with the asset by changing values in a data file, altering a program so it performs differently, etc.

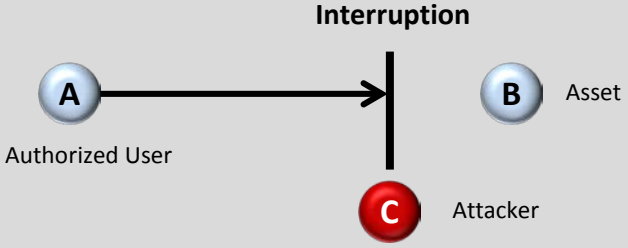
Integrity Controls - Ensure only authorized users can ***(trusted identities)*** modify the computer resources and information ***(managed assets)***



Availability

Attack on Availability (Unauthorized Interruption)- An asset becomes lost, unavailable or unusable to authorized users

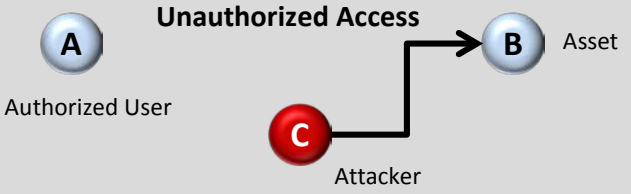
Availability Controls – Ensure assets ***(managed assets)*** are available to authorized users ***(trusted identities)*** when needed



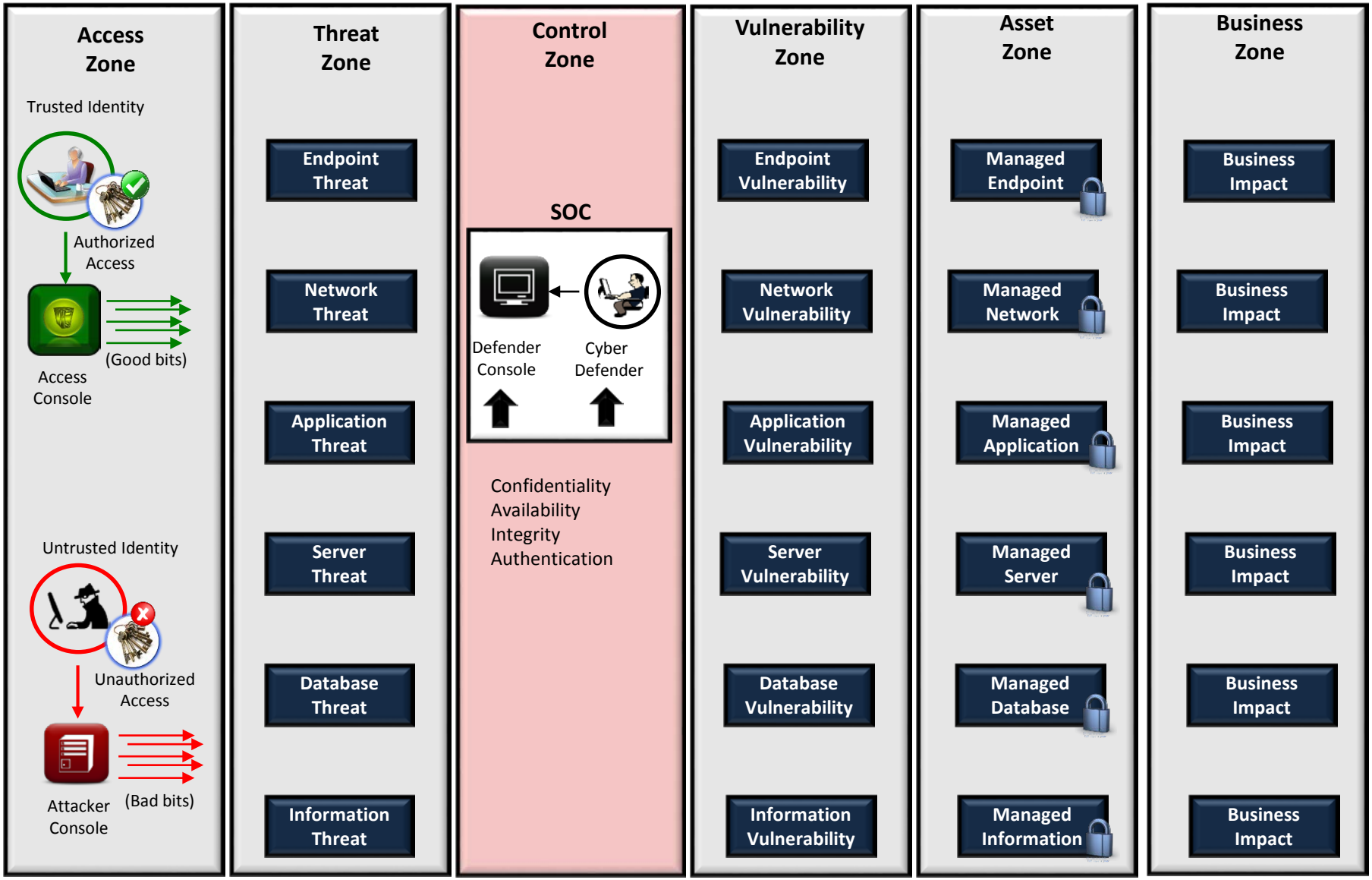
Authentication

Attack on Authentication (Unauthorized Access) - An attacker gains unauthorized access to an asset by using credentials of a known and valid user. As a result, the attacker assumes the privileges of the valid user.

Authentication Controls – Ensure the asset ***(managed assets)*** is able to verify the identity of an authorized user ***(trusted identity)***



The Cyber Attack Model



Build a Room of Controls

To protect our critical assets against known and unknown threats

Trusted Identity

Authorized Access

BUS-01	BUS-02	BUS-03	BUS-04	BUS-05	BUS-06	BUS-07	BUS-08
BUS-09	TEC-01	TEC-02	TEC-03	TEC-04	TEC-05	TEC-06	BUS-10
BUS-11	TEC-07	TEC-08			TEC-09	TEC-10	BUS-12
BUS-13	TEC-11	TEC-12			TEC-13	TEC-14	BUS-14
BUS-15	TEC-15	TEC-16			TEC-17	TEC-18	BUS-16
BUS-17	TEC-19	TEC-20	**Managed Assets**		TEC-21	TEC-22	BUS-18
BUS-19	TEC-23	TEC-24	TEC-25	TEC-26	TEC-27	TEC-28	BUS-20
BUS-21	BUS-22	BUS-23	BUS-24	BUS-25	BUS-26	BUS-27	BUS-28

B **BUS** – Business Controls

T **TEC** – Technical Controls

The NIST Cybersecurity Framework (CSF)

Framework Core

Functions	Categories	Subcategories
Identify	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management (ID.RM)	ID.AM-1 to ID.AM-6 ID.BE-1 to ID.BE-5 ID.GV-1 to ID.GV-4 ID.RA-1 to ID.RA-6 ID.RM-1 to ID.RM-3
Protect	Access Control (PR.AC) Awareness and Training (PR.AT) Data Security (PR.DS) Information Protection Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT)	PR.AC-1 to PR.AC-5 PR.AT-1 to PR.AT-5 PR.DS-1 to PR.DS-9 PR.IP-1 to PR.IP-11 PR.MA-1 to PR.MA-2 PR.PT-1 to PR.PT-5
Detect	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)	DE.AE-1 to DE.AE-5 DE.CM-1 to DE.CM-8 DE.DP-1 to DE.DP-5
Respond	Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM)	RS.RP-1 RS.CO-1 to RS.CO-5 RS.AN-1 to RS.AN-4 RS.MI-1 to RS.MI-3 RS.IM-1 to RS.IM-2
Recover	Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)	RC.RP-1 RC.IM-1 to RC.IM-2 RC.CO-1 to RC.CO-2

Framework Tiers

Weak Controls

Tier 1: Partial
- Ad hoc risk management
- Limited cybersecurity risk awareness
- Low external participation

Tier 2: Risk Informed
- Some risk management practices
- Increased awareness, no program
- Informal external participation

Tier 3: Repeatable
- Formalized risk management
- Organization-wide program
- Receives external partner info

Strong Controls

Tier 4: Adaptive
- Adaptive risk management practice
- Cultural, risk-informed program
- Actively shares information

Framework Profile

C

Current Profile

Current state of alignment between core elements and organizational requirements, risk tolerance, & resources

Where am I today relative to the Framework?

