Cybersecurity for Advanced Manufacturing (CFAM) Joint Working Group

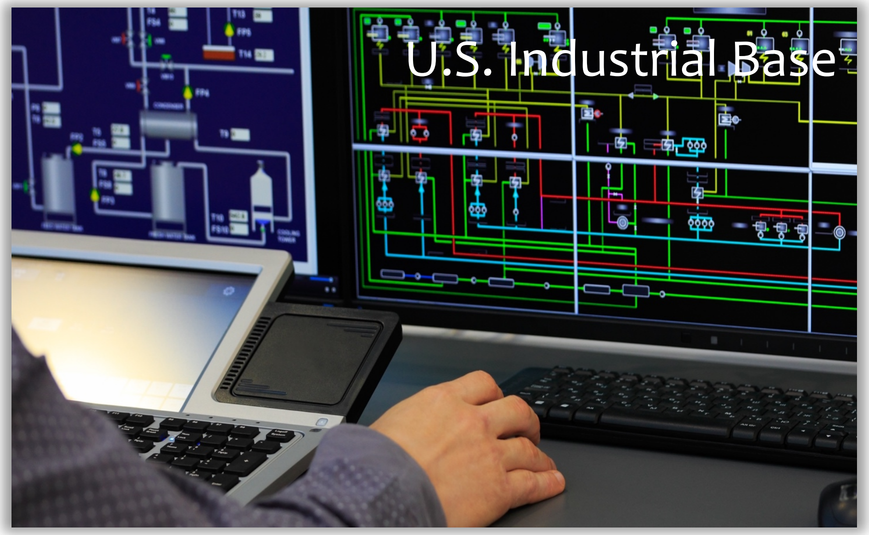
Status Report

NDIA Cyber Division

June 27, 2017

Catherine Ortiz, President
Defined Business Solutions LLC
cjortiz@definedbusiness.com

