NEW YORK METRO JOINT CYBER SECURITY CONFERENCE

Center for Internet Security Controls v8

Tom Brennan

#516 #212 #973 Region

- ✓ 34 Years of Technology Risk Management (TRM)
- ✓ Speaker and Advisory Council SecureWorld, NYU,NJIT, CCM, The RIG
- ✓ Board Member, CEO, CIO, Global Director, Regional Director, Technical Product Manager, Penetration Tester, Investigator, Incident Commander, LAN/WAN Administrator, United States Marine
- ✓ Builder of “Widgets”
- ✓ Breaker of Important Systems
- ✓ Defender Important Assets
- ✓ DHS/CISA Information and Communication Technology Risks
- ✓ MITRE System of Trust
- ✓ Nonprofit Cyber

DEPARTMENT OF THE NAVY · UNITED STATES MARINE CORPS

PALL Pall Corporation

DATEK

PROACTIVERISK

OWASP

WhiteHat SECURITY

Trustwave SpiderLabs

intel

SAFECode Software Assurance Forum for Excellence in Code Driving Security and Integrity

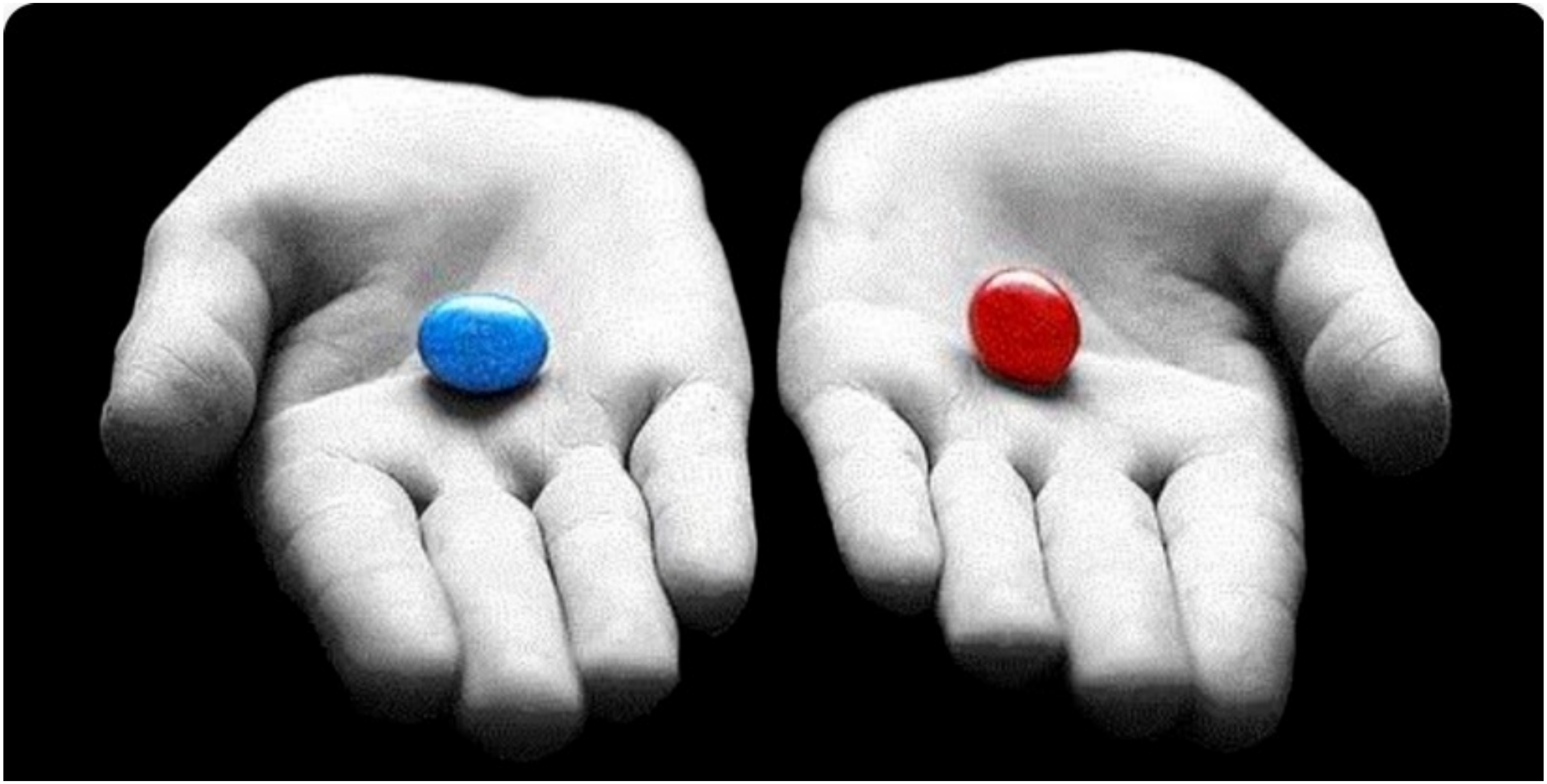
Nonprofit Cyber

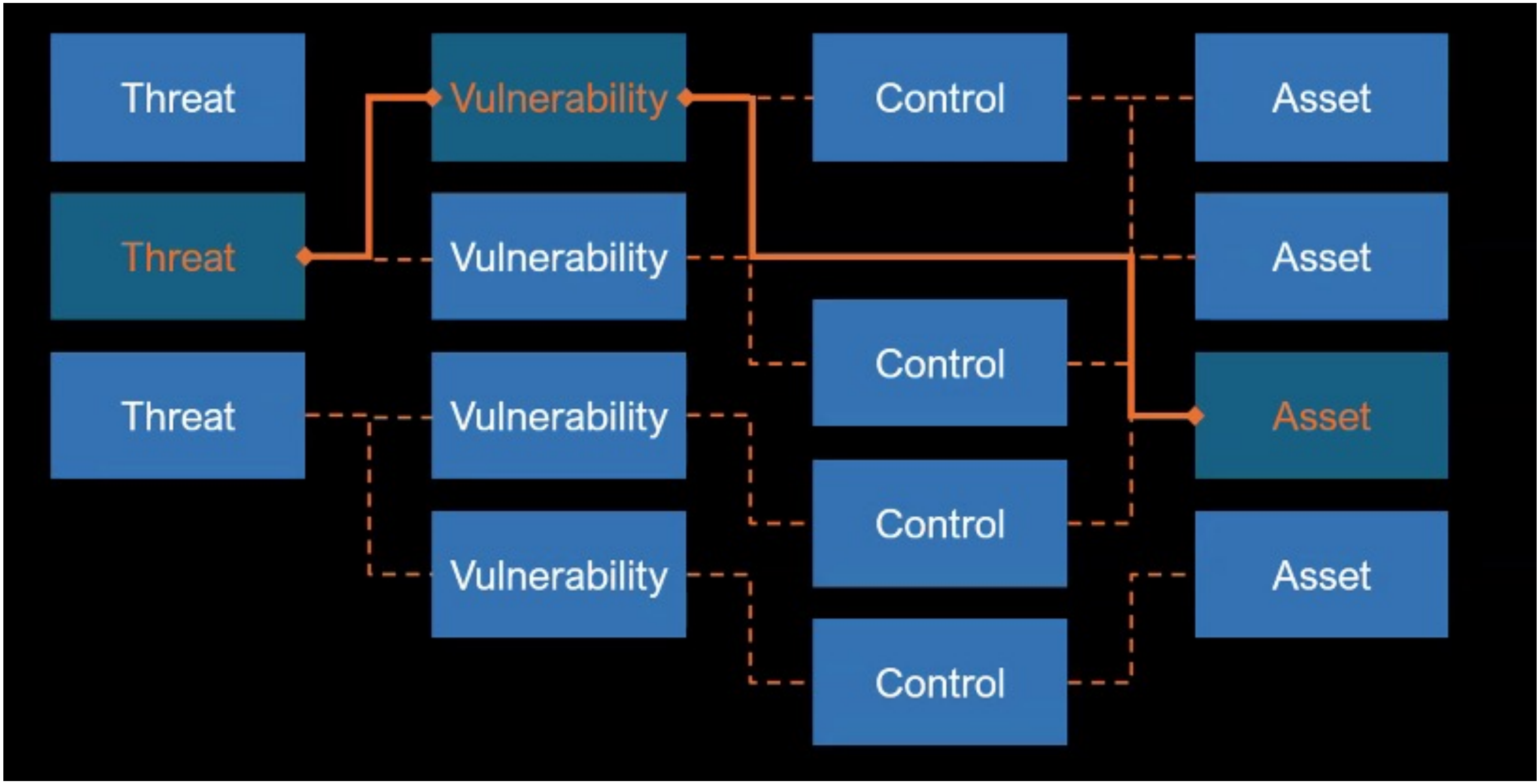
IOActive COMPREHENSIVE INFORMATION SECURITY SERVICES

