Cybersecurity for Manufacturing

NDIA Manufacturing Division Meeting

21 October 2015

Megan Brewster, PhD

Senior Policy Advisor for Advanced Manufacturing, AAAS/ORISE Fellow
Office of Science and Technology Policy
Take-Aways

• National Network for Manufacturing Innovation
  o Manufacturing generates economic activity
  o There’s innovation in manufacturing
  o 7 Manufacturing Innovation Institutes so far
  o Many topics remain for engagement
  o Some manufacturing mega-trends

• Cybersecurity for Manufacturing
  o Manufacturers received highest volume of spear-phishing attacks
  o Companies of all sizes are at risk
  o Attackers want manufacturers’ secrets
  o Malware for industry control systems represent a notable shift in targets and techniques
  o Manufacturers recognize threats, but struggle to respond
  o Some available resources... what would you add?
Manufacturing Generates Economic Activity

- **Manufacturing**: making something that can be “dropped on your foot”
- **Advanced Manufacturing**: when technology gives competitive advantage
- **Manufacturing** has the **greatest multiplier effect**: every $1 in manufacturing value added, $1.33 in additional value is created in other sectors

![Economic Activity Generated by $1 of Sector GDP, 2012](image)
There’s Innovation In Manufacturing

Source: Census Bureau
There’s Innovation In Manufacturing

Then-1980s

Ford River Rouge Complex (1920s)

1980s-Now

OEM

Tier 1

Tier 2

Tier 3

Tier 1

Tier 2

Tier 3

Tier 2

Tier 3

Tier 2

Tier 3

Library of Congress
President’s Council of Advisors on Science and Technology

Market Failure in Pre-Competitive Applied Manufacturing R&D

National Network for Manufacturing Innovation creates the space for industry and academia to work on industry-relevant problems:

- Addresses the market failure of industry underinvestment in “pre-competitive” applied R&D
- Focuses on “de-risking” new technologies and materials to scale-up for U.S. manufacturers
7 Manufacturing Innovation Institutes So Far

- America Makes
  Additive Mfg.
  Youngstown, OH
- Power America
  Power Electronics
  Raleigh, NC
- LIFT
  Light/Modern Metals
  Detroit, MI
- IACMI
  Adv. Composites
  Knoxville, TN
- DMDII
  Digital Mfg.
  Chicago, IL
- Photonics
  Rochester, NY
- Flex. Electronics
  San Jose, CA

- $495M Federal funding catalyzed over $1,214M from consortia
- Institutes have attracted hundreds of companies and universities as active partners from across the country

Three more under way...
- Fibers and Textiles
- Smart Mfg.
- Topic TBA
Each institute has:

1) Clear, unique institute focus

2) Clear industry value proposition

3) Strong Partnerships

4) Ability to address critical challenges

5) A balanced portfolio of projects

Partnerhsip: Industry – Academia – Government

Working better, together to create transformational technologies and build new products and industries
### Enabling Technologies
- bio-inspired manufacturing
- bioprocessing
- cryogenic techniques
- cyber security
- cyberphysical manufacturing
- manufacturing equipment (customizable)
- mechatronics
- MEMS/NEMS and embedded technologies
- nano/bio manufacturing
- nano/micro manufacturing
- surface engineering
- manufacturing facilities/wafer fab

### Manufacturing Processes
- additive manufacturing
- assembly and joining (multi-material joining, solid state welding and joining)
- coating and deposition (printing, roll-to-roll processing)
- composites manufacturing
- electron beam processing
- laser processing (cutting, marking, sintering, tracking and welding)
- machining and precision machining
- near-net shape technologies (casting, extrusion, forging, forming, hydroforming, molding, rolling)
- polymeric-based web conversion
- powder metallurgy
- separations and purification
- surface finishing and peening
- wide bandgap manufacturing

