southtec®
A Manufacturing Technology Series Event

sme AMT

# DEVELOPING CYBERSECURITY TRAINING FOR MANUFACTURING

Dr. Vincent W. Howell, FSME.,CMfgE, CCP
Manager, Intellectual Asset Protection (retired)
Corning Incorporated

MANUFACTURING™ TECHNOLOGY SERIES

# ABSTRACT


- Cybersecurity is a concern in manufacturing. All manufacturing organizations must manage cybersecurity risks. This presentation will help manufacturers understand its criticality and develop training strategies to manage cybersecurity risks.

# AGENDA

- THE CHALLENGE FOR MANUFACTURING
- CURRENT ISSUES
- THE COURSE OF ACTION
  - COMPREHENSIVE POLICIES
  - COMPANY-WIDE TRAINING
- COURSE CONTENT
- CONCLUSION
- Q&A

southtec®
A Manufacturing Technology Series Event

sme AMT

# THE CHALLENGE FOR MANUFACTURING

https://www.youtube.com/watch?v=jZkHpNnXLB0

MANUFACTURING™ TECHNOLOGY SERIES

southtec®
A Manufacturing Technology Series Event

sme AMT

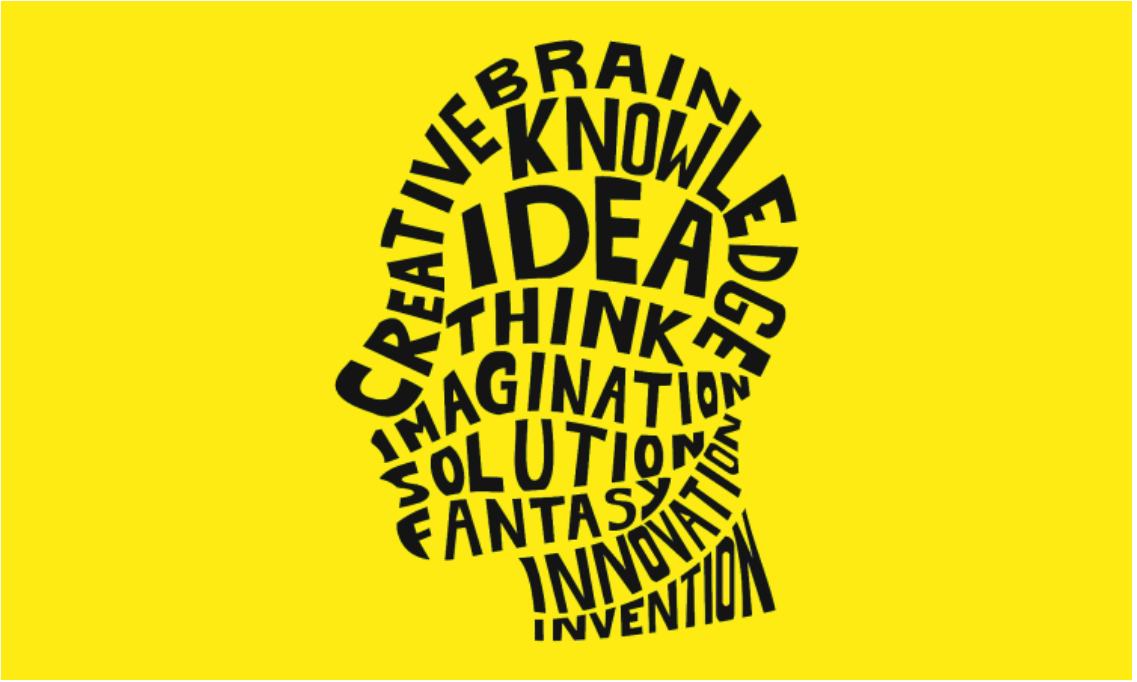
MANUFACTURING™ TECHNOLOGY SERIES

southtec®
A Manufacturing Technology Series Event

sme AMT

# THE CHALLENGE FOR MANUFACTURING - Lessons

**Manufacturing is full of ...**




**THESE THINGS - TRADE SECRETS, PATENTS, DEVELOPING IDEAS, INFORMATION, DRAWINGS, ETC. - MUST BE PROTECTED!**

MANUFACTURING™ TECHNOLOGY SERIES

southtec®
A Manufacturing Technology Series Event

# CURRENT ISSUES

sme AMT

