
NCS
NATIONAL CYBER SUMMIT
June 5-7, 2018 | Huntsville, Alabama

Cybersecurity in Advanced Manufacturing: Threats, Challenges, and Opportunities

Track Session – Advanced Manufacturing

Brandon N. Robinson

Balch & Bingham LLP

- Connectivity (IoT devices, automation, artificial intelligence, etc.) increasingly in the OT environment.
- Greater efficiency, precision, but also vulnerability.
- 2014-16, the number of cyber attacks against adv mfg nearly doubled.*

*Corey Bennett, “DHS: Cyberattacks on Critical Manufacturing Doubled in 2015” *The Hill*; 15 January 2016. http://thehill.com/policy/cybersecurity/266081-dhs-critical-manufacturing-cyberattacks-have-nearly-doubled

THREATS

Actors (Who's getting in?)	Vectors (How are they getting in?)	Information (What do they want?)
• True hackers • Nation States (China, Syria, Iran) • "Hacktivists" (e.g., radical environmentalists) • Insiders (e.g., Snowden, employees, disgruntled ex-employees)	• Traditional hacking, • Insider access • Social engineering • Vendors (e.g., Target)	• PII • Account/Financial information • Intellectual Property • M&A (insider trading)

Cyber attacks against manufacturing:

- Jeopardize product integrity
- Steal sensitive intellectual property (IP)
- Threaten production availability and safety
- Safety system failures, unreliable products

Themes:

- Managing disconnect between IT and OT
- Business systems vs. operations
- OT = production, IT = security
- Reaching IT through OT
- Increasingly global supply chain

Key Laws and Regulations:

- FERC Supply Chain Standards
- Alabama Data Breach Notification Act
- General Data Protection Regulation (GDPR)
- NIST SP 800-171 and 48 CFR 252.204-7012

- FERC NOPR on Supply Chain Risk Management Reliability Standards (Jan 2018)
  - CIP-013-1 (Cyber Security Supply Chain Risk Management)
  - CIP-005-6 (Cyber Security – Electronic Security Perimeters)
  - CIP-010-3 (Cyber Security – Configuration Change Management and Vulnerability Assessments)

NERC CIP Supply Chain Reliability Standards

- Standard addresses: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.
- NOPR proposed:
  - Inclusion of EACMS associated with medium and high impact BES Cyber Systems;
  - Direct NERC to evaluate cyber security supply chain risks presented by PACS and PCAs in NERC BOT study. Interim and final reports to be filed with FERC.

Alabama Data Breach Notification Act

- Effective June 1, 2018
- "Sensitive PII" - fairly typical, but comprehensive; electronic only
- AG enforcement only of notification measures
- 45 day notification period (10 days for 3rd party agents)
- AG notice if over 1,000
- "reasonable security measures"; breach investigation; records disposal
- Substitute notice if >100,000 or costs >$500K

Penalties:

- Violations of the notification provisions are subject to penalties of up to $2,000 per day, and a cap of $500,000 per breach.
- In addition, any business violating the notification provisions will be liable for a penalty of up to $5,000 per day for each day it fails to take reasonable action to comply with the notification provisions.

General Data Protection Regulation (GDPR)

- Effective May 25, 2018
- Data Controller v. Processor
- Applies to US businesses if “offering goods or services” or “monitoring behavior” of EU citizens even if business not established in EU

- **"Processing"**: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **"Personal data":** "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an *ID number*, *location data*, an *online identifier*, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural , or social identity of that natural person."

CHALLENGES

1) Right to be forgotten (erased) (do you know where it all is, do you have process in place?)
2) Data Portability. Subject can "port" (move) data to your competitor upon request. (Train EEs)
3) Transparency. Say what you do, do what you say (also FTC Sec. 5). Clear notice, manage to that notice.
4) Data Minimization. Only share what you need to. Only keep for period of time you absolutely need it.
5) Data Protection Officer. If Art. 3(2), controller or processor "shall designate in writing a representative in the Union." Can be EE or Ker.
6) Access. Right to obtain confirmation as to whether or not personal data is being processed and to certain details.
7) Rectification and Erasure. Correct or delete data.
8) Right to Restriction/Objection. Right to object to or restrict processing.
9) Automated profiling. Right to not be subject to decisions based solely on automated processing.

- Penalties. In some cases, up to 20 million Euros or 4% of worldwide annual turnover (revenue), whichever is greater.

- Obtaining/Retaining Trust & Competitive Advantage. Once you come out on other side you can show your competitive edge for clients and potential clients with European business. On the other hand, in the era of data breaches/Facebook/etc., it's hard to have to rebuild trust.