### Industry Sectors
- chemical
- cyber security
- electronics (custom, assembly, flexible, nano, organic, printed)
- electro-optical devices
- energy (clean/renewable/alternative, energy-conversion equipment, biofuels, fuel cells, grid technologies and integration, natural gas, solar cells, wind)
- energy storage/batteries
- fluid power/pneumatics
- food
- healthcare (biomedical devices, nanomedicine, personalized medicine, pharmaceuticals, tissue engineering)
- high-performance computing
- maritime technologies
- national security and terrorism
- optics and photonics (imaging, photonic integrated circuits)
- thermal processing and HVAC
- transportation (natural gas vehicles)
- water and water distribution

### Manufacturing Systems
- automation technologies
- autonomy
- digital manufacturing
- digital model-based manufacturing
- dynamic machine tool management
- manufacturing strategy development
- robotics and autonomy
- sensors (for diagnosis and control, harsh conditions, remote sensing)
- servo technologies
- smart/intelligent manufacturing (sensor-integrated manufacturing)

### Sustainable Manufacturing
- energy efficiency/shortage
- repair welding
- thermoplastic recycling
- reducing greenhouse gases
- wastewater reclamation and reuse

### Metrology and Characterization
- advanced metrology
- in-situ metrology
- materials characterization (thin film and bulk stoichiometry)
- non-destructive evaluation

### Product Development/Manufacturing Software/Tools
- "big data"
- design tools and informatics
- information technology systems
- modeling and simulation
- rapid prototyping
- mass customization/custom electronics

### Materials
- "smart" materials, advanced magnets, amorphous metals, bio/biomedical, ceramics
- Chemicals, coatings, thin films/surface treatments, composites, electro-optical materials, lightweight materials, metamaterials, nanomaterials, next-generation semiconductors, photovoltaics, powder, superalloys
Some Manufacturing Mega-Trends

**Service models**
- Product + service
- Lean/Just-in-time manufacturing
- Supply chain innovation
- Small batches of personalized products
- Democratization of manufacturing equipment
- On-site manufacturing

**Digitization**
- Cloud computing
- Internet of things
- Cybersecurity
- Artificial intelligence/Robotics/Virtual

**Product Design**
- Advanced materials
- Sustainability
Take-Aways

• National Network for Manufacturing Innovation
  o Manufacturing generates economic activity
  o There’s innovation in manufacturing
  o 7 Manufacturing Innovation Institutes so far
  o Many topics remain for engagement
  o Some manufacturing mega-trends

• Cybersecurity for Manufacturing
  o Manufacturers received highest volume of spear-phishing attacks
  o Companies of all sizes are at risk
  o Attackers want manufacturers’ secrets
  o Malware for industry control systems represent a notable shift in targets and techniques
  o Manufacturers recognize threats, but struggle to respond
  o Some available resources... *what would you add?*
Mfg’ers received highest volume of spear-phishing attacks

<table>
<thead>
<tr>
<th>Industry</th>
<th>2014</th>
<th>2013</th>
<th>Risk Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>13</td>
<td>13</td>
<td>1 in 3.0</td>
</tr>
<tr>
<td>Services—Nontraditional</td>
<td>14</td>
<td>14</td>
<td>1 in 2.9</td>
</tr>
<tr>
<td>Finance, Insurance &amp; Real Estate</td>
<td>18</td>
<td>13</td>
<td>1 in 4.8</td>
</tr>
<tr>
<td>Services—Professional</td>
<td>15</td>
<td>15</td>
<td>1 in 3.4</td>
</tr>
<tr>
<td>Wholesale</td>
<td>10</td>
<td>5</td>
<td>1 in 3.2</td>
</tr>
<tr>
<td>Transportation, Gas, Communications, Electric</td>
<td>7</td>
<td>6</td>
<td>1 in 3.1</td>
</tr>
<tr>
<td>Public Administration (Gov.)</td>
<td>5</td>
<td>5</td>
<td>1 in 4.8</td>
</tr>
<tr>
<td>Retail</td>
<td>3</td>
<td>2</td>
<td>1 in 6.5</td>
</tr>
<tr>
<td>Mining</td>
<td>1</td>
<td>1</td>
<td>1 in 6.9</td>
</tr>
<tr>
<td>Construction</td>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Risk ratio (Of all companies of a given industry)