Program Roadmap

T

Target Profile

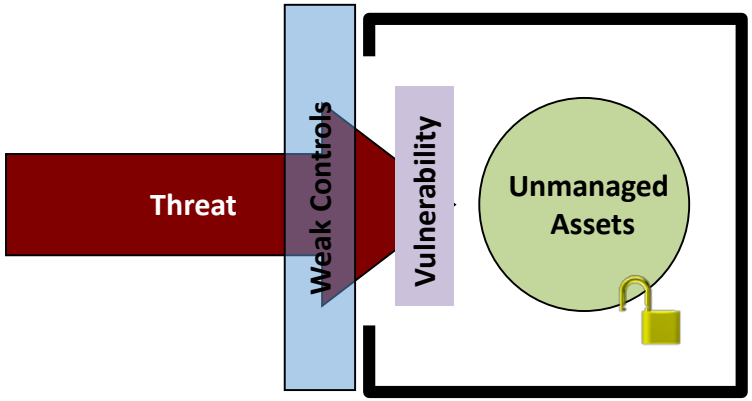
Desired state of alignment between core elements and organizational requirements, risk tolerance, & resources

Where do I aspire to be relative to the Framework?

Building a Risk Model

The Problem:

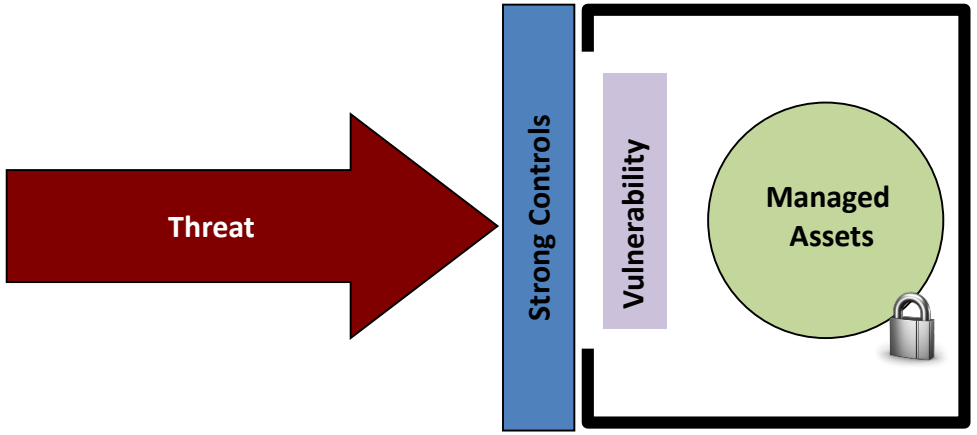
- Unmanaged Assets have weak security controls



Our Unmanaged Assets are at Risk

The Solution:

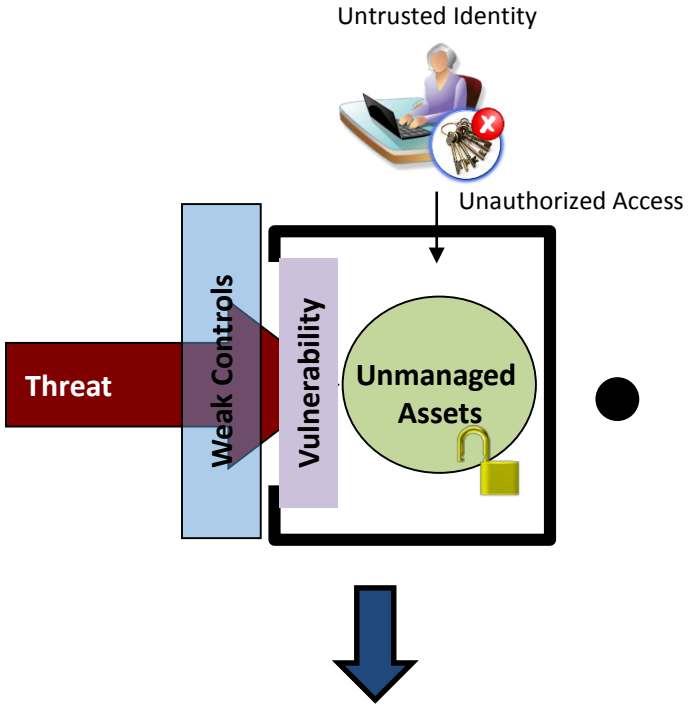
- Managed Assets have strong security controls



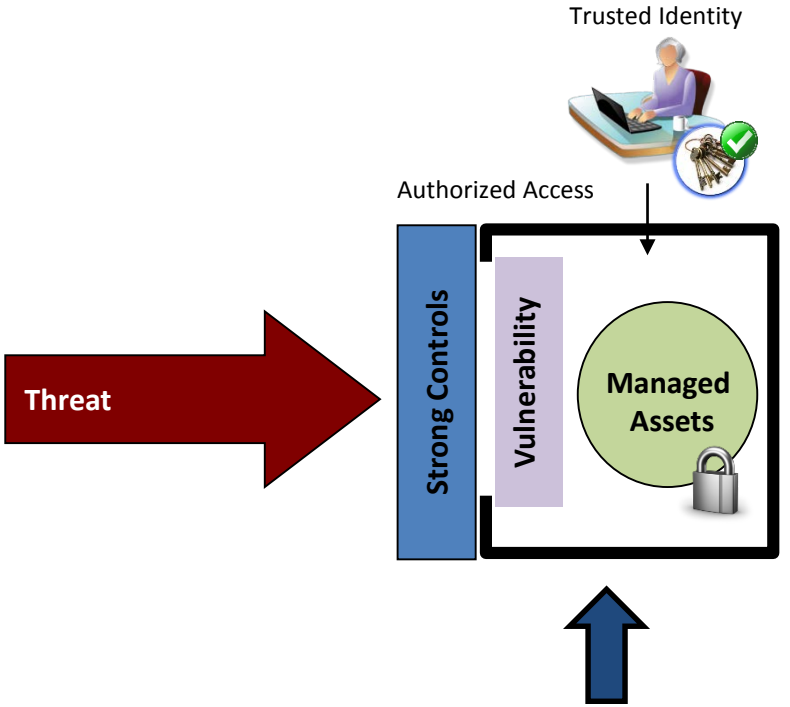
Our Managed Assets are Secure

How do we Manage Risk?