Today's Talk



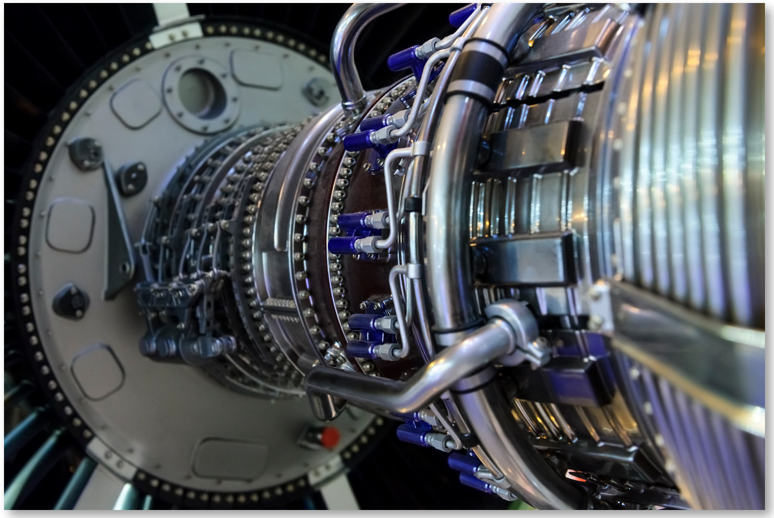
U.S. Industrial Base

Manufacturing Cyber Threats

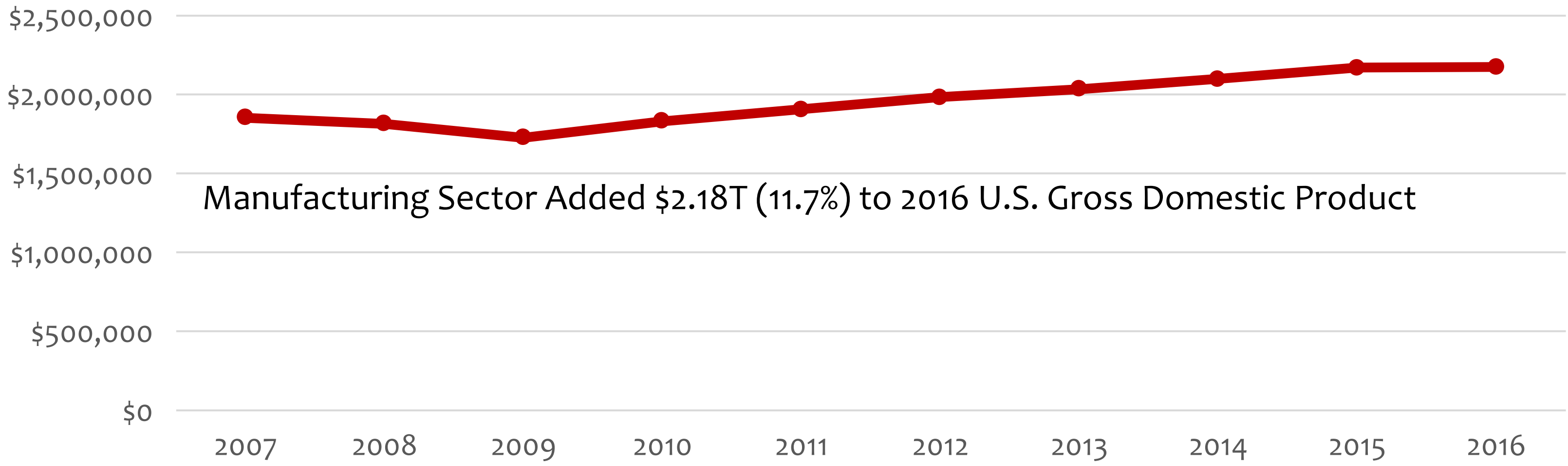
National Defense Implications

Vision for Cybersecurity in Industry 4.0

U.S. Industrial Base: Economic Importance



- Provides more than 12m direct manufacturing jobs, 9% of the U.S. workforce, with an average pay of $26/hour
- Adds nearly $1.5t to U.S. economy through global exports and foreign direct investment in U.S. firms
- Invests more than 75% of the U.S. private industry R&D



Manufacturing Sector Added $2.18T (11.7%) to 2016 U.S. Gross Domestic Product

Sources: National Association of Manufacturers and the U.S. Bureau of Economic Analysis

U.S. Industrial Base: Strategic Deterrence

- The strength of the U.S. Industrial Base has long been a deterrent and a military advantage
- Beyond the defense industrial base, commercial plants, capital equipment, technology innovations, and skilled workforce can be redeployed for national defense if needed

Impact to victory in World War II

"The entry of the United States into the war in late 1941 injected financial, human and industrial resources into Allied operations. The US produced more than its own military forces required and armed itself and its allies for the most industrialized war in history."[1]

According to WWII LTG William S. Knudsen, "We won because we smothered the enemy in an avalanche of production, the like of which he had never seen, nor dreamed possible."[2]

[1] Herman, Arthur. Freedom's Forge: How American Business Produced Victory in World War II, p. IX, Random House, New York, NY, 2012. ISBN 978-1-4000-6964-4.

[2] Parker, Dana T. Building Victory: Aircraft Manufacturing in the Los Angeles Area in World War II, pp. 5, 7, Cypress, CA, 2013. ISBN 978-0-9897906-0-4.