Companies of all sizes are at risk

Distribution of attacks

<table>
<thead>
<tr>
<th>Size</th>
<th>2014</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small (1-250 employees)</td>
<td>34%</td>
<td>30%</td>
</tr>
<tr>
<td>Medium (251-2500 employees)</td>
<td>25%</td>
<td>31%</td>
</tr>
<tr>
<td>Large (2500+ employees)</td>
<td>41%</td>
<td>39%</td>
</tr>
</tbody>
</table>

Risk ratio (Of all companies of a given size)

<table>
<thead>
<tr>
<th>Size</th>
<th>2014</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small (1-250 employees)</td>
<td>45%</td>
<td>19%</td>
</tr>
<tr>
<td>Medium (251-2500 employees)</td>
<td>63%</td>
<td>33%</td>
</tr>
<tr>
<td>Large (2500+ employees)</td>
<td>83%</td>
<td>43%</td>
</tr>
</tbody>
</table>

### Attackers Want Manufacturers’ Secrets

Bars in each box depict data from 2012, 2013, and 2014.

<table>
<thead>
<tr>
<th>Category</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crimeware</td>
<td>1%</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
</tr>
<tr>
<td>Cyber-espionage</td>
<td>9%</td>
<td>27%</td>
<td>45%</td>
<td>18%</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>11%</td>
<td>13%</td>
<td>73%</td>
<td>7%</td>
</tr>
<tr>
<td>Physical Theft/Loss</td>
<td>26%</td>
<td>7%</td>
<td>14%</td>
<td>31%</td>
</tr>
<tr>
<td>Miscellaneous Errors</td>
<td>16%</td>
<td>32%</td>
<td>12%</td>
<td>26%</td>
</tr>
<tr>
<td>Payment Card Skimmers</td>
<td>2%</td>
<td>7%</td>
<td>7%</td>
<td>9%</td>
</tr>
<tr>
<td>Point of Sale</td>
<td>14%</td>
<td>5%</td>
<td>4%</td>
<td>1%</td>
</tr>
<tr>
<td>Insider Misuse</td>
<td>2%</td>
<td>5%</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td>Web App Attacks</td>
<td>2%</td>
<td>5%</td>
<td>2%</td>
<td>1%</td>
</tr>
<tr>
<td><strong>Manufacturing</strong></td>
<td>34%</td>
<td>60%</td>
<td>79%</td>
<td>7%</td>
</tr>
</tbody>
</table>

---

### Attackers Want Manufacturers’ Secrets

**Distribution of espionage-targeted attacks**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manufacturing</td>
<td>27.4%</td>
</tr>
<tr>
<td>Public</td>
<td>20.2%</td>
</tr>
<tr>
<td>Professional</td>
<td>13.3%</td>
</tr>
<tr>
<td>Information</td>
<td>6.2%</td>
</tr>
<tr>
<td>Utilities</td>
<td>3.9%</td>
</tr>
<tr>
<td>Transportation</td>
<td>1.8%</td>
</tr>
<tr>
<td>Educational</td>
<td>1.7%</td>
</tr>
<tr>
<td>Real Estate</td>
<td>1.3%</td>
</tr>
<tr>
<td>Financial Services</td>
<td>0.8%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>0.7%</td>
</tr>
</tbody>
</table>
Malware for ICS = Notable Shift in Targets, Techniques

'DRAGONFLY' VIRUS STRIKES U.S. POWER PLANTS
Cyberattacks seek to control or even sabotage America's energy grid
Published: 07/06/2014 at 6:32 PM

Sandworm Windows zero-day vulnerability being actively exploited in targeted attacks
Critical new Windows zero-day has reportedly been used in a limited number of targeted cyberespionage attacks to deliver a back door on to the victim's computer.
By: Symantec Security Response
Created 14 Oct 2014