CREST

MANDELBAUM BARRETT

ADP

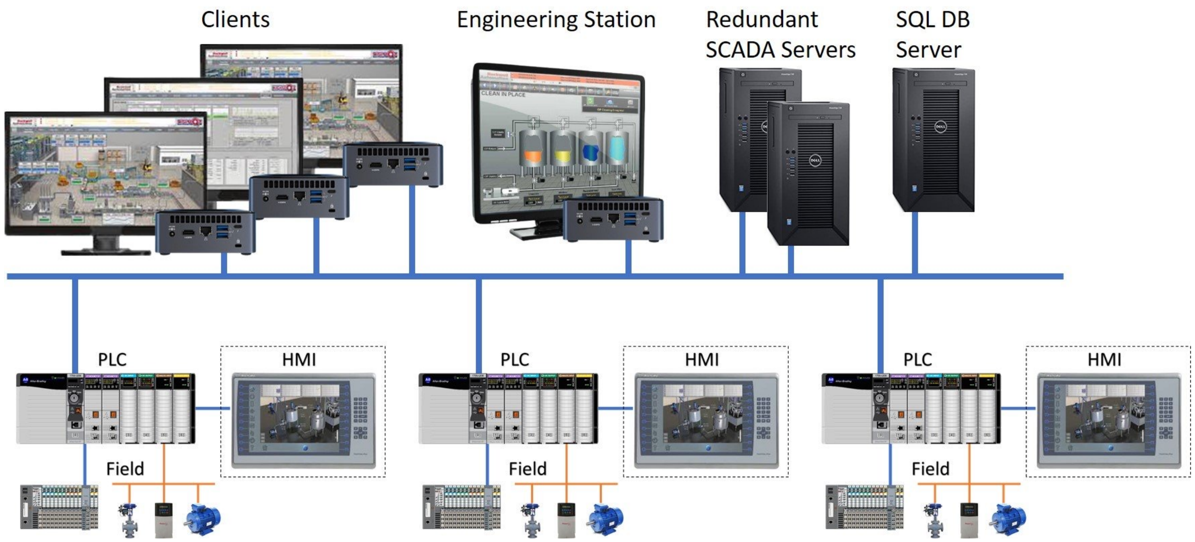




Threat
Threat
Threat
Vulnerability
Vulnerability
Vulnerability
Vulnerability
Control
Control
Control
Control
Asset
Asset
Asset
Asset

Cyber Attacks

Supervisory Control and Data Acquisition (SCADA) systems, which monitor and control water and wastewater processes, are vulnerable to cyber attacks. Compromising these systems can lead to significant disruptions in water treatment and distribution.

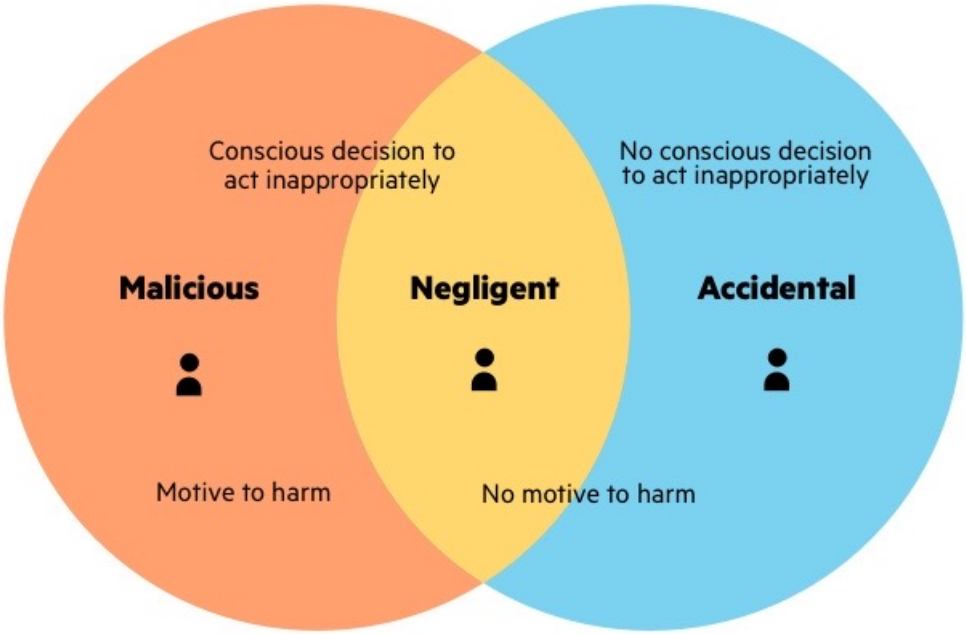


Unauthorized Access:

Lack of proper authentication and authorization mechanisms can allow unauthorized personnel to access critical control systems, potentially leading to intentional or unintentional system failures.