U.S. Industrial Base: Enabling Technology

Manufacturing is an increasingly digital business

Smart Manufacturing

Industrial Internet of Things

Industry 4.0

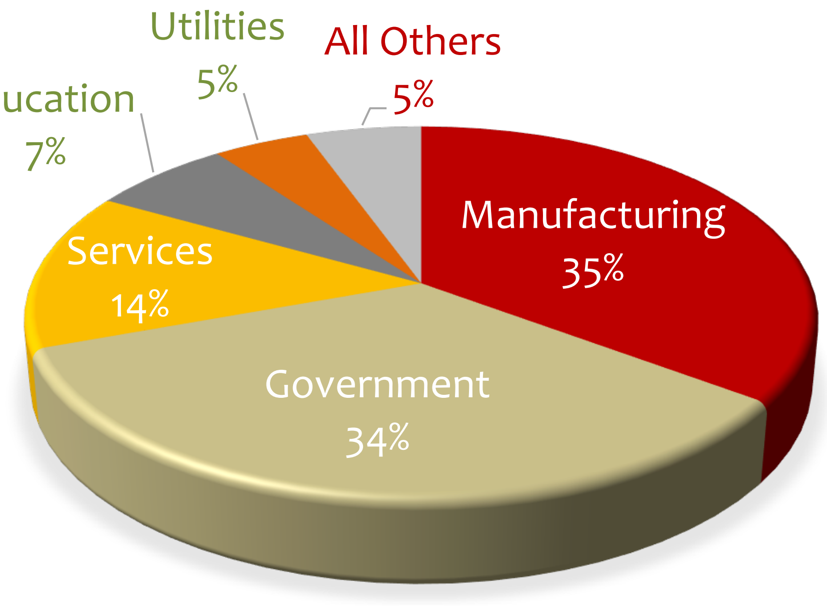
- Networked at every level to gain efficiency, speed, quality and agility
- Constantly learning from models and data throughout the life cycle
- Driven by a "Digital Thread" of product and process information
- Has a "Digital Twin" (models and simulations) used to mirror and predict activities and performance of processes and product

Data demands protection throughout the network and product lifecycle

Cybersecurity: Manufacturing is Under Attack

NDIA

Percent of 2016 Cyber Espionage Incidents, by Industry

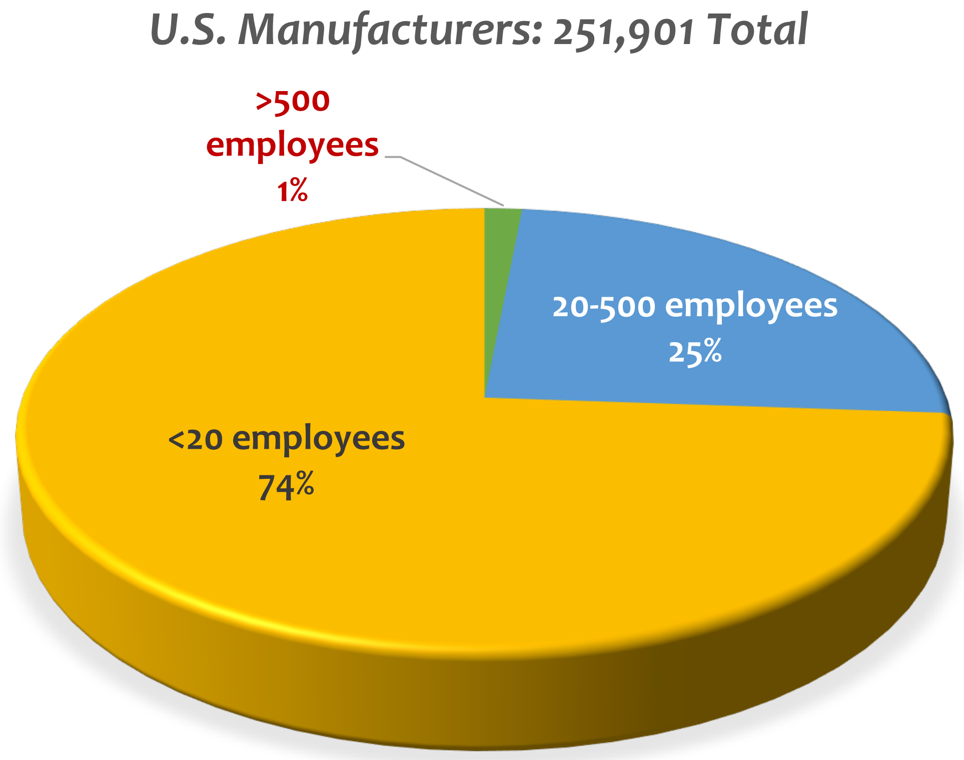


Source: 2017 Verizon Data Breach Investigations Report

- Over half of companies operating industrial control systems (ICS) worldwide suffered between one and five IT security incidents in the last year
- 81% of companies report increased use of wireless connections to the industrial network
- 54% haven't implemented vulnerability scanning and patch management
- Half allow external providers to have access to their industrial control networks

