

# Cyber Securing Supply Chain

Harsha Banavara

Cybersecurity Technical Policy Manager

Signify (previously Philips Lighting)

# Signify is the World Leader in Lighting

We provide high-quality energy efficient lighting products, systems and services

## Light sources



## Luminaires



## Systems and Services



**No. 1**

Conventional.  
LED, Connected

**€7bn**

sales in 2017,  
~ 75%  
professional

**32,000**

people in 70  
countries

**No. 1**

Industry leader  
Dow Jones  
Sustainability Index

# Signify Proudly Markets the Best Lighting Brands in the World

**PHILIPS**



Our global brand in professional and consumer lighting

**interact**



Our Internet of Things platform and connected lighting systems

**MODULAR**  
LIGHTING —  
INSTRUMENTS



Our international brand in architectural lighting

**LUCE  
PLAN**



Our high-end lighting brand made in Italy

# Before



# After



**Harsha Banavara, CSSLP, Security+, CIPP, ...**  
Cybersecurity Technical Policy Manager  
Standards & Regulations Americas  
Burlington, MA





Egham, U.K., February 7, 2017

[View All Press Releases](#)

**Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016**

STAMFORD, Conn., March 21, 2018

[View All Press Releases](#)

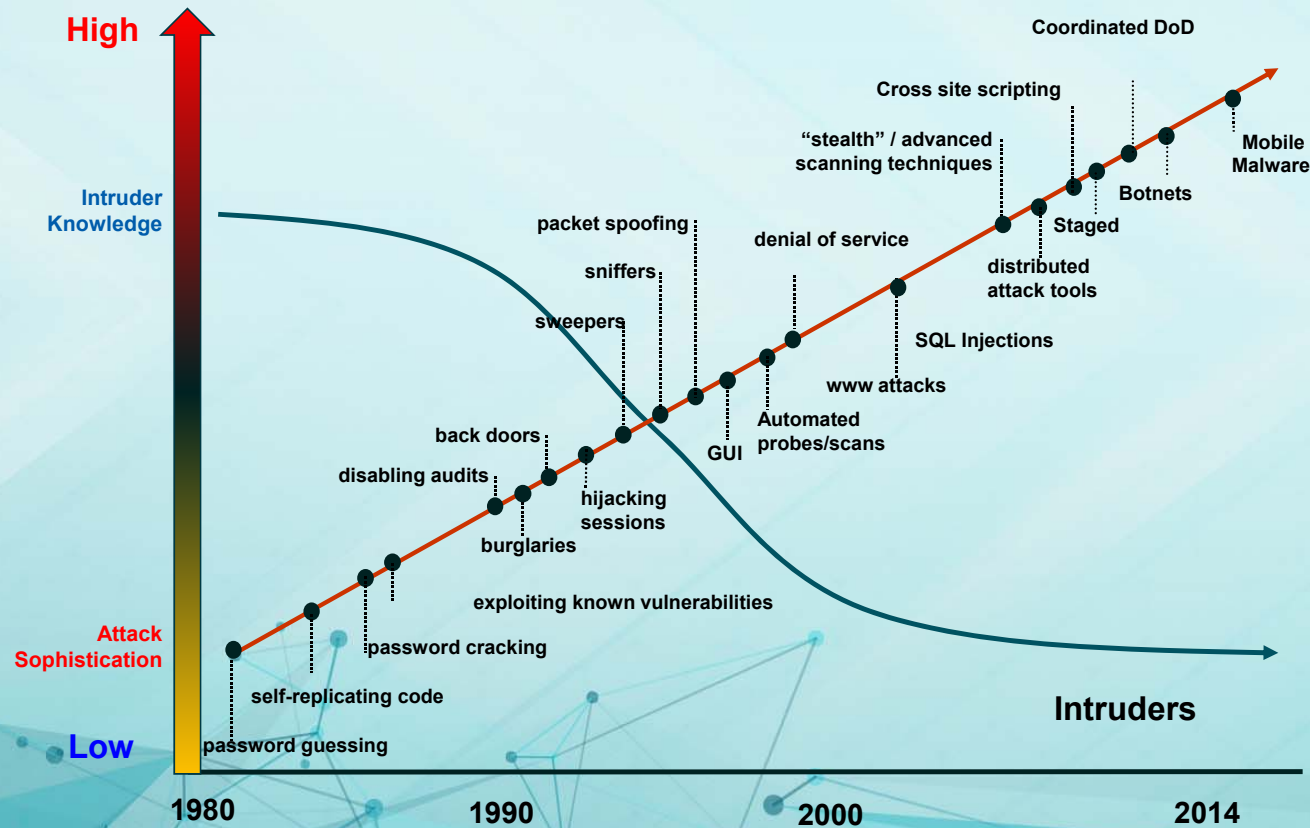
**Gartner Says Worldwide IoT Security Spending Will Reach \$1.5 Billion in 2018**