Insider Threats

Employees or contractors with malicious intent or those who inadvertently compromise security can cause significant damage to OT systems, including data breaches and operational disruptions.



Conscious decision to act inappropriately

No conscious decision to act inappropriately

Malicious

Negligent

Accidental

Motive to harm

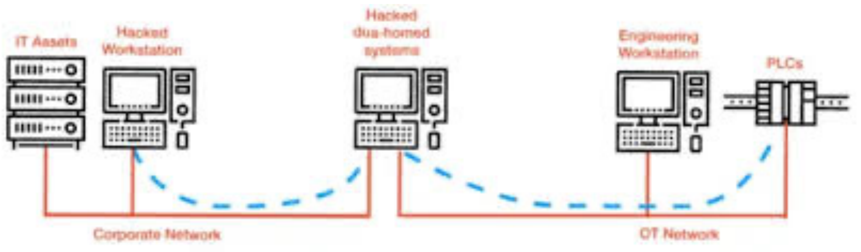
No motive to harm

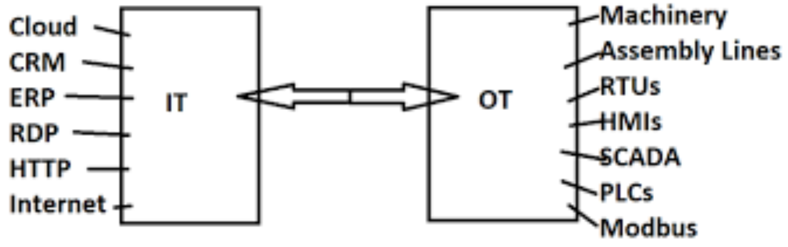
Outdated Technology

Many water and wastewater facilities use outdated control systems and software that are no longer supported or updated, making them vulnerable to known exploits and vulnerabilities.

Lack of Network Segmentation

Poorly segmented networks can allow attackers to move laterally within the OT environment once they gain initial access, increasing the potential impact of a breach.





Cloud
CRM
ERP
RDP
HTTP
Internet

IT

OT

Machinery
Assembly Lines
RTUs
HMIs
SCADA
PLCs
Modbus

Inadequate Monitoring and Incident Response

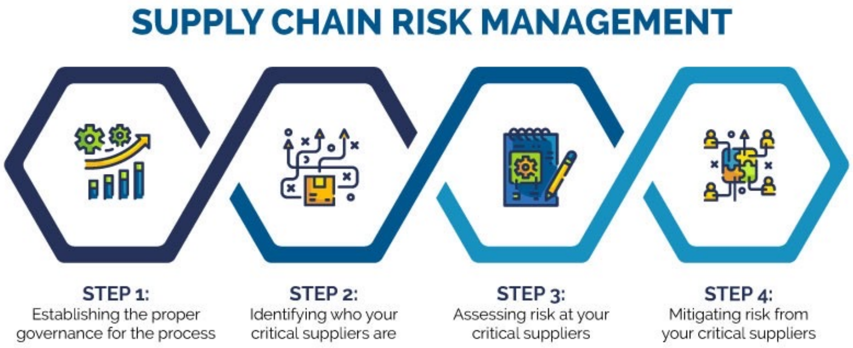
- Without effective monitoring and incident response capabilities, detecting and responding to cyber threats in real-time is challenging, leading to prolonged downtime and potential safety hazards.

Physical Security Breaches

Supervisory Control and Data Acquisition (SCADA) systems, which monitor and control water and wastewater processes, are vulnerable to cyber attacks. Compromising these systems can lead to significant disruptions in water treatment and distribution.

Supply Chain Risks

Vulnerabilities in the supply chain, such as compromised hardware or software components, can introduce backdoors or other security weaknesses into the OT environment.



