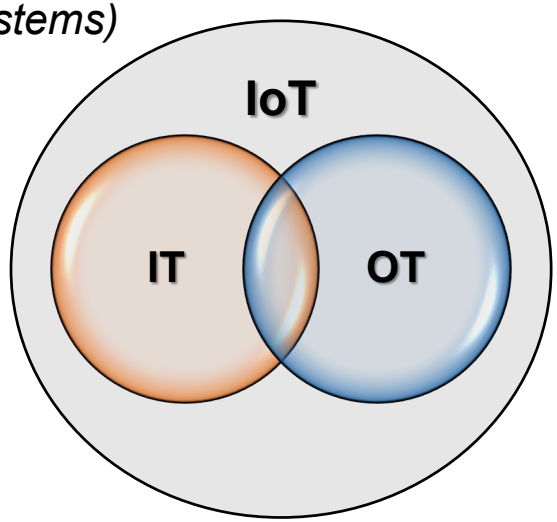
Cyber Threats to Industrial Assets

IT vs OT and the IoT

- **Information Technology (IT):** *The entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT, historically, does not include embedded technologies that do not generate data for enterprise use. (Business Systems)*

- **Operational Technology (OT):** *Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. (Production Systems)*

- **Internet of Things (IoT):** *The concept of extending Internet connectivity beyond conventional computing platforms such as personal computers and mobile devices, and into any range of traditionally dumb or non-internet-enabled physical devices and everyday objects. (Convergence of Systems)*



Evolving Threats

- Network and Endpoint Breaches (early 2000s)
  - Transition from industrial Protocols to TCP/IP
- Custom Built OT/ICS Malware
  - STUXNET (2010), HAVEX (2013), BlackEnergy 2 (2014), Crash Override/Industroyer (2016), TRITON (2017)
- Crossover breaches from IoT (Present)
  - Convergence of threats

Main Threat Vectors

- Email
- Removable Media
- Internet Connectivity

Main Attack Types:

- Phishing
- Watering Hole
- Malware (Trojan installers)

So what?

- Steady increase in OT attacks in 2018
  - 43% of all monitored OT faced an intrusion attempt last Year.
  - Increasing number of intrusions for OT network reconnaissance.
- Increasing connectivity in OT
  - Lifecycles decreasing.
  - Lines between IT and OT blurring.
- Threats to OT pose increased risk to other operations on corporate networks
  - Data integrity.
  - Intellectual property theft.
  - Cyber crime (ransomware, banking fraud, identity theft, etc.)
- Threat to OT outpacing defense efforts
  - Defender has to be right all the time, attacker only has to be right once.

Notable ICS attacks

- STUXNET: Attack against Iranian nuclear industry, 2010
- German Steel Mill Attack: Destroyed Blast Furnace, 2014
- Ukrainian Power Grid: Blacked out power across parts of Ukraine, 2015
- New York Dam Attack: Nation State actions gained control of dams, 2013-2016
- US Water Treatment System: Flow control and chemical distribution effected, 2016
- San Francisco Transit System: Ransomware aimed at ticketing and track controls, 2016
- City of Atlanta: Ransomware shuts down City Services, 2018