The Unsecure State:
Unmanaged Assets & Untrusted Identities



The Secure State:
Managed Assets & Trusted Identities

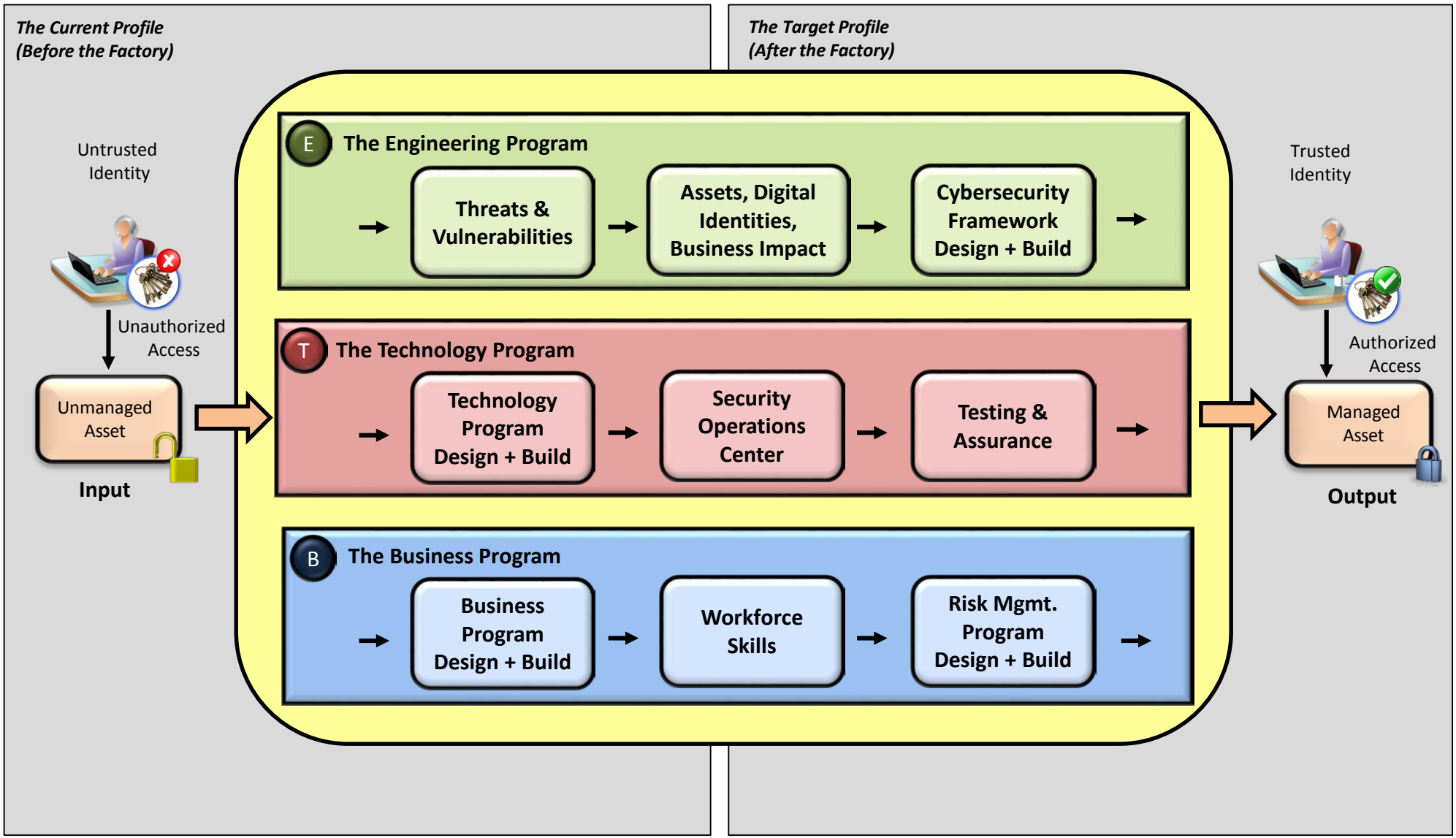


The Engineering Center
- Threat and Vulnerability Area
- Asset and Identity Area
- Controls Framework Area

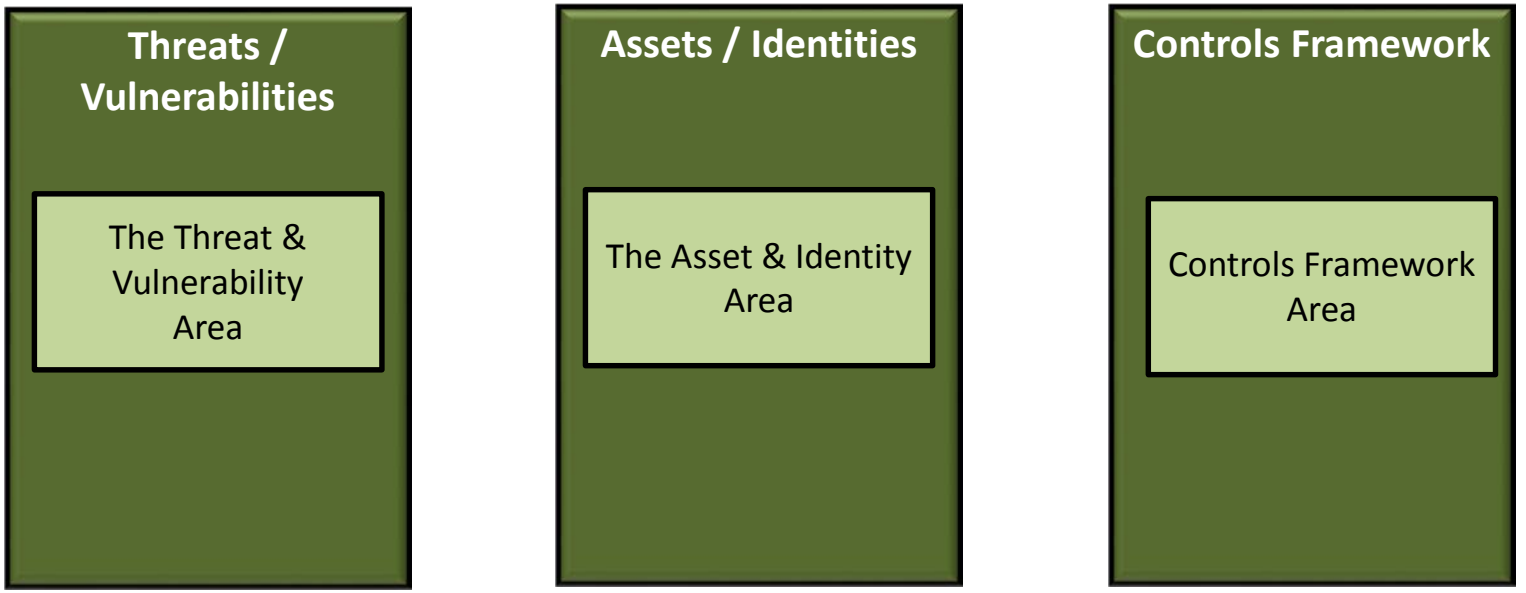
The Technology Center
- Controls Design and Build Area
- Security Operations Center Area
- Testing and Assurance Area

The Business Center
- Controls Design and Build Area
- Workforce Development Area
- Cyber Risk Program Area

The Controls Factory Model



The Engineering Program

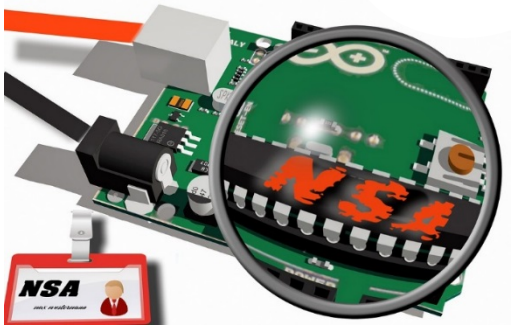


The Cyber Threat Landscape

Distributed Denial of Service Attack

Insider Threat

Cyber Espionage



Malicious Software

Phishing Email

Web Based Attack

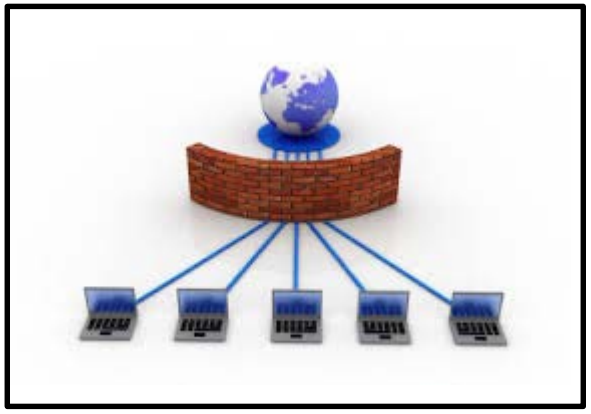
The Vulnerabilities & Exposures

Ineffective Cybersecurity Program

Weak Risk Management Program

Security Policy Deficiencies

Misconfigured Firewalls



Application Vulnerabilities

```
01110010111001111010 11
10001100101010010101 01
10101101101010110110 11
11101011HACKED11110110
00010101001000010111 11
10010101010101010100 10
11111001111110110010 00
```

