Cybersecurity

Mike Warner, P.E.
VP, Chief Information Security Officer

January 2020

OSHKOSH™

Today's Agenda

Key Security Trends

1. **Security Fundamentals**
   - Included in 80% of recommendations made after a breach (e.g., patch, user account management, server configuration)[1]

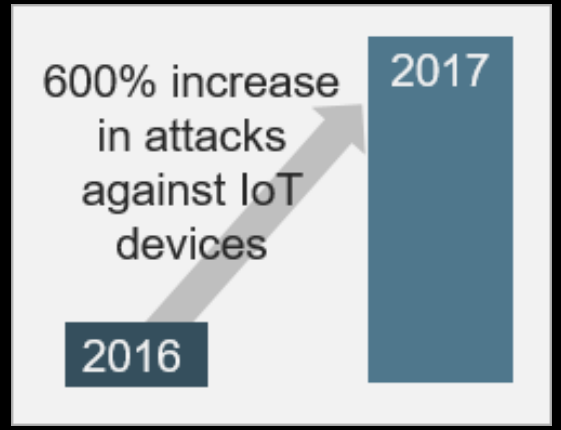
2. **Social Engineering via Email**
   - In manufacturing, 98% of malware is delivered via email[2]
   - 90% of all successful breaches start with phishing emails[2]
   - Social Engineering up 18% over 5 years, most of any threat action[2]

3. **Internet of Things ("IoT")**
   - With 41.6 billion devices by 2025, expanding target attracts criminals[4]
   - IoT devices average 5,200 attacks per month[3]

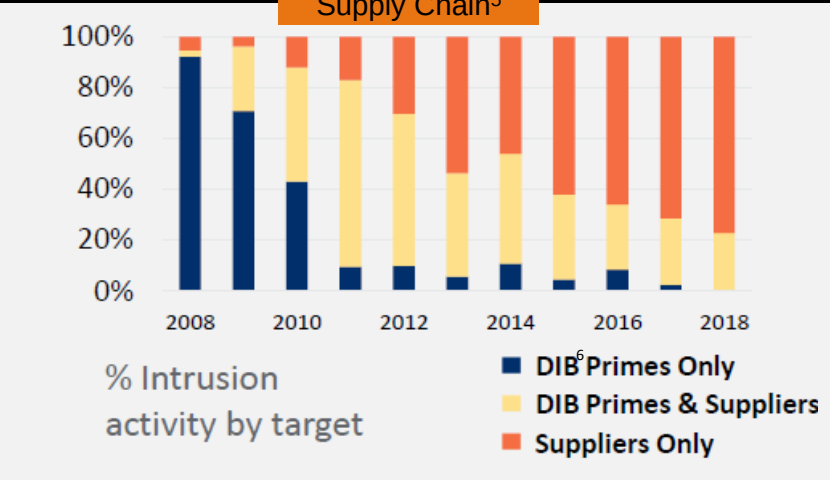
4. **Supply Chain**
   - Attackers find smaller companies outside the Defense Industrial Base ("DIB") an easier path to their target[1,2,3,5]
   - All major 2018 breaches involved tier 1 and 2 suppliers[5]

5. **Contractual / Regulatory**
   - Introduction of a single standard (Cyber Maturity Model Certification) across all U.S. Department of Defense ("DoD") contracts starting in 2021
   - Security a "go/no-go" requirement
   - Based on the NIST[7] 800-171 controls and may include others

IoT[4]



Supply Chain[5]



1. Secureworks Incident Response Insights Reports 2018 and 2019
2. Verizon Data Breach Incident Report 2019
3. Symantec Internet Security Threat Report 2019
4. McKinsey and IDC
5. ("NDISAC") = National Defense Information Sharing and Analysis Center
6. ("DIB") = Defense Industrial Base
7. ("NIST") = US National Institute of Standards and Technology

Major Attacks and Key Themes

* Estimated scope and cost

When	Organization	Summary	Themes	Scope*	Cost*
2019	Wind River	Vulnerabilities found in widely used software embedded in industrial devices (e.g. industrial control systems, robotics arms, elevators, medical devices)	Internet of Things ("IoT") Cloud Platforms Known Vulnerabilities	2 Billion devices	TBD
2019	Capital One	Misconfigured cloud server allowed insider to steal names, income, credit scores, balances, and payment history	Insider Threat Cloud Platforms Misconfigured Systems	106 Million individuals	TBD
2018	Marriott	The Marriott acquisition of Starwood included a data breach which started in 2014. Guest credit card and passport data were compromised	Merger & Acquisition	500 Million individuals	$1 Billion
2017	Equifax	Entry gained through vulnerability in a web portal	Unpatched Applications Known Vulnerabilities	148 Million individuals	$1.4 Billion
2016	Target	A phishing email succeeded at a small refrigeration maintenance supplier; hackers pivoted into Target's cashier systems	Supply Chain Social Engineering by Email	110 Million individuals	$300 million

"

Attackers are a profit center. Defenders are on a budget and often seen as a cost center vs. a strategic enabler.