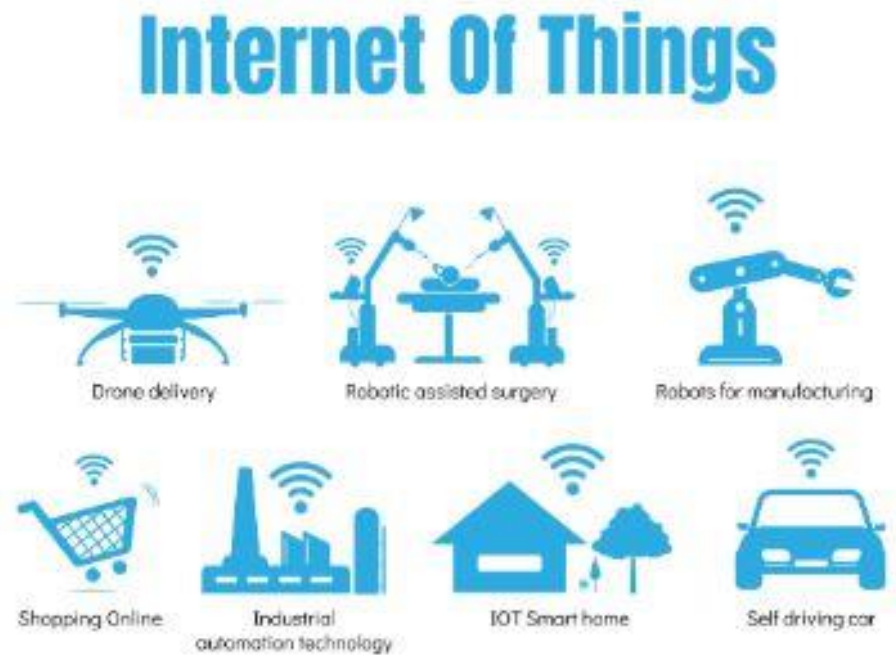
- 50% of Manufacturers Experienced Data Breaches in Past Year (Industry Week, Jun 24, 2019)

MANUFACTURING™ TECHNOLOGY SERIES

# CURRENT ISSUES



- A June 2019 Security Magazine article provided the following data according to the 2019 Manufacturing and Distribution Report.



# CURRENT ISSUES



- “Digital technologies—Industrial Internet of Things, artificial intelligence, and robotics, among others—continue to receive significant attention. These technologies are rewriting the rules of competition for industrial companies, while also increasing their vulnerability to the growing threat of cyber attacks and data breaches.” 7

# CURRENT ISSUES

- “More than half of the companies participating in the survey reported they have at least some automation in production processes/machining (79 percent), assembly (64 percent), and packaging (60 percent).” [7]

# CURRENT ISSUES

- “Larger companies are roughly twice as likely as smaller companies to have extensively automated their production process/machining (56 percent vs. 31 percent), assembly (53 percent vs. 21 percent), and packing (45 percent vs. 23 percent).”7
-

**THE BOTTOM LINE -**

"Manufacturers face a barrage of cybersecurity threats today, and half of companies have fallen victim to at least one data breach during the past 12 months"[6]