Inadequate Logging & Monitoring

The Known & Managed Assets

Endpoint Family

Owner = Desktop Manager

Network Family

Owner = Network Manager

Applications

Owner = Application Manager

Servers

Owner = Systems Manager

Databases

Owner = Database Manager

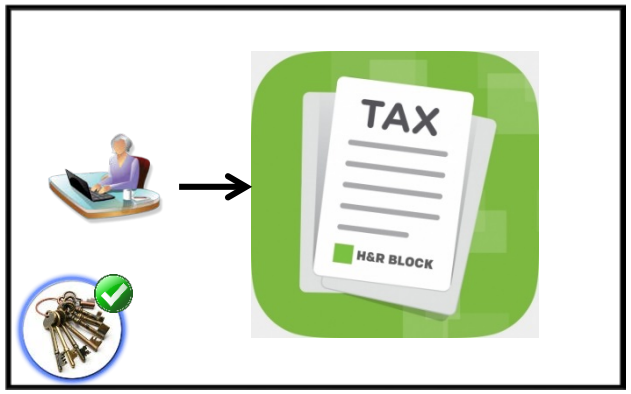
Information / Data

Owner = Business Process Manager

The Known & Trusted Identities

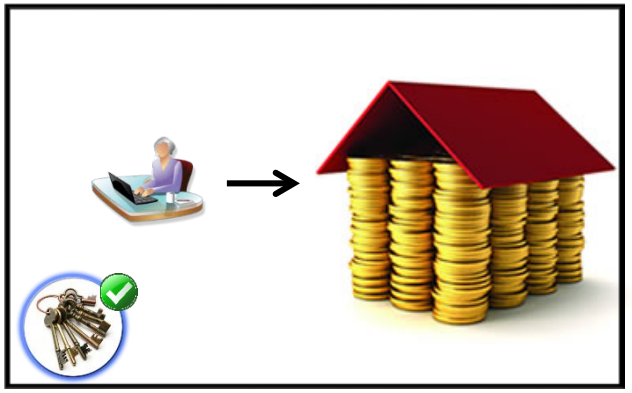
Business Roles

Payroll Analyst



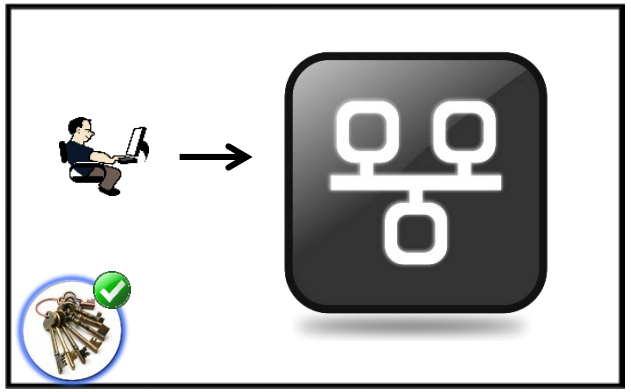
Finance Analyst

Fund Account Analyst

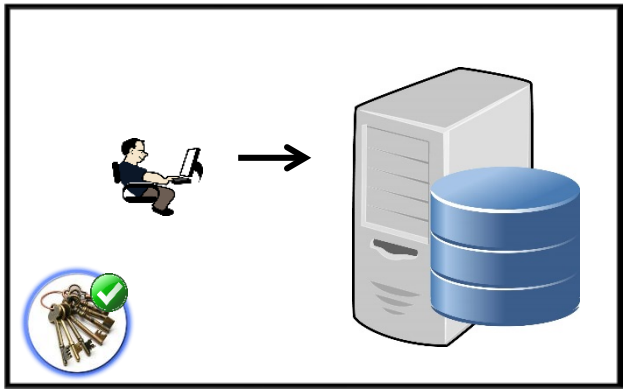


Technical Roles

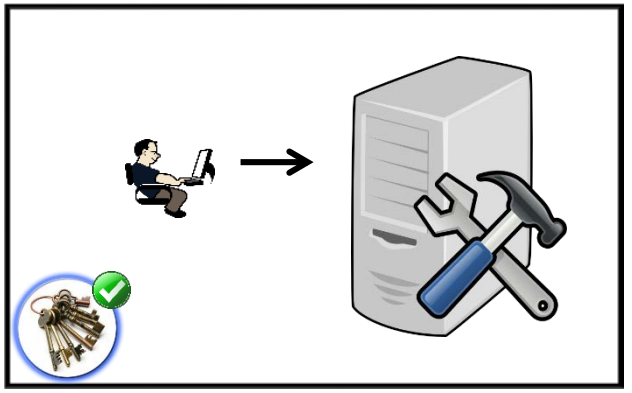
Network Administrator



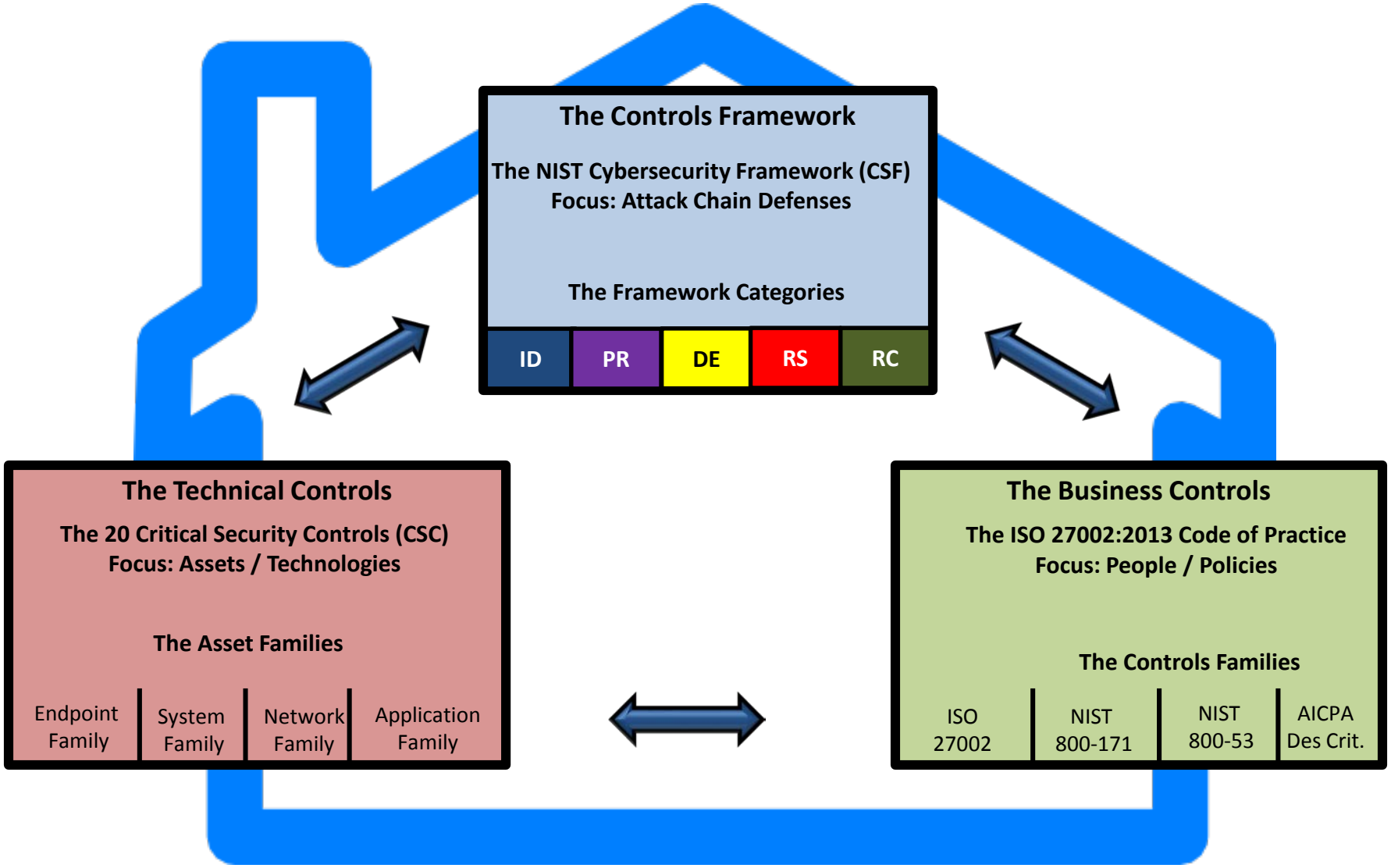
Database Administrator



Systems Administrator

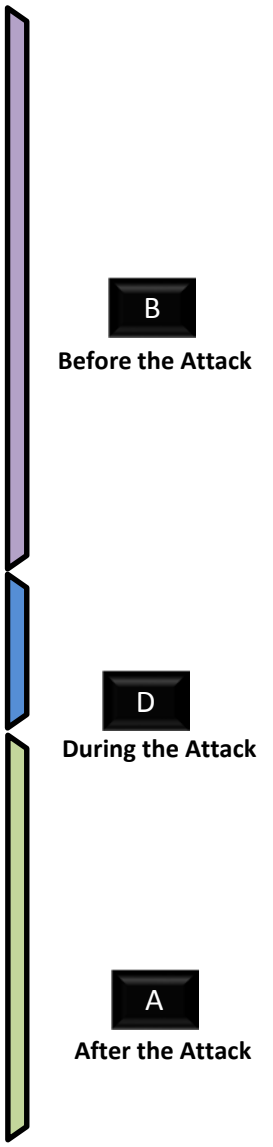


Building a House of Controls



NIST Cybersecurity Framework: Mapping Controls

Core Functions	Categories	Technical Controls	Business Controls
Identify	Asset Management	20 Critical Security Controls	ISO 27002 Code of Practice
	Business Environment	Not Applicable	ISO 27002 Code of Practice
	Governance	Not Applicable	ISO 27002 Code of Practice
	Risk Assessment	20 Critical Security Controls	ISO 27002 Code of Practice
	Risk Management	Not Applicable	Not Applicable
Protect	Access Control	20 Critical Security Controls	ISO 27002 Code of Practice
	Awareness and Training	20 Critical Security Controls	ISO 27002 Code of Practice
	Data Security	20 Critical Security Controls	ISO 27002 Code of Practice
	Information Protection Process	20 Critical Security Controls	ISO 27002 Code of Practice
	Maintenance	20 Critical Security Controls	ISO 27002 Code of Practice
	Protective Technology	20 Critical Security Controls	ISO 27002 Code of Practice
Detect	Anomalies and Events	20 Critical Security Controls	ISO 27002 Code of Practice
	Continuous Monitoring	20 Critical Security Controls	ISO 27002 Code f Practice
	Detection Processes	20 Critical Security Controls	ISO 27002 Code of Practice
Respond	Response Planning	20 Critical Security Controls	ISO 27002 Code of Practice
	Communications	Not Applicable	ISO 27002 Code of Practice
	Analysis	20 Critical Security Controls	ISO 27002 Code of Practice
	Mitigation	20 Critical Security Controls	ISO 27002 Code of Practice
	Improvements	20 Critical Security Controls	ISO 27002 Code of Practice
Recover	Recovery Planning	20 Critical Security Controls	ISO 27002 Code of Practice
	Improvements	20 Critical Security Controls	Not Applicable
	Communications	20 Critical Security Controls	Not Applicable