SUPPLY CHAIN RISK MANAGEMENT

STEP 1: Establishing the proper governance for the process

STEP 2: Identifying who your critical suppliers are

STEP 3: Assessing risk at your critical suppliers

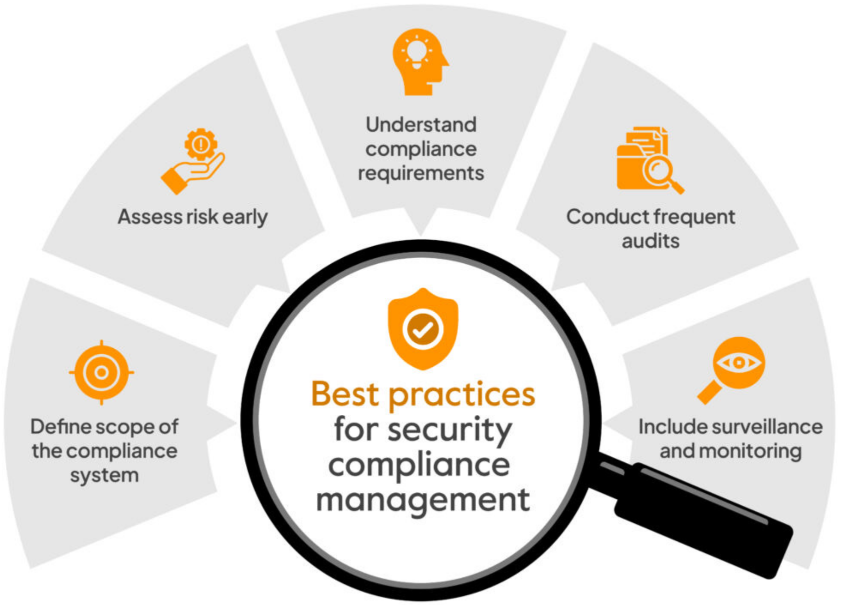
STEP 4: Mitigating risk from your critical suppliers

Human Error

Misconfigurations, poor maintenance practices, and inadequate training can lead to accidental security breaches and operational failures.

Lack of Security Standards and Compliance

Inconsistent application of security standards and regulatory compliance across different facilities can result in varying levels of protection, leaving some systems more vulnerable than others.