*By 2021, Regulatory Compliance Will Become the Prime Influencer for IoT Security Uptake*



- Cybersecurity and Privacy standards & regulations are rapidly becoming a priority with the ever increasing number of connected systems and the risk of hackers, making it a major security concern for individuals, companies and governments.

# Attack Sophistication vs. Intruder Technical Knowledge



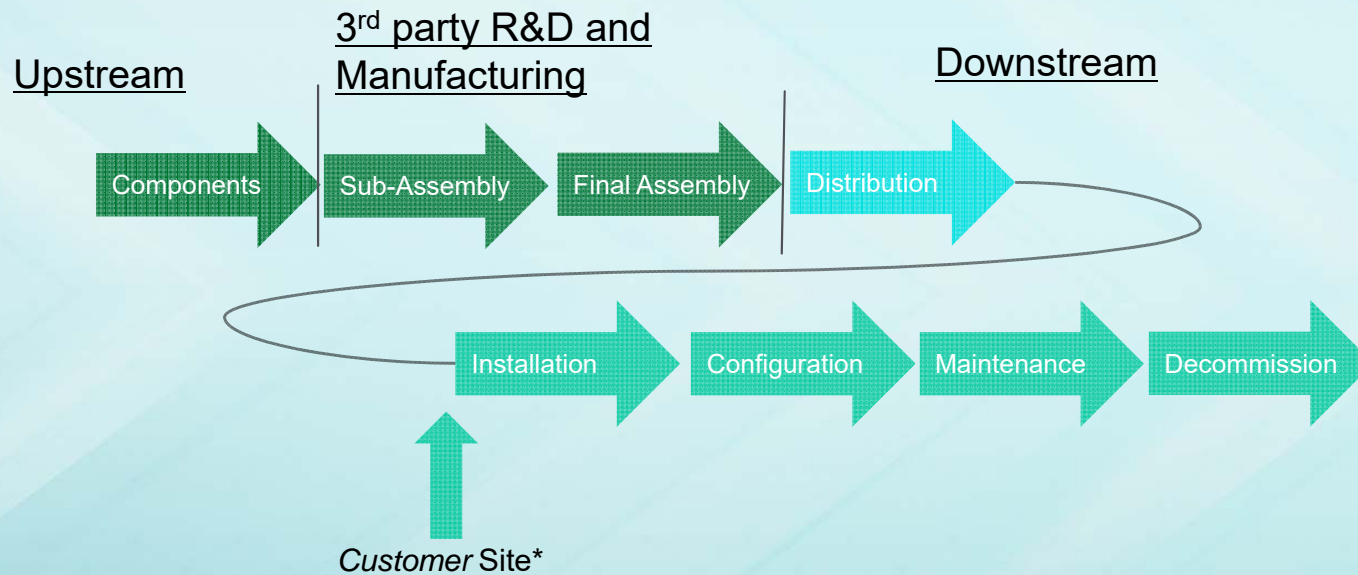
October 4, 2018, 5:00 AM EDT

# The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

- Nested on the servers' motherboards, the testers found a tiny microchip, not much bigger than a grain of rice, that wasn't part of the boards' original design.
- Investigators determined that the chips allowed the attackers to create a stealth doorway into any network that included the altered machines.
- Investigators found that the chips had been inserted at factories run by manufacturing subcontractors in China.