Technical Controls Mapping

Mapping Critical Security Controls to NIST Cybersecurity Framework (The Technical Controls)

	B	B	D	A	A
CIS Critical Security Control	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
CSC-01: Inventory of Authorized and Unauthorized Devices	ID.AM	PR.DS			
CSC-02: Inventory of Authorized and Unauthorized Software	ID.AM	PR.DS			
CSC-03: Secure configuration of laptops, workstations, servers		PR.IP			
CSC-04: Continuous Vulnerability Assessment and Remediation	ID.RA	PR.IP	DE.CM	RS.MI	
CSC-05: Controlled Use of Administrative Privileges		PR.AC			
CSC-06: Maintenance, Monitoring and Analysis of Audit Logs		PR.PT	DE.AE	RS.AN	
CSC-07: Email and Web Browser Protections		PR.PT			
CSC-08: Malware Defenses		PR.PT	DE.CM		
CSC-09: Limitation and Control of Ports, Protocols, and Services		PR.IP			
CSC-10: Data Recovery Capability					RC.RP
CSC-11: Secure Configuration of Network Devices		PR.IP	DE.AE		
CSC-12: Boundary Defense		PR.AC	DE.AE		
CSC-13: Data Protection		PR.DS			
CSC-14: Controlled Access Based on Need to Know		PR.AC			
CSC-15: Wireless Access Control		PR.AC			
CSC-16: Account Monitoring and Control		PR.AC	DE.CM		
CSC-17: Security Skills Assessment and Appropriate Training		PR.AT			
CSC-18: Application Software Security		PR.IP			
CSC-19: Incident Response and Management			DE.AE	RS. RP	RC.CO
CSC-20: Penetration Tests and Red Team Exercises	ID.RA			RS.IM	RC.IM

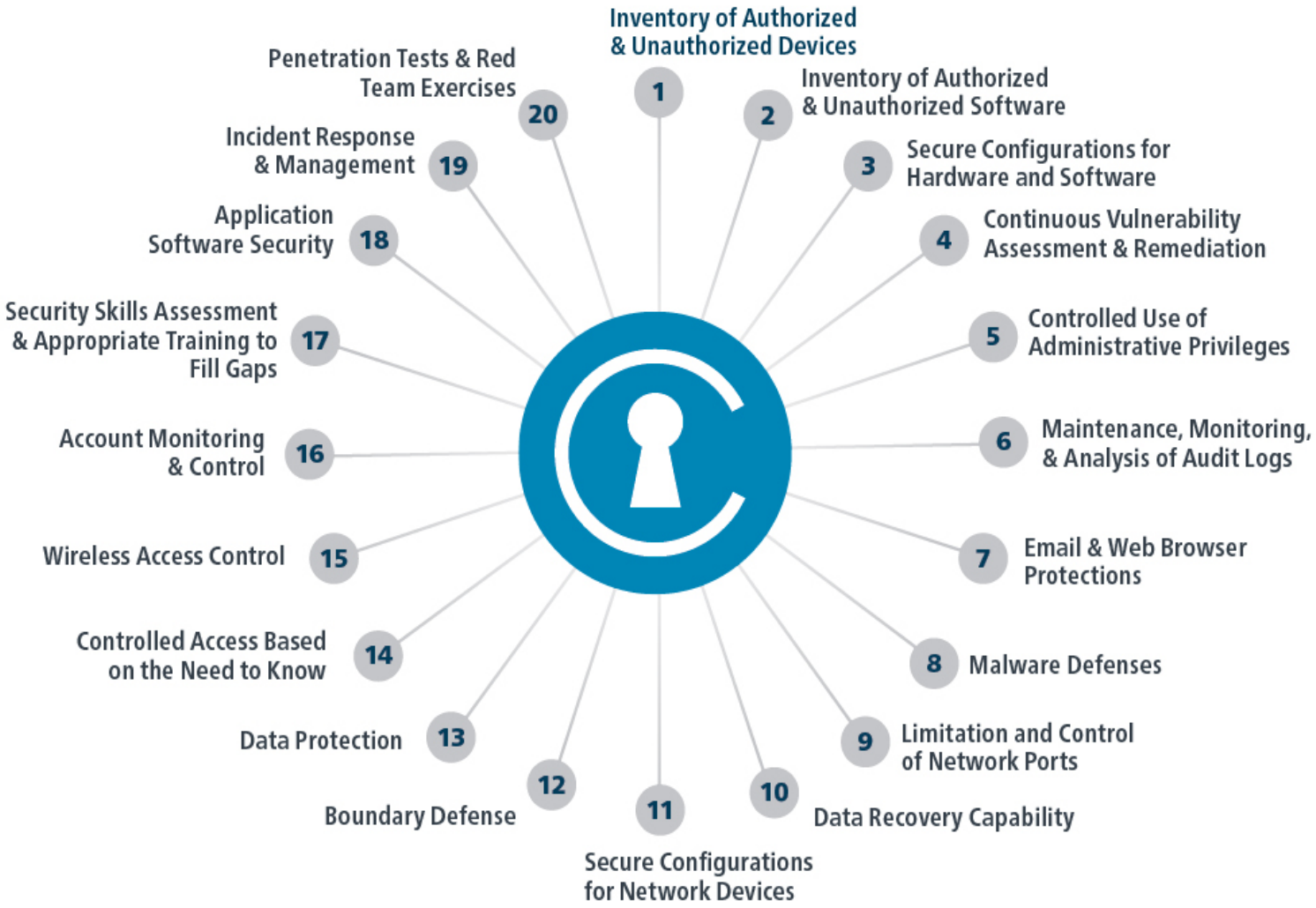
Business Controls Mapping

Mapping ISO 27002 Controls to NIST Cybersecurity Framework (The Business Controls)

	B	B	D	A	A
ISO 27002 Control	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
ISO-A5: Information Security Policies	ID.GV				
ISO-A6: Organization of Information Security	ID.AM	PR.AC	DE.DP	RS.CO	
ISO-A7: Human Resources Security	ID.GV	PR.AT			
ISO-A8: Asset Management	ID.AM	PR.DS			
ISO-A9: Access Control		PR.PT			
ISO-A10: Cryptography		PR.AC			
ISO-A11: Physical and Environmental Security	ID.BE	PR.DS			
ISO-A12: Operations Security	ID.RA	PR.PT	DE.CM	RS.AN	
ISO-A13: Communications Security	ID.AM	PR.DS			
ISO-A14: System Acquisition, Development and Maintenance		PR.DS	DE.DP		
ISO-A15: Supplier Relationships	ID.BE	PR.MA	DE.CM		
ISO-A16: Information Security Incident Management		PR.IP	DE.AE	RS.RP	RC.RP
ISPO-A17: Information Security Aspects of Business Continuity Management	ID.BE	PR.IP			
ISO-A18: Compliance with Internal and External Requirements	ID.GV	PR.IP	DE.DP		