# THE COURSE OF ACTION

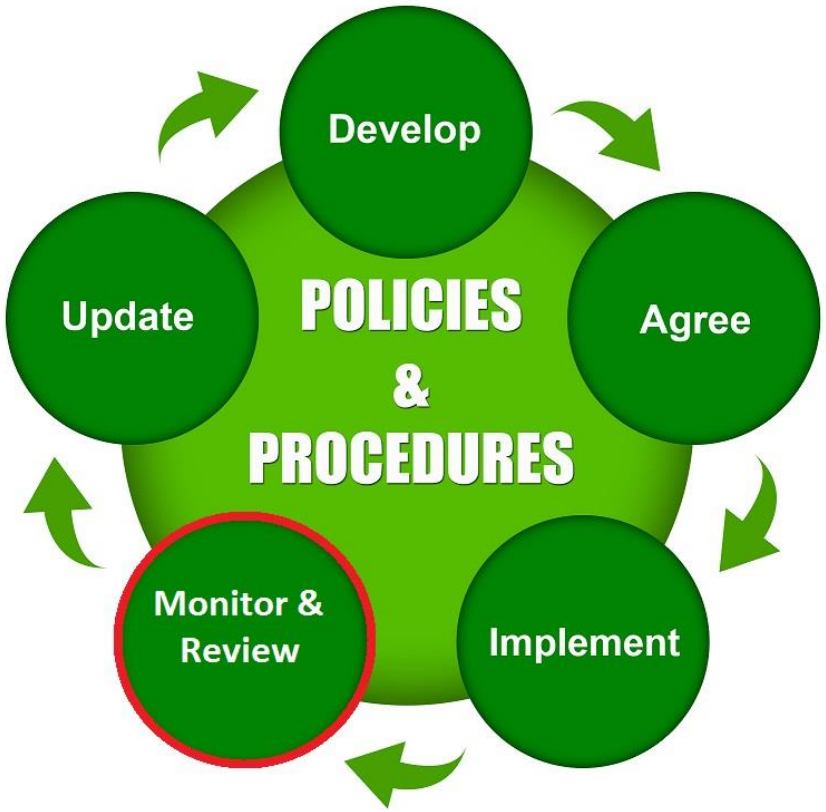



Image Source: http://betweenwallandmain.com/focus-monitoring-reviewing-policies-procedures/

# THE COURSE OF ACTION

- Salo Fajer, chief technology officer with Digital Guardian, sums it up succinctly: “The weakest link in data defense is the employee. Train them on your policies regarding the use of confidential data. It also helps to perform regular security awareness training and invite your contractors, vendors and partners to participate, as they should be subject to your data protection policies as well.”[5]

# THE COURSE OF ACTION-Training

Image Source: https://www.moonstone.co.za/training-requirements-under-the-new-fit-and-proper-determination/

# THE COURSE OF ACTION

Ron Christie of UC-Riverside - “Studies have shown that a substantial number of cyber-attacks involve the unintended actions of users of information systems, and this risk can be significantly lowered through an effective training program.”[4]

# THE COURSE OF ACTION

- All employees should be required to complete information security awareness training.
- Provide this training for new hires so that a culture of information security is taught at the onset.
- If your supply chain has access to information systems, they should be required to complete training as a supplement to non-disclosure agreements

# THE COURSE OF ACTION

- Training can be offered online.
- Local community colleges can often provide resources for smaller manufacturers.
- Your cybersecurity awareness training does not need to be an all-day affair; can be video-based training classes; can be one hour modules.

southtec®

# TRAINING CONTENT

MANUFACTURING™ TECHNOLOGY SERIES

sme AMT

# TRAINING CONTENT


## Computer Usage

- Company guidelines for the use of company-issued computers, as well as portable media (particularly that which interfaces with company hardware, software and data).

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## Social Networking

- Address whether social networking is appropriate on company assets; company's guidelines for what employees should share (or not) about their work in order to prevent company secrets being inadvertently leaked.

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## Email

- Guidelines for using the company email system. For example, are employees restricted from sending company email to their personal accounts?

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## Browsing

- What are the company's guidelines regarding browsing the Internet?

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## Mobile Device Security

- Guidelines for the appropriate use of company mobile phones, BYOD, USB drives and other mobile media.

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## Passwords

- How frequently should passwords be changed? What password format(s) are acceptable?