- Cyber crime would have the 13th highest GDP[1] in the world if it was a country[2]
- Cyber criminals reinvest 20% of their profits into new forms of attack[2]

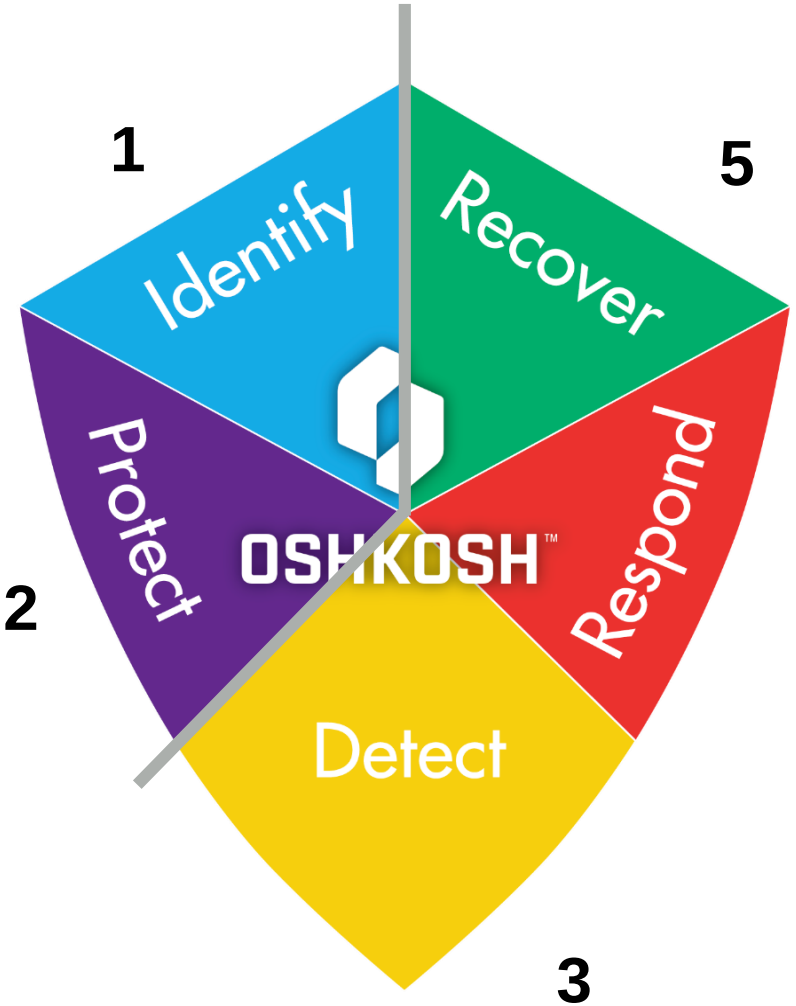
1. ("GDP") = Gross Domestic Product
2. *Into the Web of Profit.* Dr. Michael McGuire. University of Surrey. UK. 2017

Threat Landscape: The Enemy for Manufacturing

	Manufacturing	All Industries
How	**86% Targeted Attacks** ▪ 42% Malware ▪ 37% Social Engineering (e.g. Phishing) ▪ 17% Hacking	Opportunistic attacks most common ▪ 30% Malware ▪ 17% Social Engineering ▪ 48% Hacking
Who	**89% External** ▪ 53% State-affiliated actors ▪ 35% Organized Crime	73% External ▪ 12% State-affiliated actors ▪ 50% Organized crime
Why	47% Espionage 53% Financial motive	13% Espionage 76% Financial motive
Where	76% of Breaches occur in Applications	Varies
What's Stolen	32% Personal Data 30% Trade Secrets 24% Credentials*	35% Personal Data 7% Secrets 10% Credentials*
*Credentials are used to compromise other data		source: 2018 Verizon Data Breach Investigations Report

Our Approach

First, Defense-in-Depth



Second, Resilience

Our **security posture is driven** by:

- Customer contracts
- Regulations
- Risk Mitigation:
  - External threat landscape
  - OSK evolving threat surface