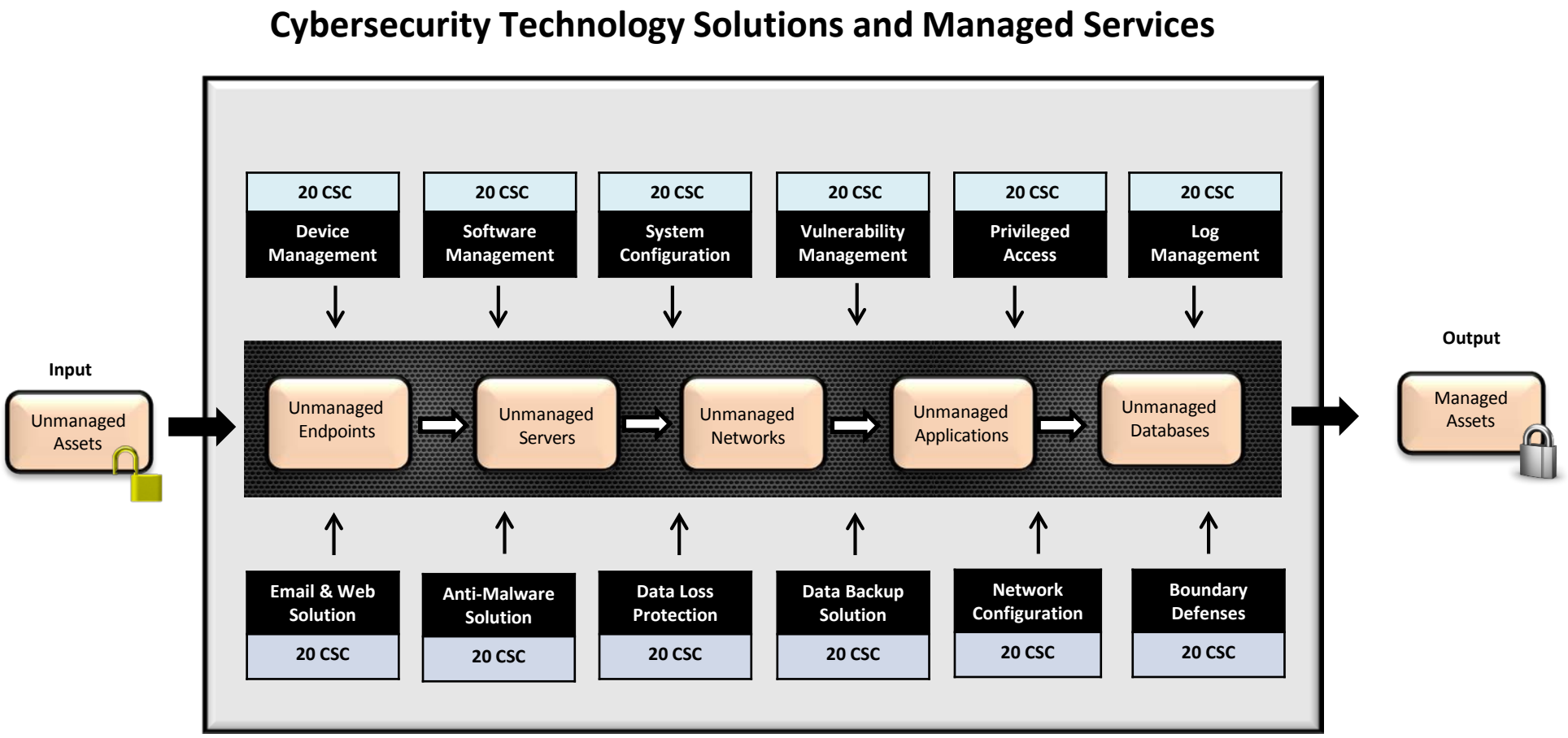
The Technology Program

The Technology System: The 20 Critical Security Controls

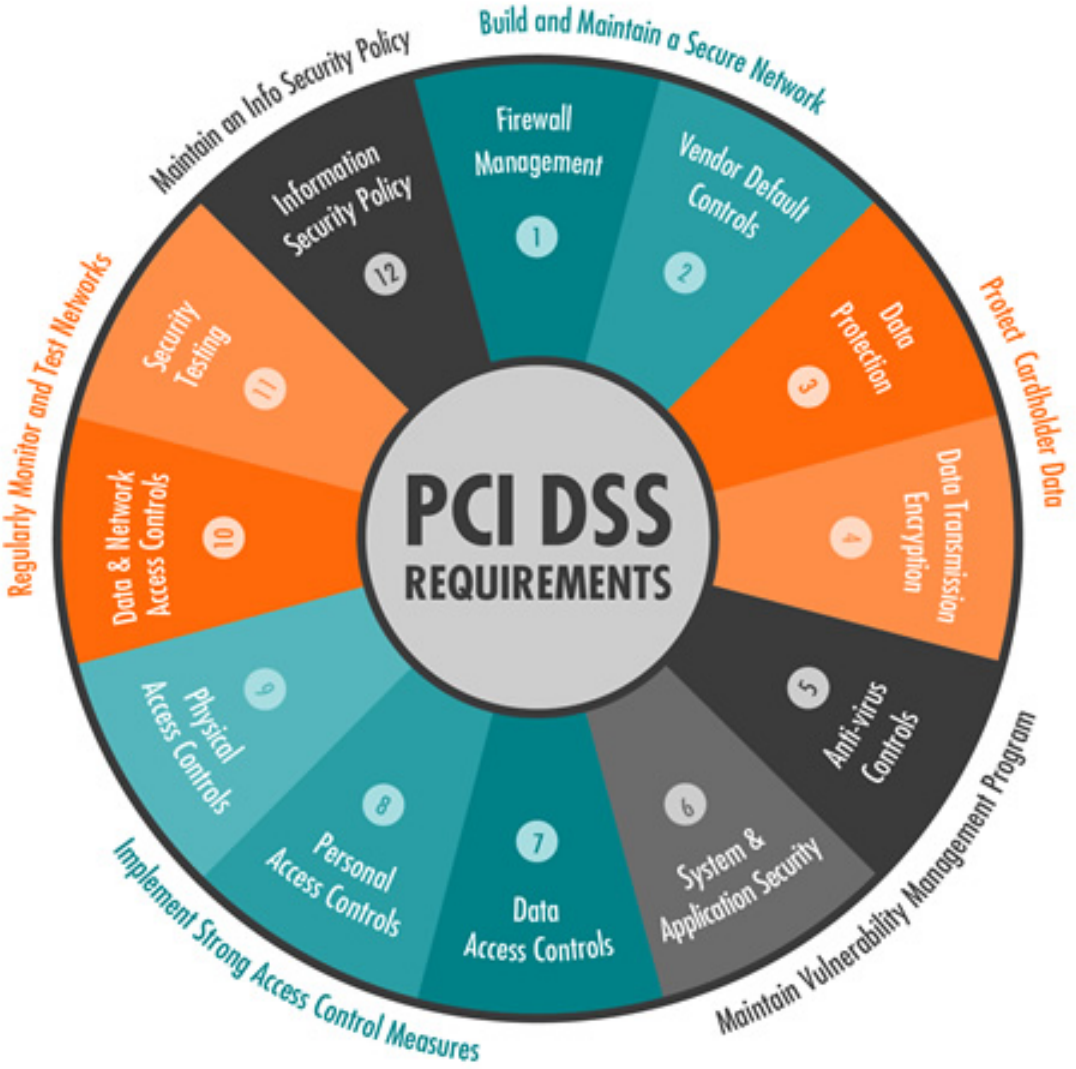


Used with permission from Center for Internet Security (CIS)

Applying the Technical Controls



Technology Testing & Assurance

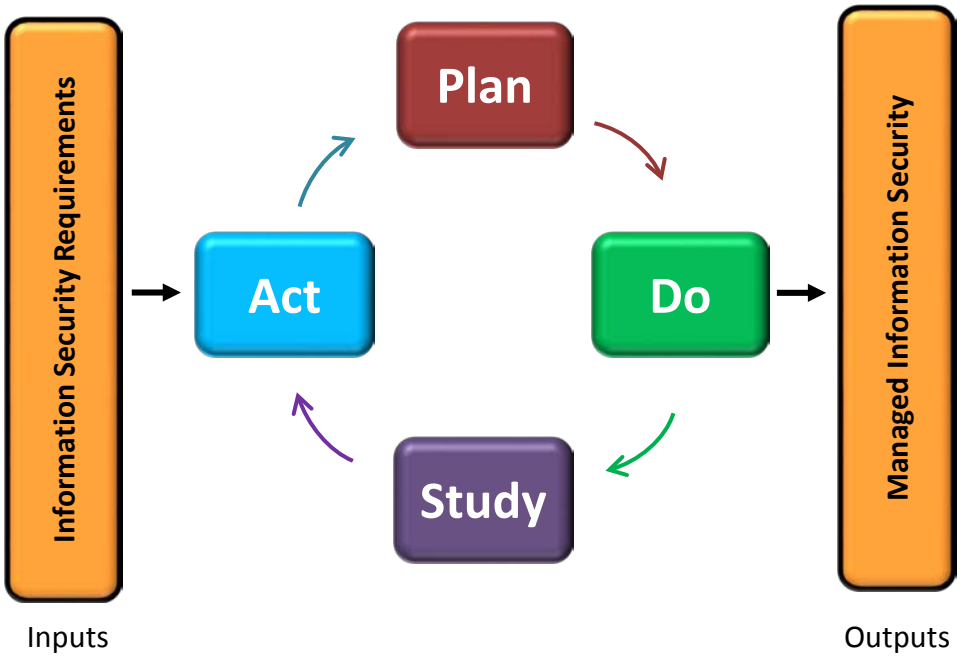


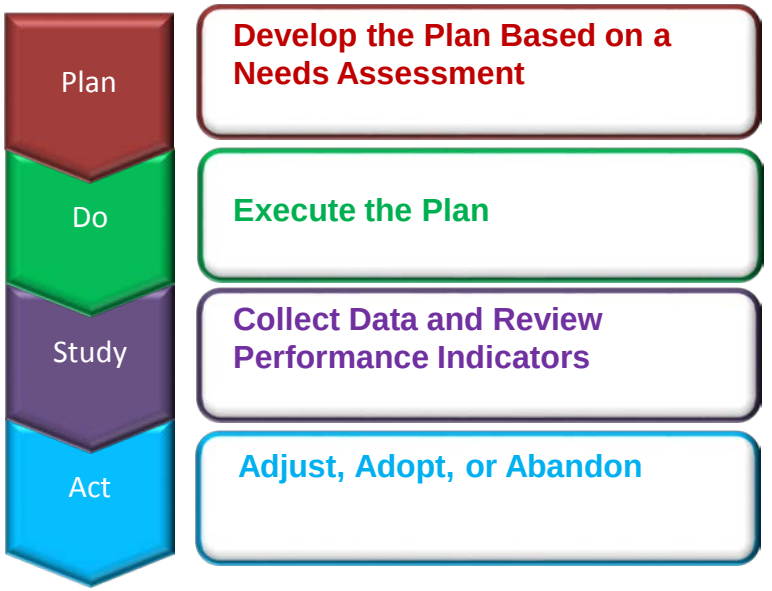
Used with permission from Payment Card Industry Data Security Standard