Source: Kaspersky Labs, State of Industrial Cybersecurity 2017 Survey

Cybersecurity: Most Manufacturers are Small & Medium Enterprises (S&MEs)



Source: http://www.nam.org/Newsroom/Facts-About-Manufacturing/20170615

- Often lack cybersecurity knowledge and resources
- Most have no full time cybersecurity staff
- Believe they are not targets, so they focus on perimeter defense for IT network
- Many lack a business case for investing in OT cybersecurity

S&MEs are critical to manufacturing sector and are most vulnerable

Cybersecurity: Insecure Operational Environment

ICS systems are long-lived capital investments (15-20 year life)

"Production mindset" with little tolerance for OT down time

Nascent cybersecurity awareness and limited workforce training

Manufacturing jobs bring executable code into system

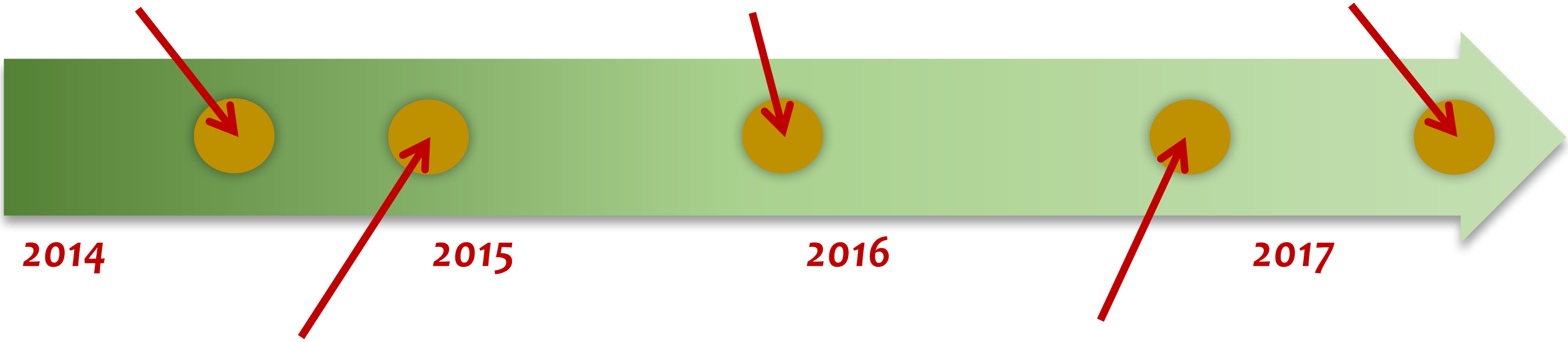
Technical data flowing through the system is highly valued by adversaries

NDIA Cybersecurity Studies Timeline

NDIA Manufacturing and Cyber Divisions recommended actions to improve cybersecurity in defense industrial base manufacturing networks

NDIA-DoD Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG) organized to develop implementation paths for those recommendations