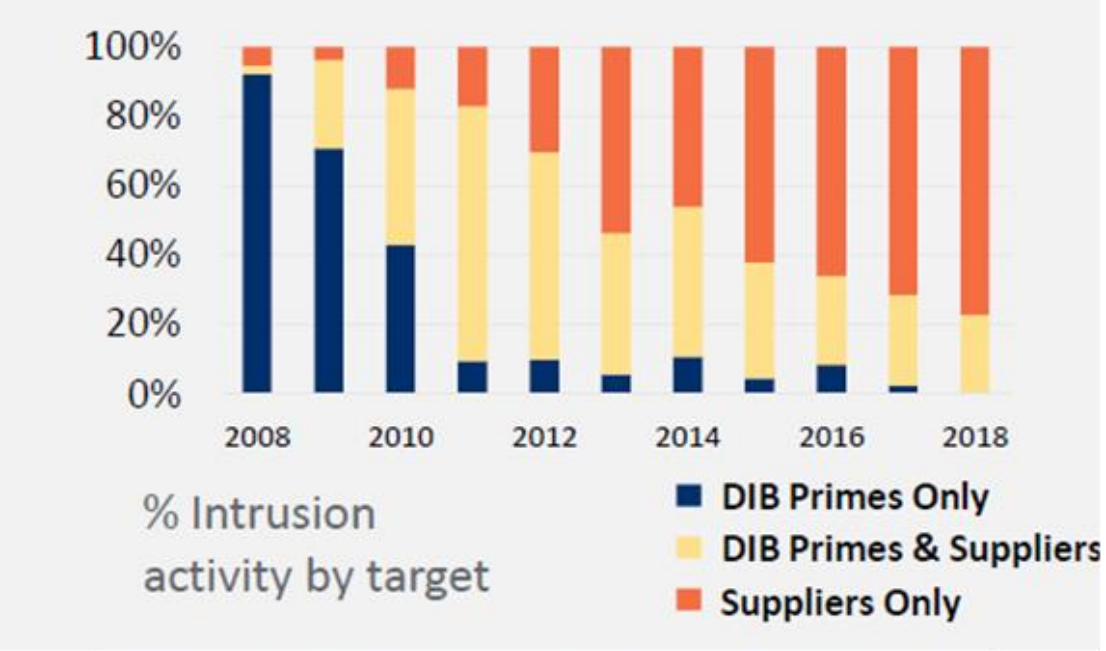
CMMC Background

DoD's Cybersecurity Maturity Model Certification (CMMC) Vision

"Be a unified cybersecurity standard for DoD acquisitions to reduce exfiltration of Controlled Unclassified Information (CUI) from the Defense Industrial Base (DIB)"

CMMC Schedule

- CMMC Rev 1.0 will be released in January 2020
- Will be included in RFIs starting in June 2020
- Will be included in RFPs starting in Fall 2020



Source National Defense Information Sharing and Analysis Center, NDISAC

CMMC Levels

	Description of Practices	Description of Processes
Level 1	• Basic cybersecurity • Achievable for small companies • Subset of universally accepted common practices • Limited resistance against data exfiltration • Limited resilience against malicious actions	• Practices are performed, at least in an ad-hoc matter
Level 2	• Inclusive of universally accepted cyber security best practices • Resilient against unskilled threat actors • Minor resistance against data exfiltration • Minor resilience against malicious actions	• Practices are documented
Level 3	• Coverage of all NIST SP 800-171 rev 1 controls • Additional practices beyond the scope of CUI protection • Resilient against moderately skilled threat actors • Moderate resistance against data exfiltration • Moderate resilience against malicious actions • Comprehensive knowledge of cyber assets	• Processes are maintained and followed
Level 4	• Advanced and sophisticated cybersecurity practices • Resilient against advanced threat actors • Defensive responses approach machine speed • Increased resistance against and detection of data exfiltration • Complete and continuous knowledge of cyber assets	• Processes are periodically reviewed, properly resourced, and improved across the enterprise
Level 5	• Highly advanced cybersecurity practices • Reserved for the most critical systems • Resilient against the most-advanced threat actors • Defensive responses performed at machine speed • Machine performed analytics and defensive actions • Resistant against, and detection of, data exfiltration • Autonomous knowledge of cyber assets	• Continuous improvement across the enterprise

CMMC v0.4 Examples

- Examples of Level 1 Practices
  - FAR requirements
  - Anti-virus
  - Ad hoc incident response*
  - Ad hoc cybersecurity governance*
- Examples of Level 2 Practices
  - Risk management
  - Awareness and training
  - Back-ups & security continuity*
- Examples of Level 3 Practices
  - All NIST SP 800-171 Rev 1 requirements are met
    - Multi-factor authentication
  - Information Security Continuity Plan*
  - Communicate threat information to key stakeholders*

* Example capability not covered by NIST SP 800-171 Rev 1

CMMC v0.4 Examples

- Examples of Level 4 Practices
  - Consideration of supply chain risk
  - Threat hunting
  - Out-of-band administration
  - Use of Data Loss Prevention (DLP) technologies
  - Detonation chambers
  - Inclusion of mobile devices
  - Network segmentation
- Examples of Level 5 Practices
  - Deployment of organizational custom protections
  - Cyber maneuver operations
  - Hardware root of trust for boot
  - Real-time asset tracking
  - 24x7 SOC operation
  - Context aware access control and step-up authentication
  - Device authentication
  - Autonomous initial response actions

CMMC Levels 4 & 5 are targeted toward a small subset of the DIB sector that supports DOD critical programs and technologies

Observations

1) As goes the DoD, so goes the federal government (and the states)
2) If you handle or generate CUI, you will need to be at a Level 3
    - Compliance at Level 3 means you are also compliant at Levels 1 and 2
3) DoD has said it will start including the CMMC requirement in “select” RFPs, phasing it into all RFPs by 2022
    - Eventually, you will not be able to bid on a contract unless you have the stated certification level
    - A 3rd party will certify you, all controls must be met
    - Certification will be good for three years