The Business Program

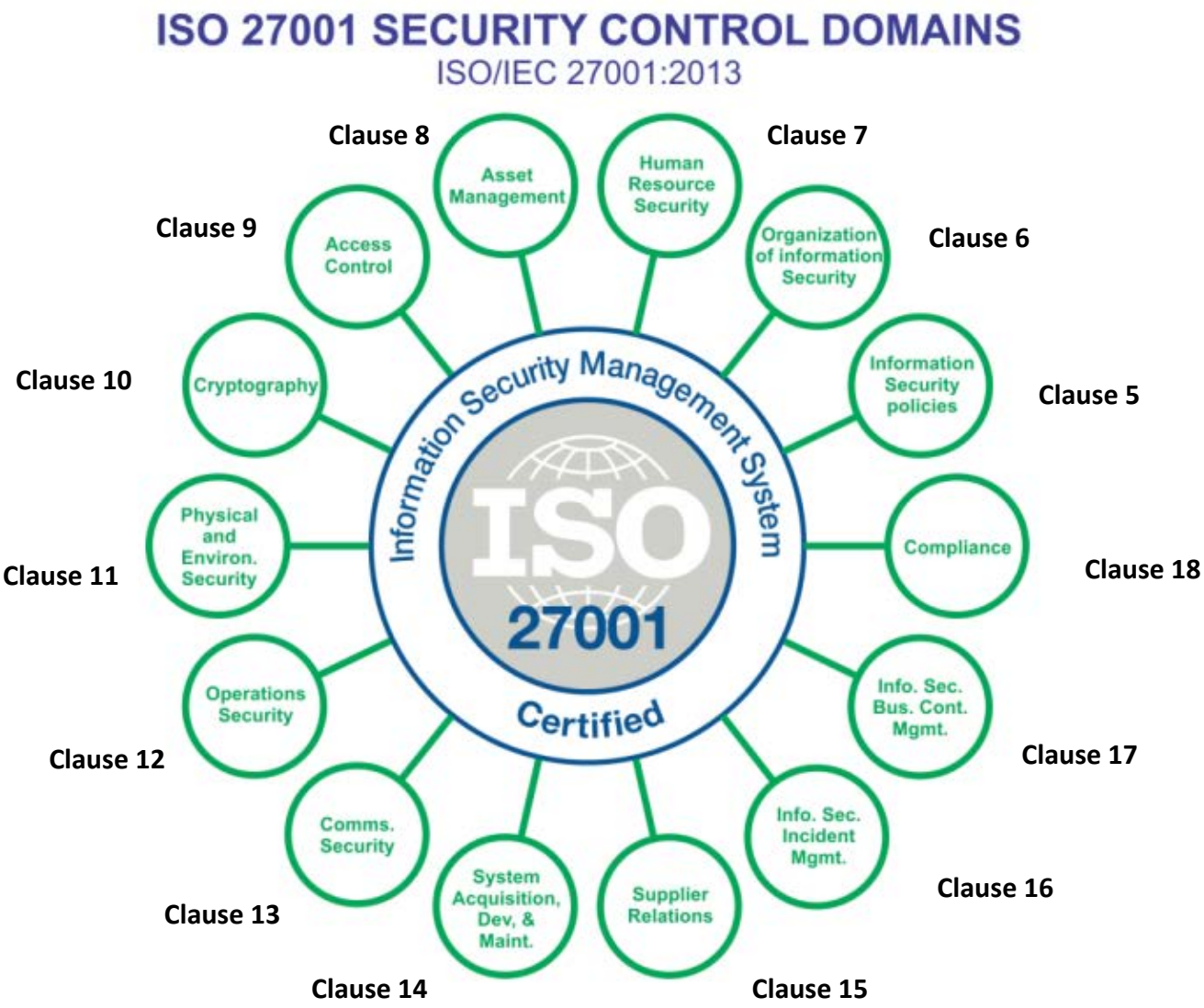
The Business System: ISO 27001

Information Security Management System (ISMS)



