Better Security for Manufacturers in a Month

3 things you can do in the next 30 days to improve security

webit

IMEC
Plan. Implement. Excel.

1

Presenter:

Eric Rieger, Founder/CEO
WEBIT Services

webit

Moderator:

Ken Wunderlich, Technical Specialist
IMEC

IMEC
Plan. Implement. Excel.

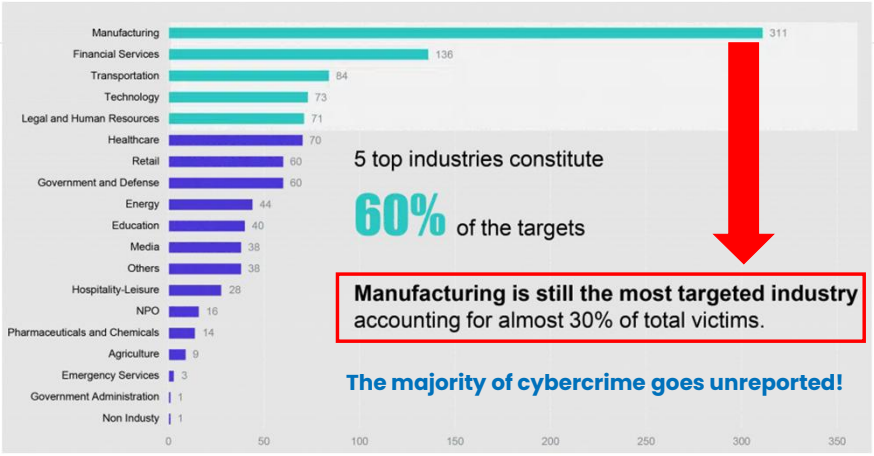
2

Today's Agenda

- **The big problem in Manufacturing**
- **It's happening, locally, far more than you think**
- **Mindset & Approach to better security**
- **What you can do in the next 30 days to take that next step**

3

The Problem: Reported Security Incidents



- Source: https://www.cognyte.com/blog/ransomware_2021/

4

Story Time

A recent, local example of ransomware in manufacturing

5

Is this happening in your company?

6

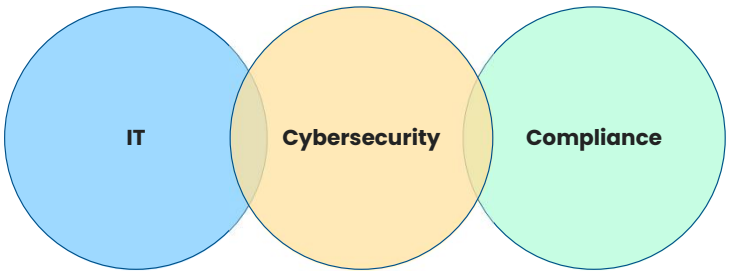
Story Time - Recap

- Not following a recognized framework
- One person wearing 4 hats
- No strategic planning for asset lifecycle mgt.
- Not properly budgeting for risk/need
- Insurance costs will skyrocket or be unobtainable

7

Understanding roles & skill sets

Each role has different skillsets that require specialized training



It is impossible for one person to be proficient in every area, especially if they have other responsibilities in the business or on the shop floor.

8

CIS Center for Internet Security®

Security Framework Options

9

NIST CSF 1.1

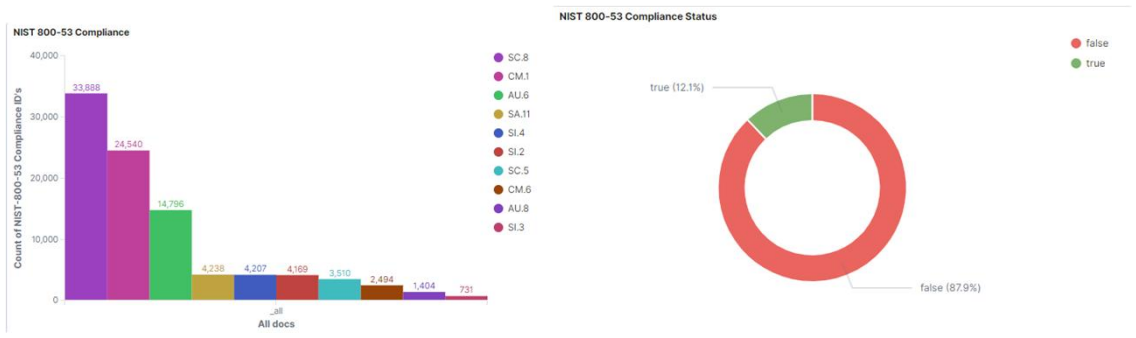
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information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

10

Why this approach works

- **Identify:** You can't properly execute the other core pieces of the framework if you haven't spent time identifying ALL your data/tech.
- **Protect:** Once you've identified everything, creating a **RESILIENT** strategy is possible. This goes far beyond anti-virus and firewalls…
- **Detect:** This is where tools/systems have evolved and it's where most companies are lacking. The average time to detect a breach is currently **200 DAYS!**
- **Respond:** Having a response plan **BEFORE** a crisis is critical to avoid panic, mistakes and increased **LIABILITY**.
- **Recover:** A proper recovery plan includes ensuring key systems and data have solid backup and continuity systems that are tested frequently.