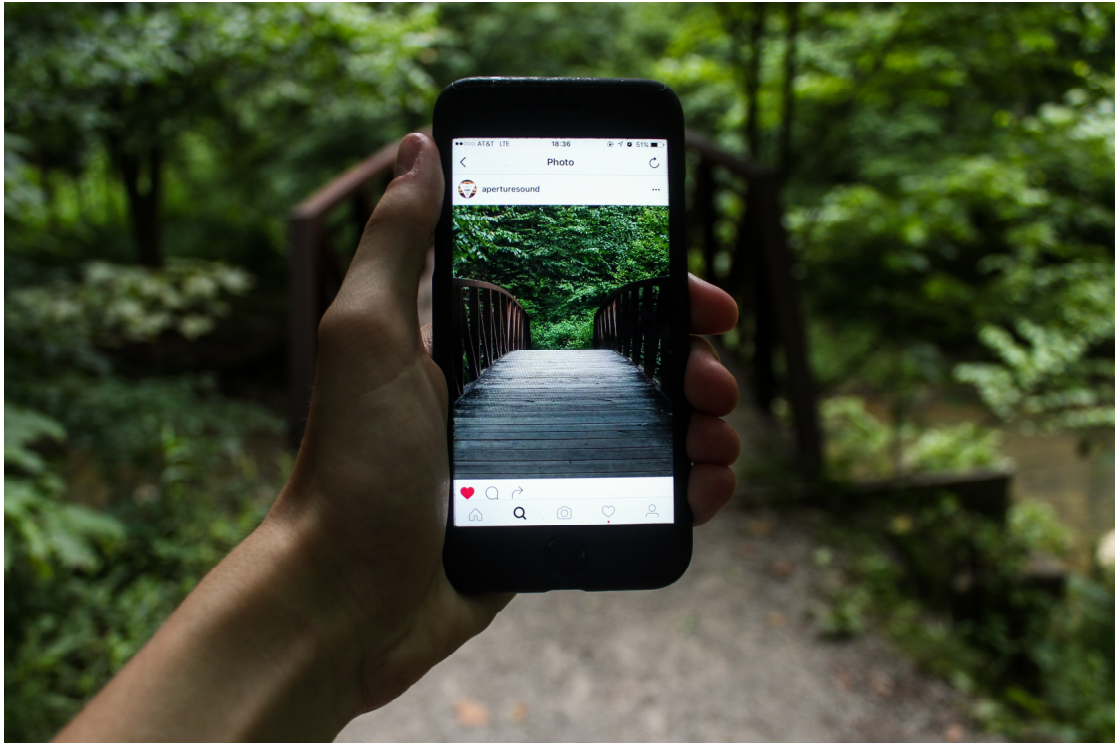
- Privacy By Design. Seeking compliance with GDPR forces you to engage in deep, comprehensive, and productive conversations about your ongoing relationship with data.

One week after GDPR …

- Inboxes filling with updated privacy policies
- Within 48 minutes, complaints filed in France, Austria, Belgium, and Germany against Facebook, Google, and others.
- Many US news outlets blocking European access until they can comply
- European Commission itself experiences data leak (although it’s not liable under GDPR)

- 48 C.F.R. 252.204–7012; and NIST SP 800-171
- Some manufacturers are having issues applying 252.204-7012 and NIST SP 800-171 effectively because they are designed for IT systems not OT systems
- In order to modify the regulations to better fit an OT environment, a Contractor shall submit a request to deviate from NIST SP 800–171 in writing to the Contracting Officer, for consideration by the DoD

OPPORTUNITIES



It doesn't matter how high you build the castle walls…

What to do before a breach:

- Create an Incident Response team
- Inventory data; create a plan
- Create/review policies and procedures
- Train employees on policies and procedures as well as on good info gov practices (passwords, phishing, etc.)
- Maintain a good relationship with law enforcement.
- Consider cyber insurance; review your policies
- Vendor management

What to do AFTER a suspected breach

- HOPEFULLY – Activate your incident response team and implement your plan. If not … some rules of thumb:
- Engage legal counsel (attorney/client work product, privilege) – can be in-house or outside
- Investigate immediately. – identify source and compromised data, restore system integrity
- Control the story = communicate internally and externally, as promptly and accurately as possible. “art of the statement”. Review for notification obligations (AL data breach law, contracts, insurance policies)

Questions?

Brandon N. Robinson, CIPP/US

Balch & Bingham LLP

bnrobinson@balch.com

205-226-3427

www.dataprivacyandsecurityobserver.com

Twitter: @BrandonNRobinso

https://www.linkedin.com/in/brandonnrobinson/