Understand compliance requirements

Assess risk early

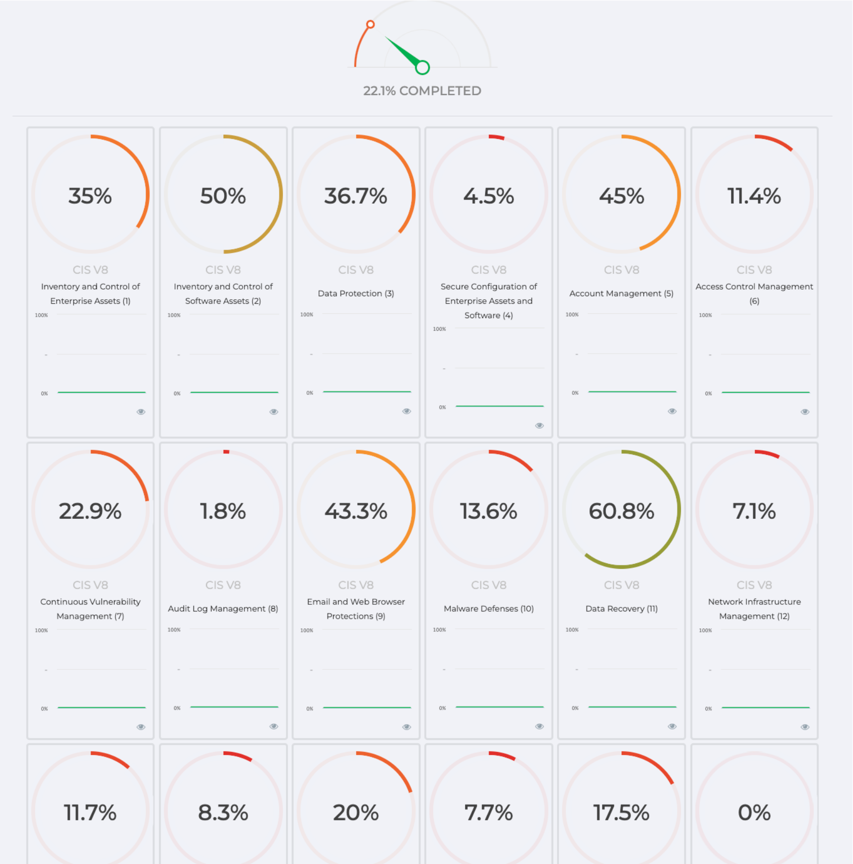
Conduct frequent audits

Define scope of the compliance system

Best practices for security compliance management

Include surveillance and monitoring

easy



22.1% COMPLETED

35% CIS V8 Inventory and Control of Enterprise Assets (1)	50% CIS V8 Inventory and Control of Software Assets (2)	36.7% CIS V8 Data Protection (3)	4.5% CIS V8 Secure Configuration of Enterprise Assets and Software (4)	45% CIS V8 Account Management (5)	11.4% CIS V8 Access Control Management (6)
22.9% CIS V8 Continuous Vulnerability Management (7)	1.8% CIS V8 Audit Log Management (8)	43.3% CIS V8 Email and Web Browser Protections (9)	13.6% CIS V8 Malware Defenses (10)	60.8% CIS V8 Data Recovery (11)	7.1% CIS V8 Network Infrastructure Management (12)
11.7%	8.3%	20%	7.7%	17.5%	0%

Maturity Scoring

20% (.5-10) - INITIAL - Ad Hoc, unpredictable, poorly controlled, reactive

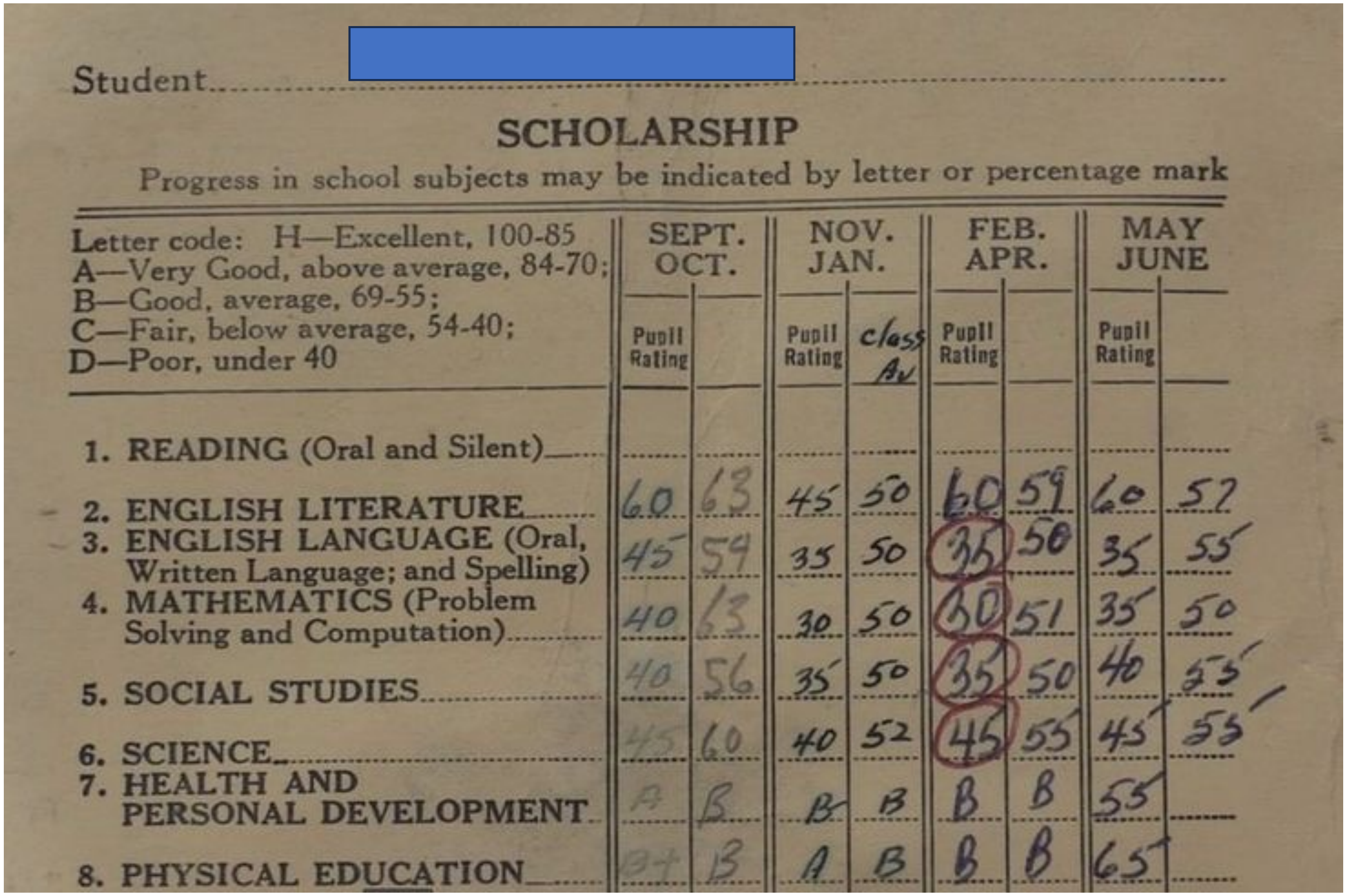
40% (1.5 to 2.5) - REPEATABLE - Basic Process management and repeatable tasks