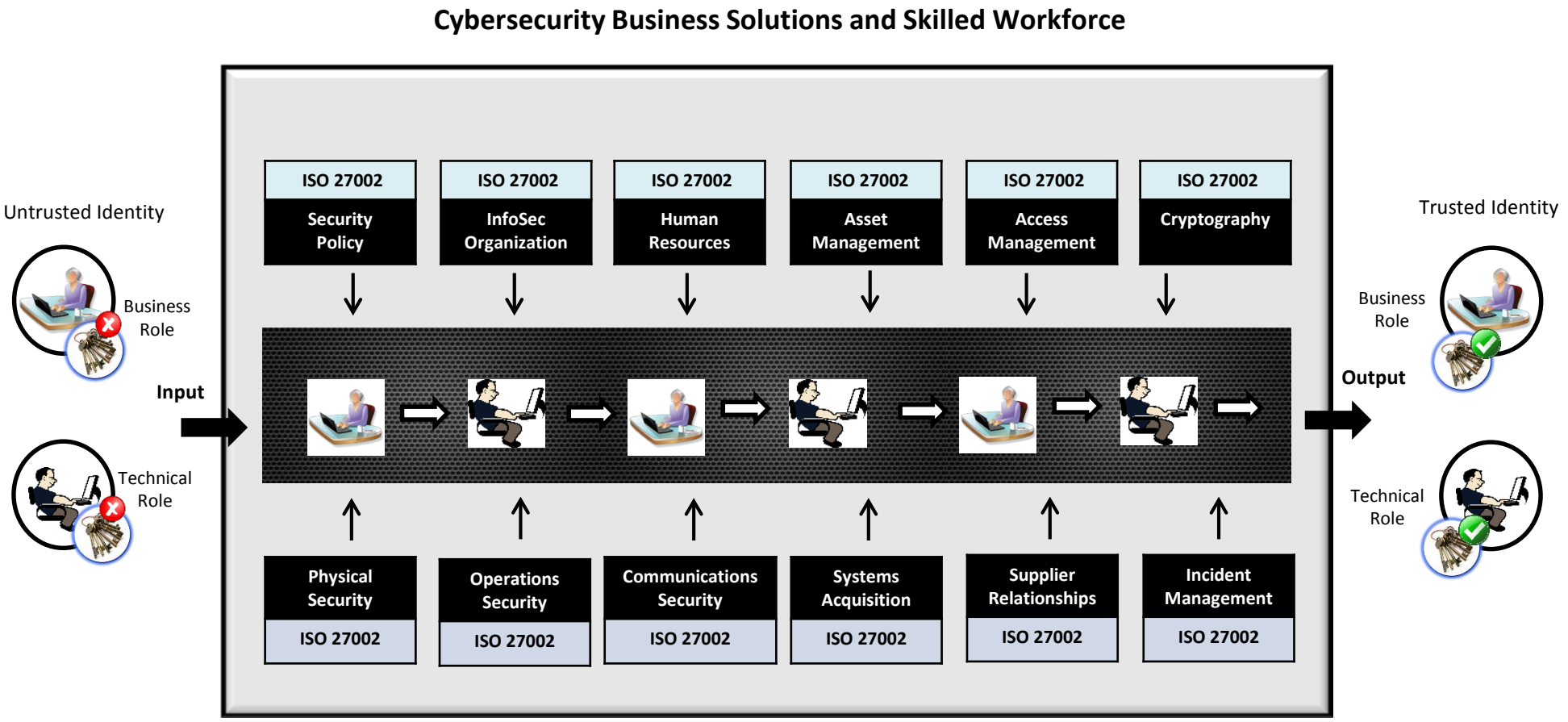


The Business Controls: ISO 27002:2013

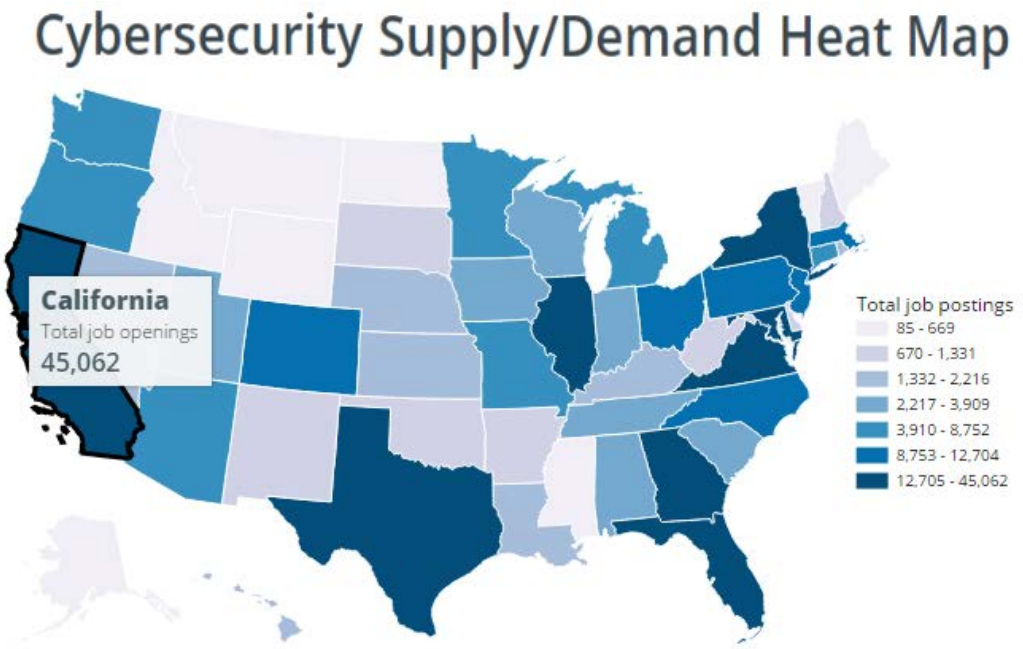


Used with permission of ANSI on behalf of ISO

Applying the Business Controls



Cyber Seek Website



Pennsylvania Job Postings

Cybersecurity Job Openings : 8,874
Employed Cybersecurity Workforce: 23,897

Postings by NCWF Category:

- Securely Provision (SP): 4,332
- Operate and Maintain (OM): 6,096
- Oversee and Govern (OG): 2,572
- Protect and Defend (PR): 2,904
- Analyze (AN): 3,462
- Collect and Operate (CO): 1,334
- Investigate (IN): 575

Certification Holders

- Security+: 4,165
- CIPP: 159
- CISSP: 2,059
- CISA: 1,196
- CISM: 314

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

The NICE Workforce Framework

No.	Workforce Categories	Workforce Category Descriptions
1	Securely Provision (SP)	Conceptualizes, designs, and builds secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.
2	Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
3	Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
4	Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
5	Analyze (AN)	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
6	Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
7	Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

The National Cybersecurity Workforce Framework provides a blueprint to categorize, organize, and describe cybersecurity work into Specialty Areas, tasks, and knowledge, skills, and abilities (KSAs). The Workforce Framework provides a common language to speak about cyber roles and jobs and helps define personal requirements in cybersecurity. The Workforce Framework organizes cybersecurity into seven high-level Categories, each comprised of several Specialty Areas.

AICPA Cybersecurity Risk Management Program (DRAFT)

The American Institute of CPAs (AICPA) is working to develop a voluntary, market-based solution to evaluating cybersecurity risk management that could enhance public trust in the effectiveness of a company's cybersecurity programs.

Used with permission on ANSI on behalf of ISO

AICPA Cybersecurity Risk Management Program (DRAFT)

- The AICPA is developing a common foundation to assess the effectiveness of an entity's cybersecurity risk management program.

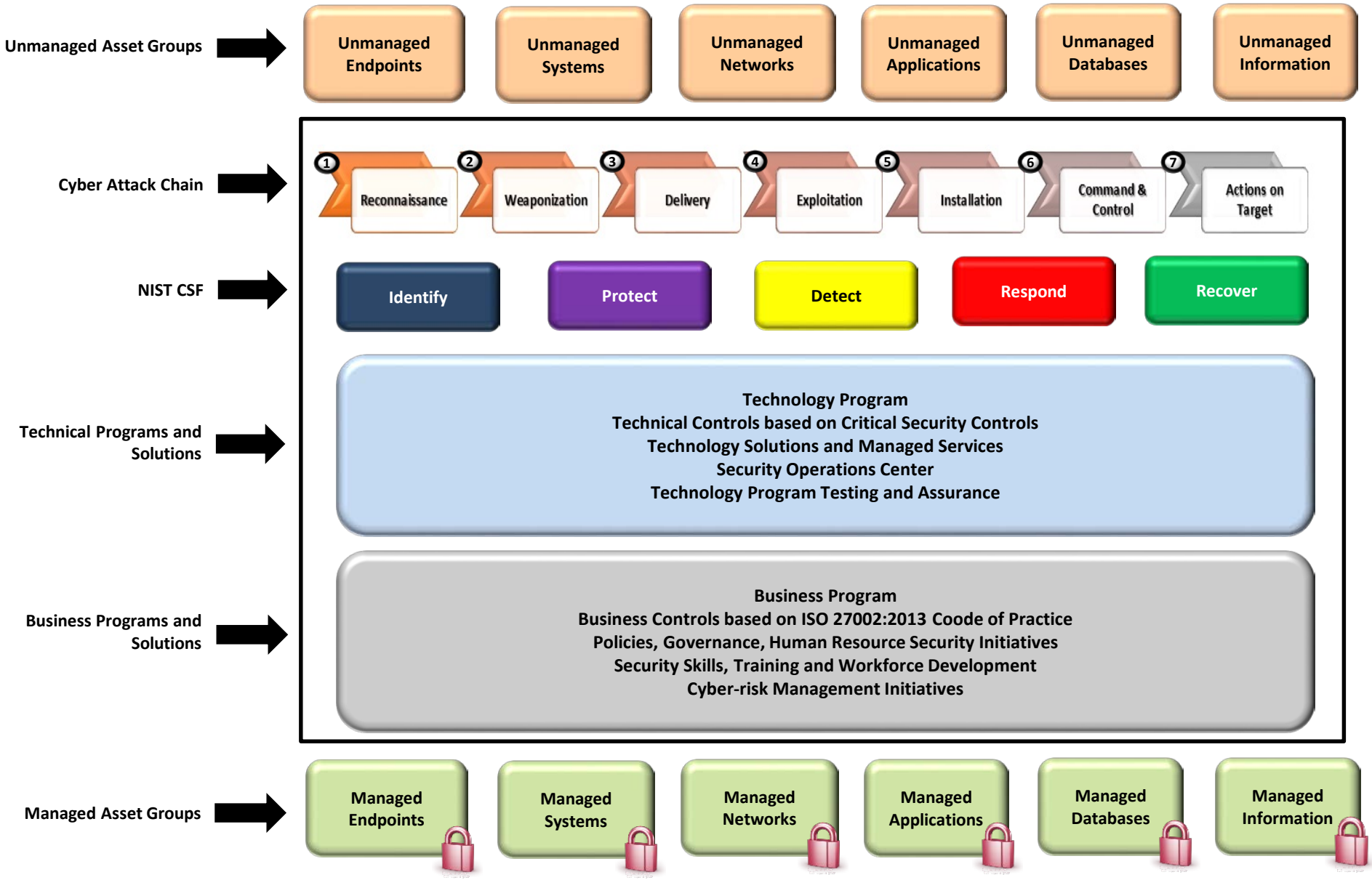
- The primary objective is to propose a reporting framework through which organizations can communicate useful information regarding their cybersecurity risk management programs to stakeholders.

- The development of a common set of criteria will pave the way for the introduction of a new engagement to assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of an entity's cybersecurity risk management program.

- The existence of multiple, disparate frameworks and programs for evaluating security programs and their effectiveness, as well as different stakeholders' preferences for each, has created a chaotic environment that only increases the burden on organizations trying to communicate how they design, implement and maintain an effective cybersecurity risk management program.

- The AICPA's cybersecurity engagement will be a consistent, market-driven approach to examine and report on an entity's cybersecurity measures that addresses the information needs of a broad range of users.

Lesson 2: The Controls Factory Model



Questions?