11



Assessing Risk

12

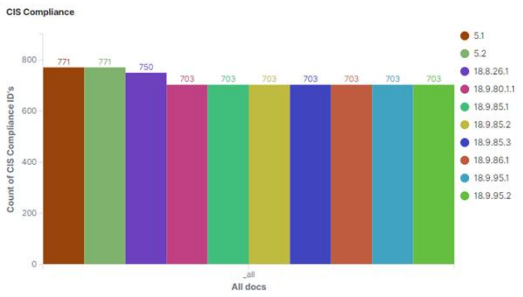
CIS Controls V8

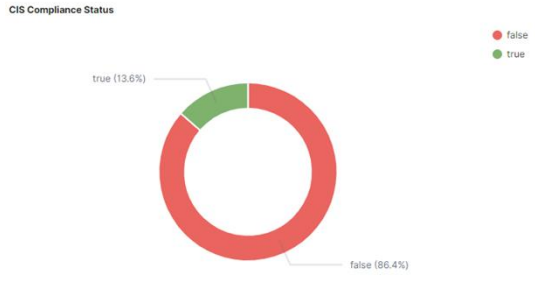
Center for Internet Security®

CIS Controls

01 Inventory and Control of Enterprise Assets	02 Inventory and Control of Software Assets	03 Data Protection	
04 Secure Configuration of Enterprise Assets and Software	05 Account Management	06 Access Control Management	
07 Continuous Vulnerability Management	08 Audit Log Management	09 Email and Web Browser Protections	
10 Malware Defenses	11 Data Recovery	12 Network Infrastructure Management	
13 Network Monitoring and Defense	14 Security Awareness and Skills Training	15 Service Provider Management	
16 Applications Software Security	17 Incident Response Management	18 Penetration Testing	

13





Assessing Risk

14

Cyber Security vs. Cyber Resilience

- ASSET INVENTORY
- BUSINESS CONTINUITY / DATA BACKUPS
- COMPLIANCE SERVICES
- COMPUTER ACCESS CONTROL/ADMIN ACCESS RESTRICTIONS
- CYBERLIABILITY INSURANCE
- DARK WEB RESEARCH
- DATA LOSS PREVENTION (DLP)
- DISK ENCRYPTION/PROTECTION
- EMAIL ENCRYPTION/SPAM FILTERING
- EMAIL SECURITY (GATEWAY, MONITORING, MANAGEMENT, ETC)
- ENDPOINT DETECTION & RESPONSE (EDR) OR ADVANCED END POINT PROTECTION (EPP)
- FIREWALL - MANAGED
- INCIDENT RESPONSE/FORENSICS
- INTERNET ACCESS CONSTRAINTS/DNS FILTERING/WEB CONTENT FILTERING
- INTRUSION DETECTION SYSTEM (IDS)
- INTRUSION PREVENTION SYSTEM (IPS)
- LOG COLLECTION/SIEM
- MANAGED DETECTION & RESPONSE (MDR)
- MOBILE DEVICE SECURITY
- MULTI-FACTOR AUTHENTICATION
- NETWORK MANAGEMENT
- PASSWORD PROTECTION/PASSWORD MANAGEMENT/PASSWORD POLICIES
- PATCH MANAGEMENT
- PEN TESTING
- PHISH PREVENTION
- PHISH TESTING
- SECURE REMOTE ACCESS / VPN
- SECURITY ASSESSMENT/PII SCANNING & ENCRYPTION
- SECURITY AWARENESS TRAINING
- SOCAAS/MANAGED SOC
- SSO
- THREAT HUNTING
- USER BEHAVIORAL ANALYTICS
- VENDOR MANAGEMENT & VENDOR SELECTION FOR ALL 3RD PARTY SECURITY VENDORS
- VIRTUAL CISO
- VULNERABILITY SCANS/VULNERABILITY MANAGEMENT/RISK ASSESSMENT
- WEB WHITELISTING
- ZERO TRUST ARCHITECTURE

15

3 things – 30 days – better security

1) Conduct a security risk assessment
(information is power)

Use a recognized security framework as your guide

- https://www.nist.gov/cyberframework
- https://www.cisecurity.org/controls/v8/

16

3 things – 30 days – better security

2) Enable Multi-Factor Authentication (2FA/MFA) everywhere you can! Especially your email.

https://www.microsoft.com/en-us/security/mobile-authenticator-app

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en_US&gl=US

https://authy.com/

https://duo.com/product/multi-factor-authentication-mfa

17

3 things – 30 days – better security

3) Implement a structured security awareness training program

Everyone participates!

Results are reviewed on a regular, consistent basis

Goals are set and measured

https://www.sans.org/security-awareness-training/

https://learnsecurity.amazon.com/

18

Resources

No need to run your marathon alone

- NIST CSF: https://www.nist.gov/cyberframework
- CIS Controls V8: https://www.cisecurity.org/controls/v8/
- State of Cybersecurity 2020: https://www.webitservices.com/state-of-security-2021/

19

Q & A

20

Thank You

IMEC
Plan. Implement. Excel.

www.imec.org

webit℠ 25 years secure

www.webitservices.com
hello@webitservices.com

21