60% (2.5 to 3.5) - DEFINED - Defined and documented processes, proactive

80% (3.5 to 4.5) - MANAGED - Integrated, measured, and controlled processes

100% (4.5 to 5) - OPTIMIZED - Continued improvement and significant automation

NEW YORK METRO JOINT CYBER SECURITY CONFERENCE



Student [redacted]

SCHOLARSHIP

Progress in school subjects may be indicated by letter or percentage mark

Letter code: H—Excellent, 100-85
A—Very Good, above average, 84-70;
B—Good, average, 69-55;
C—Fair, below average, 54-40;
D—Poor, under 40
	SEPT. OCT.		NOV. JAN.		FEB. APR.		MAY JUNE	

	Pupil Rating		Pupil Rating	class Av	Pupil Rating		Pupil Rating	
1. READING (Oral and Silent)								
2. ENGLISH LITERATURE	60	63	45	50	60	59	60	57
3. ENGLISH LANGUAGE (Oral, Written Language; and Spelling)	45	59	35	50	35	50	35	55
4. MATHEMATICS (Problem Solving and Computation)	40	63	30	50	30	51	35	50
5. SOCIAL STUDIES	40	56	35	50	35	50	40	55
6. SCIENCE	45	60	40	52	45	55	45	55
7. HEALTH AND PERSONAL DEVELOPMENT	A	B	B	B	B	B	55	
8. PHYSICAL EDUCATION	B+	B	A	B	B	B	65	

ADVICE
HELP
SUPPORT
TIPS
ASSISTANCE
GUIDANCE

Center Internet Security – Version 8.0 Controls
https://www.cisecurity.org/controls/v8

Control 1: Inventory and Control of Enterprise Assets

Control 2: Inventory and Control of Software Assets

Control 3: Data Protection

Center Internet Security – Version 8.0 Controls
https://www.cisecurity.org/controls/v8

Control 4: Secure Configuration of Enterprise Assets and Software

Control 5: Account Management

Control 6: Access Control Management

Center Internet Security – Version 8.0 Controls
https://www.cisecurity.org/controls/v8

- **Control 7: Continuous Vulnerability Management**
- **Control 8: Audit Log Management**
- **Control 9: Email and Web Browser Protections**

Center Internet Security – Version 8.0 Controls
https://www.cisecurity.org/controls/v8

- **Control 10: Malware Defenses**
- **Control 11: Data Recovery**
- **Control 12: Network Infrastructure Management**

Center Internet Security – Version 8.0 Controls
https://www.cisecurity.org/controls/v8