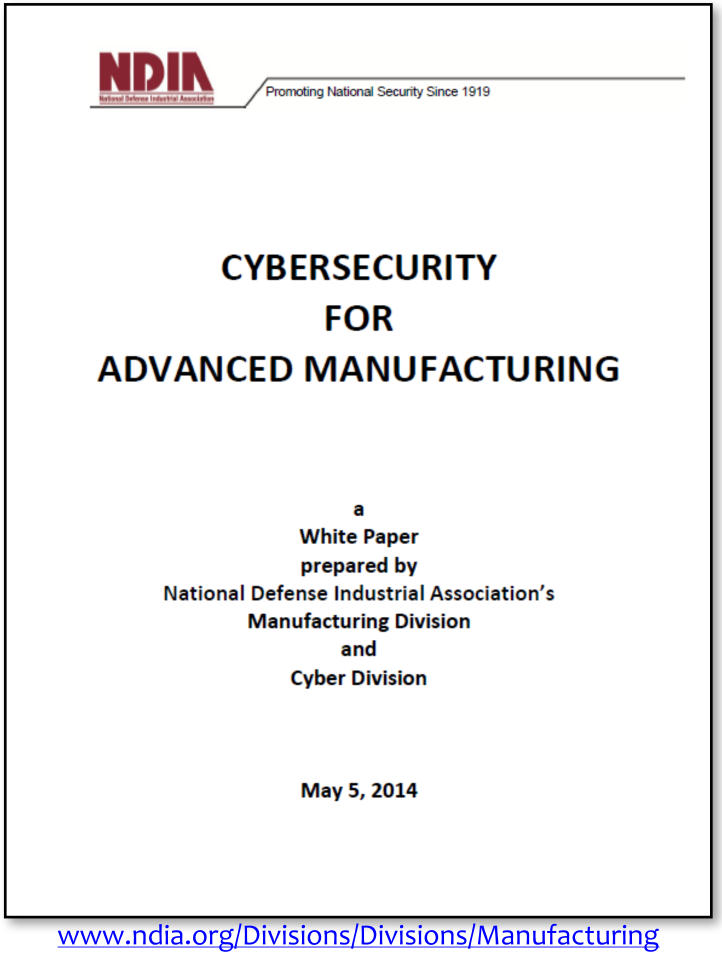
CFAM JWG report, including implementation recommendations *(under development)*



DoD USD Frank Kendall endorses report's findings and asks DASD Kristen Baldwin to direct implementation development

DFARS amended to require defense contractors to implement NIST SP 800-171 controls throughout the organization and supply chain

NDIA White Paper: National Security Implications



NDIA

Promoting National Security Since 1919

CYBERSECURITY
FOR
ADVANCED MANUFACTURING

a
White Paper
prepared by
National Defense Industrial Association's
Manufacturing Division
and
Cyber Division

May 5, 2014

www.ndia.org/Divisions/Divisions/Manufacturing

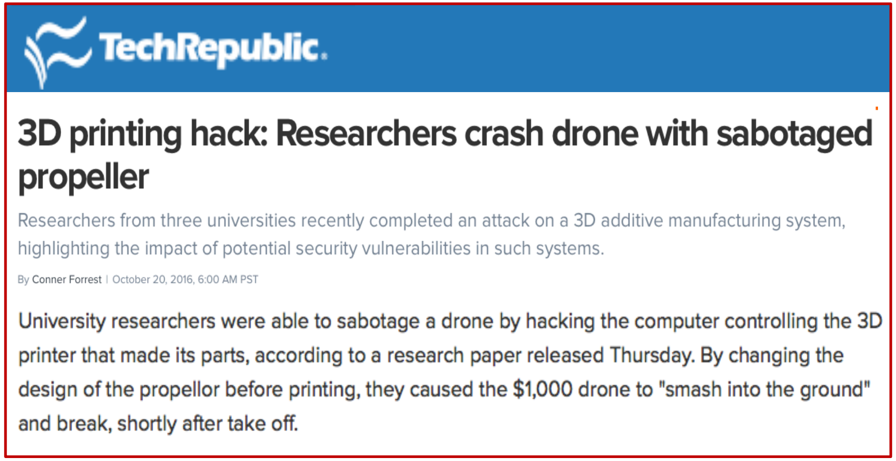
Cyber risks in defense industrial base are national security concerns

Confidentiality	**Theft of technical info** -- can compromise national defense and economic security
Integrity	**Alteration of technical data** -- can alter the part or the process, with physical consequences to mission and safety
Availability	**Disruption or denial of process control** -- can shut down production and impact readiness