HACK ATTACK CAUSES 'MASSIVE DAMAGE' AT STEEL WORKS
22 December 2014 | Technology

AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON
Malware for ICS = Notable Shift in Targets, Techniques

<table>
<thead>
<tr>
<th>Metric</th>
<th>Information Technology (IT)</th>
<th>Operational Technology (OT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>Supports people</td>
<td>Controls machines</td>
</tr>
<tr>
<td>Purpose</td>
<td>Process transactions, provide information</td>
<td>Control/monitor physical process and equipment</td>
</tr>
<tr>
<td>Lifetime</td>
<td>~5 years, updated regularly</td>
<td>15-30 years, little/no tolerance for delays or downtime required to update</td>
</tr>
<tr>
<td>Architecture</td>
<td>Generic</td>
<td>Custom: event-driven, real-time, embedded hardware/software</td>
</tr>
<tr>
<td>Interfaces</td>
<td>GUI, web, keyboard</td>
<td>Electromechanical, sensors, actuators, coded displays, hand-held devices</td>
</tr>
<tr>
<td>Ownership</td>
<td>CIO, IT</td>
<td>Engineers, technicians, operators, managers</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Corporate network (IP)</td>
<td>Control networks (hard-wired twisted pair and IP)</td>
</tr>
</tbody>
</table>
Mfg’ers Recognize Threats, But Struggle To Respond

Manufacturing is behind the curve
- “On a scale of 1 to 100, we are at a 0.0001. It’s why the government is offering us money”
- “Machine shops are still in the dark ages of digitization”
- “Nothing is obvious anymore when compared to pre-cyber security problems”

The threat is significant
- “We need to successful 100% of the time, but the bad guys only need to be successful once”
- “There are two types of companies - ones that have been hacked and ones that don’t know they have been hacked”
- “Havoc is more easily recognized and responded to but the subtle attacks (e.g., taking over a machine) are what keep people up at night”

Companies underestimate the risks
- “Security isn’t going to pay the bills”
- “The mindset is that it’s always someone else who is going to hacked”
- “There is a constant optimization problem of where to put the next dollar”
- “You don’t think about back door being unlocked”
- “How many people have seen a password taped to a machine tool?”

We need to act quickly
- “Cyber security is the next arms race”
- “How do we position ourselves for excellence that is survivable?”
- “Government can provide the playground for industry and academia”
Some Available Resources... what would you add?

- NIST: Framework for Improving Critical Infrastructure Cybersecurity
- PCAST: reports on NITRD reviews, Cybersecurity, etc.
Some Available Resources... *what would you add?*

- NIST: Cybersecurity Center of Excellence
- DHS: Business Continuity Planning Tool
- NIST: National Initiative for Cybersecurity Education
- NSF: Advanced Technological Education centers on cyber
Potential Industry Roadmap Initiatives Brainstorm:

• Manage legacy manufacturing systems and production equipment (e.g., security layer)
• Create cyber-physical testing environment
• Create secure protocols for the digital thread
• Develop small- and medium-sized manufacturer support tools
• Model manufacturing cyber threats (visualize, simulate)
• Conduct threat analysis research for operational technology
• Create industry consortium for knowledge/data/threat sharing
• Create/manage supplier certification for cyber-secure practices
• Map policy landscape
Take-Aways

• National Network for Manufacturing Innovation
  o Manufacturing generates economic activity
  o There’s innovation in manufacturing
  o 7 Manufacturing Innovation Institutes so far
  o Many topics remain for engagement
  o Some manufacturing mega-trends

• Cybersecurity for Manufacturing
  o Manufacturers received highest volume of spear-phishing attacks
  o Companies of all sizes are at risk
  o Attackers want manufacturers’ secrets
  o Malware for industry control systems represent a notable shift in targets and techniques
  o Manufacturers recognize threats, but struggle to respond
  o Some available resources... what would you add?