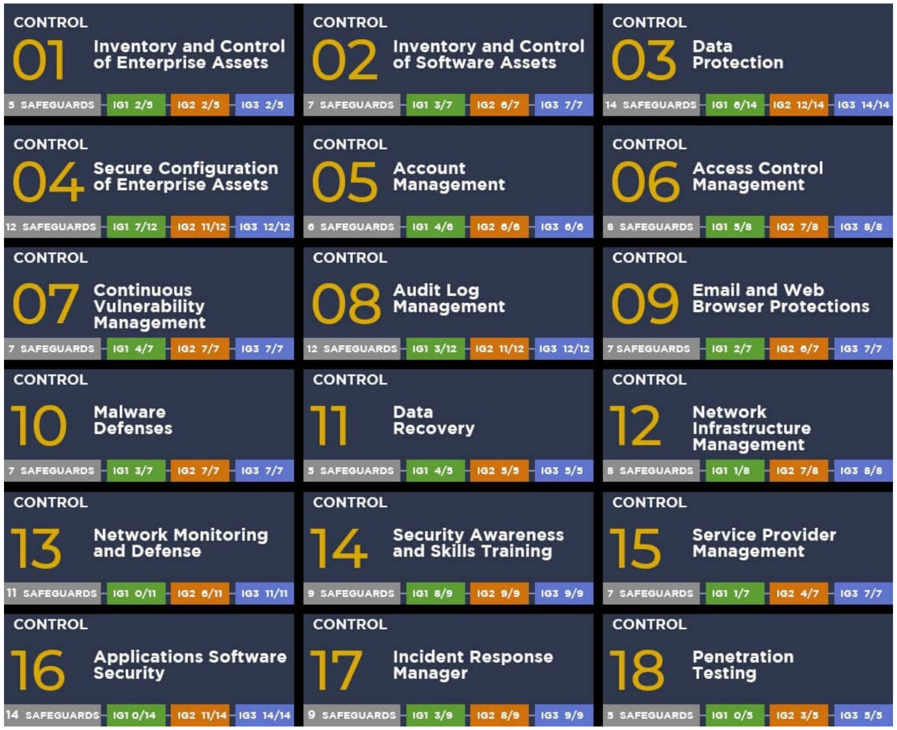
- **Control 13: Network Monitoring and Defense**
- **Control 14: Security Awareness and Skills Training**
- **Control 15: Service Provider Management**

Center Internet Security – Version 8.0 Controls
https://www.cisecurity.org/controls/v8

Control 16: Application Software Security

Control 17: Incident Response Management

Control 18: Penetration Testing



CONTROL 01	Inventory and Control of Enterprise Assets	5 SAFEGUARDS	IG1 2/5	IG2 2/5	IG3 2/5
CONTROL 02	Inventory and Control of Software Assets	7 SAFEGUARDS	IG1 3/7	IG2 6/7	IG3 7/7
CONTROL 03	Data Protection	14 SAFEGUARDS	IG1 6/14	IG2 12/14	IG3 14/14
CONTROL 04	Secure Configuration of Enterprise Assets	12 SAFEGUARDS	IG1 7/12	IG2 11/12	IG3 12/12
CONTROL 05	Account Management	6 SAFEGUARDS	IG1 4/6	IG2 6/6	IG3 6/6
CONTROL 06	Access Control Management	8 SAFEGUARDS	IG1 5/8	IG2 7/8	IG3 8/8
CONTROL 07	Continuous Vulnerability Management	7 SAFEGUARDS	IG1 4/7	IG2 7/7	IG3 7/7
CONTROL 08	Audit Log Management	12 SAFEGUARDS	IG1 3/12	IG2 11/12	IG3 12/12
CONTROL 09	Email and Web Browser Protections	7 SAFEGUARDS	IG1 2/7	IG2 6/7	IG3 7/7
CONTROL 10	Malware Defenses	7 SAFEGUARDS	IG1 3/7	IG2 7/7	IG3 7/7
CONTROL 11	Data Recovery	5 SAFEGUARDS	IG1 4/5	IG2 5/5	IG3 5/5
CONTROL 12	Network Infrastructure Management	8 SAFEGUARDS	IG1 1/8	IG2 7/8	IG3 8/8
CONTROL 13	Network Monitoring and Defense	11 SAFEGUARDS	IG1 0/11	IG2 6/11	IG3 11/11
CONTROL 14	Security Awareness and Skills Training	9 SAFEGUARDS	IG1 8/9	IG2 9/9	IG3 9/9
CONTROL 15	Service Provider Management	7 SAFEGUARDS	IG1 1/7	IG2 4/7	IG3 7/7
CONTROL 16	Applications Software Security	14 SAFEGUARDS	IG1 0/14	IG2 11/14	IG3 14/14
CONTROL 17	Incident Response Manager	9 SAFEGUARDS	IG1 3/9	IG2 8/9	IG3 9/9
CONTROL 18	Penetration Testing	5 SAFEGUARDS	IG1 0/5	IG2 3/5	IG3 5/5

NEW YORK METRO JOINT CYBER SECURITY CONFERENCE

Time is the most valuable thing we have.
There is never enough of it, Thank you for spending yours with me.

@brennantom | tomb@proactiverisk.com