The Attack Scenarios Are Real

NDIA

Product tampering



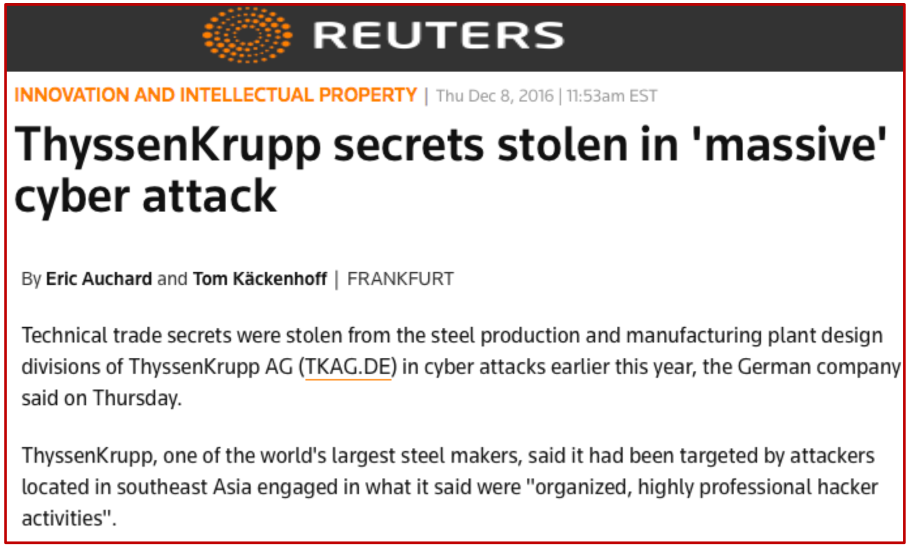
TechRepublic.

3D printing hack: Researchers crash drone with sabotaged propeller

Researchers from three universities recently completed an attack on a 3D additive manufacturing system, highlighting the impact of potential security vulnerabilities in such systems.

By Conner Forrest | October 20, 2016, 6:00 AM PST

University researchers were able to sabotage a drone by hacking the computer controlling the 3D printer that made its parts, according to a research paper released Thursday. By changing the design of the propellor before printing, they caused the $1,000 drone to "smash into the ground" and break, shortly after take off.



REUTERS

INNOVATION AND INTELLECTUAL PROPERTY | Thu Dec 8, 2016 | 11:53am EST

ThyssenKrupp secrets stolen in 'massive' cyber attack

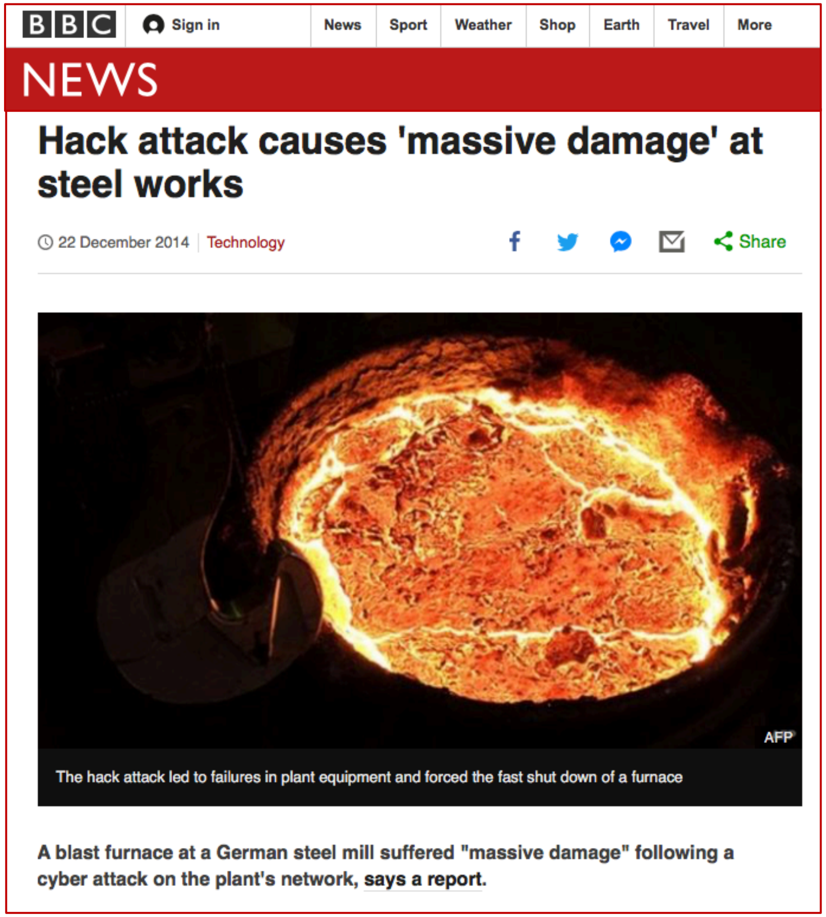
By **Eric Auchard** and **Tom Käckenhoff** | FRANKFURT