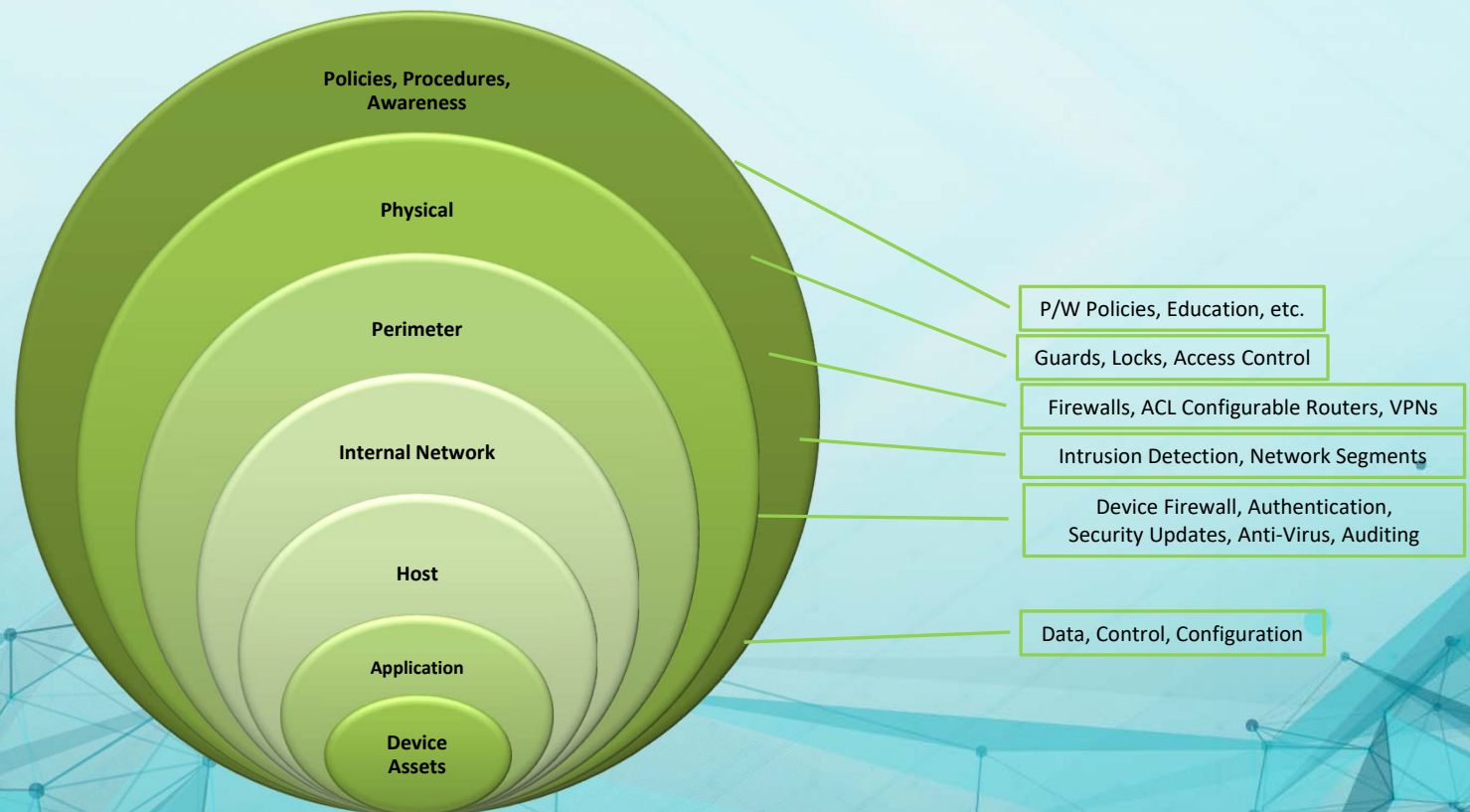
# Supply Chain and its complexities





# Defense in Depth

- Defense in Depth manages risk with diverse defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach.



