Cybersecurity Issues for Small-to-Medium-sized Manufacturers

Chris Peters
CEO
The Lucrum Group
410-647-3200
cpeters@thelucrumgroup.com
Threats To Interoperability

Supply Chains Targeted

Suppliers Building Walls

Manufacturers Denying Supply Chain Connections
## Manufacturing Risks Are Different

<table>
<thead>
<tr>
<th>Information Technology (IT)</th>
<th>Operations Technology (OT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Business apps (Acct, ERP)</td>
<td>• Industrial control systems</td>
</tr>
<tr>
<td>• Modern operating systems</td>
<td>• Windows NT/DOS</td>
</tr>
<tr>
<td>• Priorities: C-I-A</td>
<td>• Priorities: A-I-C</td>
</tr>
<tr>
<td>• Regularly maintained</td>
<td>• No “Patch Tuesday”</td>
</tr>
<tr>
<td>• Use anti-virus/firewalls</td>
<td>• Not easily protected</td>
</tr>
</tbody>
</table>
Why Is This Important?

• Verizon 2018 Data Breach report
  – 86% of manufacturing incidents are targeted
  – 47% of breaches involve theft of IP
• Industrial Control Systems decoy
  – 1,300 access attempts in one month
  – 400 were successful
• DoD intently focused on the issue
DoD Focus

• DFARS Clause 252.204-7012
  “Safeguarding covered defense information and cyber incident reporting”

• NIST 800-171
  “Protecting controlled unclassified information in nonfederal information systems and organizations”

• DoD Announcement: New requirements
  – “Cybersecurity Maturity Model Certification”
#1-Supply Chain Is A Target

- NDIA Research
  - 60% had not read DFARS
    - 46% said it was difficult to understand
  - 45% had not read NIST 800-171
    - 40% said document was easy to understand
  - Rate OT lower importance than IT and IP
  - Underestimate cost by factor of 10
#1-Supply Chain Is A Target

- Poorly defended
- Have “What” and “How”
- Don’t report incidents
- Island Hopping
#2-Suppliers Building Walls

Recipes
Drawings/Models
Computer code
Production schedules

Production data
Sensor data
Quality data
Inventory data
#2-Suppliers Building Walls

Recipes
Drawings/Models
Computer code
Production schedules

Production data
Sensor data
Quality data
Inventory data
#3-Mfrs Denying SC Connections

- Concerned about cyber threats
- NIST 800-171 hard to apply to OT
- No effective compliance audit
- Exchange static data by email
What To Do

Look internally
• OT Addressed?
• IT and OT collaborating?
• Compliance?
• Resilient supply chain?
• Resources?
What To Do

Educate your suppliers

- Risks and impact
- Reduce risk
- Simplify reporting
- Ongoing campaign
Resources

“Cybersecurity for Manufacturing networks”

“Implementing Cybersecurity in DoD Supply Chains”

“2018 Data Breach Investigations Report”

“The State of Industrial Cybersecurity 2018”
Thank you

Chris Peters
CEO
The Lucrum Group
410-647-3200
cpeters@thelucrumgroup.com