Technical trade secrets were stolen from the steel production and manufacturing plant design divisions of ThyssenKrupp AG (TKAG.DE) in cyber attacks earlier this year, the German company said on Thursday.

ThyssenKrupp, one of the world's largest steel makers, said it had been targeted by attackers located in southeast Asia engaged in what it said were "organized, highly professional hacker activities".

Intellectual property theft

Physical damage



Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology

The hack attack led to failures in plant equipment and forced the fast shut down of a furnace

A blast furnace at a German steel mill suffered "massive damage" following a cyber attack on the plant's network, says a report.

Need Solutions Specifically for OT Environment

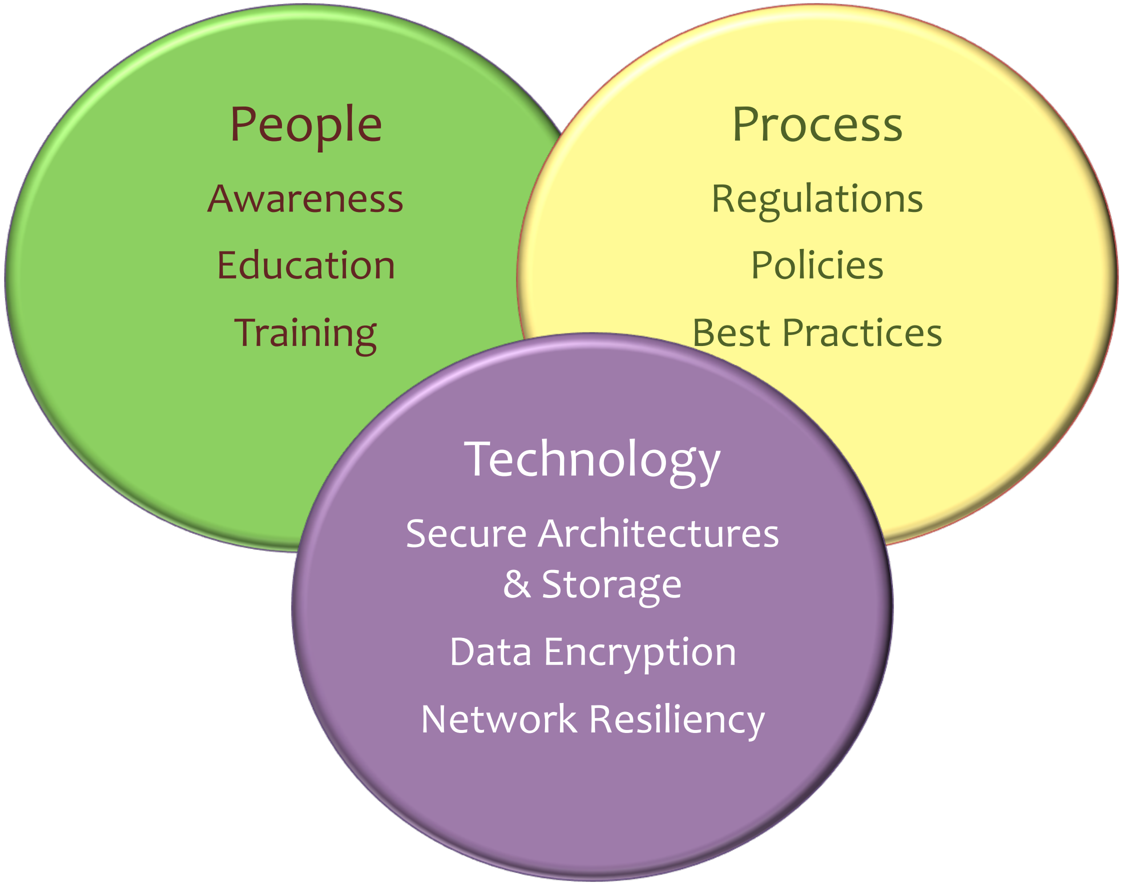
- Training at all organizational levels
- Raising cybersecurity awareness with operators
- Incentives for improving cyber hygiene
- Implementing selected IT best practices
- Increasing interaction with IT network personnel and production engineers
- Including component security features in selection criteria