# CTPAT

- Started right after 9/11.
- When an entity joins CTPAT, an agreement is made to work with CBP to protect the supply chain, identify security gaps, and implement specific security measures and best practices.
- The first step is for the company to review the CTPAT Minimum Security Criteria for their business entity to determine eligibility for the program.
- The second step is for the company to submit a basic application via the CTPAT Portal system and to agree to voluntarily participate.
- The third step is for the company to complete a supply chain security profile.
- The security profile explains how the company is meeting CTPAT's minimum security criteria.
- In order to do this, the company should have already conducted a risk assessment.

CTPAT: Customs Trade Partnership  
Against Terrorism





# Authorised Economic Operator (AEO)

- The program, which aims to enhance international supply chain security and to facilitate legitimate trade, is open to all supply chain actors. It covers economic operators authorized for customs simplification (AEOC), security and safety (AEOS) or a combination of the two.

Conditions and criteria	AEOC	AEOS
Compliance with customs legislation and taxation rules and absence of criminal offences related to the economic activity.	X	X
Appropriate record keeping.	X	X
Financial solvency.	X	X
Proven practical standards of competence or professional qualifications.	X	
Appropriate security and safety measures.		X

The AEO status granted by one Member State is recognised by the customs authorities in all Member States (Article 38 (4) UCC).

# TAPA Standards



- Facility Security Requirements (FSR) set minimum standards for security and industry best practices for facilities storing and handling HVTT assets.
- They also specify the proper methods for maintaining those standards. TAPA members who purchase supply chain services should choose suppliers who meet or exceed TAPA's FSR certification requirements.
- FSR certifications apply to individual facilities, not entire companies.
- Trucking Security Requirements (TSR) set minimum standards of security and best practices for over-the-road carriers of HVTT goods.

EXPERT GROUP TO DELIVER RECOMMENDATIONS ON NEW TAPA  
CYBER SECURITY STANDARD BY END OF 2018



# Threat Intelligence

- Resilience360 Risk Assessment
- Resilience360 Incident Monitoring
  
- Provide a comprehensive solution for mitigating the risks associated with theft, spoilage, counterfeiting, diversion, pilferage, and other cargo security threats.
- Used for monitoring, alerting and recovery.



# Standards/Guidelines/ Whitepapers

- ISO 28000
- ISO 20243
- NIST 800-161
- ISO 270XX series
- NIST IR 7622
- IEC 62443 series
- Whitepapers – DOE, UTC
- Guideline - NEMA



**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce





# Few Other Things We've Been Doing

- Creating Awareness
- Physical Security and Access Control
- Sharing Security Expertise
- SDL – Product and Process Requirements
- Contractual Agreements with Suppliers

# Conclusion

- Do things you can sustain

25-Jan-2018 9:02 PM

## Southwest Airlines marks 45th consecutive year of profitability

**Southwest Airlines** CEO Gary Kelly stated (25-Jan-2018) the carrier's "strong" results in the Dec-2017 quarter "capped another year of extraordinary achievements, including 45 straight years of profitability". Mr Kelly said the carrier, which reported net profit of USD1.9 billion in 4Q2018 and annual net profit of USD3.5 billion, experienced "strong profits, cash flow, and financial position" in 2017, enabling the carrier to deploy capital wisely and sustain high returns on invested capital. He said the carrier made significant progress "modernising our fleet, investing in technology and facilities, and returning value in excess of our free cash flow". The carrier returned approximately USD1.6 billion in share repurchases. [[more - original PR](#)]

- This provides a safety margin for growth.
- Does not take a huge hit on cost.
- Willingness of upper management to set an upper bound for growth.



# Compliance vs Security