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## Data Security

- Define company-critical data, drawing, trade secrets, research notebooks, data security systems; provide detailed instructions regarding how to keep them secure.

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## What to Do if Hacked

- Provide guidelines as to who employees should contact if they suspect a cyber-attack or a virus on a computer.

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## Information Privacy

- Emphasize how important it is to maintain the privacy of information related to assets like collected personal information, employee records, financial data, and other business-related details.

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# TRAINING CONTENT


## International and Domestic Travel

- The focus regarding travel should be in preventing company information from being discussed in public areas such as airports, hotels, and restaurants, such that critical data or trade secrets might be overheard.

.

Image Source:
https://security.it.miami.edu/services/awareness-training/index.html

# ONE FINAL THOUGHT

**POLICIES, PROCEDURES, TRAINING, AND ALL OTHER INFORMATION SECURITY METHODS IN MANUFACTURING ARE CRITICAL. COLLABORATION WITH YOUR I.T. FUNCTION IS EQUALLY AS CRITICAL!**

.


Image Source:
https://www.lakewoodwater.org/lwd/page/information-technology
ning/index.html

# CONCLUSION

**A recent observation from Samir Agarwal, in his article "The 3 Major Cybersecurity Gaps Enterprises Face" (July 6, 2017 issue of Security Magazine,) highlights the complexity and challenge this topic has for manufacturing. It is an issue that large through small manufacturing organizations must keep at the forefront of all employee.**

southtec®
A Manufacturing Technology Series Event

# CONCLUSION

sme AMT

"Cybersecurity becomes more challenging every year as hackers, criminals and other bad actors look for new and more sophisticated ways to break into systems and wreak havoc. Within the past few years, ransomware and distributed denial-of-service attacks have become commonplace across a variety of industries. With attacks such as these, time is of the essence. Enterprises can't spend days or weeks assessing what happened before taking action -- the damage will have already been done."
https://youtu.be/ArvEq2tzMMY

MANUFACTURING™ TECHNOLOGY SERIES

southtec®
A Manufacturing Technology Series Event

**Contact Info:**
Vincent Howell
607-377-1866
vincent.w.howell@gmail.com


sme AMT

southtec®
A Manufacturing Technology Series Event

# References


1. Beshar, Peter J., “The Cybersecurity Challenge Every Business Should Prepare For,” http://fortune.com/2016/01/26/davos-cybersecurity-challenge-business.

2. “KU to Train Next-Generation Cybersecurity Experts for Government Service,” http://news.ku.edu/2016/01/20/ku-train-next-generation-cybersecurity-experts-government-service#sthash.CLtJfvYt.dpuf http://news.ku.edu/2016/01/20/ku-train-next-generation-cybersecurity-experts-government-service#sthash.CLtJfvYt.dpuf.

3. Neil, Stephanie, “Cybersecurity and the Manufacturing Mindset,” www.automationworld.com/all/cybersecurity-and-manufacturing-mindset.


sme AMT

southtec®
A Manufacturing Technology Series Event

# References


4. Marantos, Jeanette, “UC Wants YOU to Complete Cyber Security Training By Jan. 31,” https://ucrtoday.ucr.edu/34412.

5. Fajer, Salo, “What Manufacturers Need to Know about Cybersecurity,” March 3, 2015, www.industryweek.com/information-technology/what-manufacturers-need-know-about-cybersecurity.

6.”Manufacturing Companies Face Cybersecurity Threats,” https://www.securitymagazine.com/articles/90411-manufacturing-companies-face-cybersecurity-threats

7.Agarwal, Samir, “The 3 Major Cybersecurity Gaps Enterprises Face,” by July 6, 2017, https://www.securitymagazine.com/articles/88136-the-3-major-cybersecurity-gaps-enterprises-face


sme AMT

# southtec®

A Manufacturing Technology Series Event

MANUFACTURING™ TECHNOLOGY SERIES

sme AMT