Shop floor concerns and priorities must be understood and addressed to improve solution adoption

NDIA CFAM JWG Vision – *Not Finalized*

Resilient U.S. industrial base that operates continuously in a cyber-contested environment, responds rapidly to national security needs, and contributes to the nation’s economic development without interruption.

Approach: Understand – Value – Enable



People

Awareness

Education

Training

Process

Regulations

Policies

Best Practices

Technology

Secure Architectures & Storage

Data Encryption

Network Resiliency

Manufacturing Cybersecurity is a Multi-Agency Issue

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
DEPARTMENT OF ENERGY UNITED STATES OF AMERICA
U.S. DEPARTMENT OF HOMELAND SECURITY
DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA
NATIONAL SECURITY COUNCIL UNITED STATES OF AMERICA
SECURITAS
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
DEPARTMENT OF STATE UNITED STATES OF AMERICA
DEPARTMENT OF HEALTH & HUMAN SERVICES USA
THE DEPARTMENT OF THE TREASURY
1789
DEPARTMENT OF LABOR UNITED STATES OF AMERICA
DEPARTMENT OF TRANSPORTATION UNITED STATES OF AMERICA
UNITED STATES DEPARTMENT OF AGRICULTURE
1862
1889

Near-Term Recommendations: DoD Lead

1. Assist S&ME efforts to achieve compliance with DFARS 252.204-7012 to curb the flight of defense suppliers
2. Develop communications plan that includes awareness campaigns, training, and outreach
3. Assess existing and emerging federal government and industry activities that can be leveraged to achieve vision, including existing and emerging policies, standards, and best practices
4. Institute collaboration between Government and Industry to improve manufacturing operational technology security by continuously evaluating emerging technologies and launching research to fill gaps

Aggressive effort to immediately strengthen manufacturing cybersecurity

Longer-Term Recommendations: DoD Lead

Mid-Term:

- Institute a DoD-sponsored program (industrial cybersecurity test range) that offers current and prospective DIB members the ability to assess the cybersecurity of current and emerging design, production and sustainment systems and processes
- Institute a DoD-sponsored program of targeted incentives that will encourage (1) control system vendors to improve the cybersecurity of their offerings to current and prospective defense suppliers and (2) current and prospective defense suppliers to acquire and use the more secure equipment

Long-term:

Create a whole-of-government national consortium to integrate disparate efforts and develop comprehensive solutions to known and emerging defense supply chain cybersecurity issues. This consortium should include representatives from the control systems, manufacturing and cybersecurity industries, the academic and applied research communities, and relevant policy-generating organizations.

Next Steps

- **Complete coordination of recommendations**
- **Engage in outreach to share progress, validate findings, and continue information collection**
- **Submit formal report to DoD in summer 2017**
- **Continue to collaborate with DoD and other agencies**

Report will be coordinated within DoD, and other government agencies as appropriate, after new leadership team is in place

Contact Information:

Catherine J Ortiz, President
Defined Business Solutions, LLC

cjortiz@definedbusiness.com

804-462-0564
202-683-2021

Stock photos licensed from Getty Images