Can Developers Benefit From Regulatory Compliance?

Maria C. Horton
Founder, CEO
CISSP-ISSMP, Cloud Essentials, IAM

Who We Are

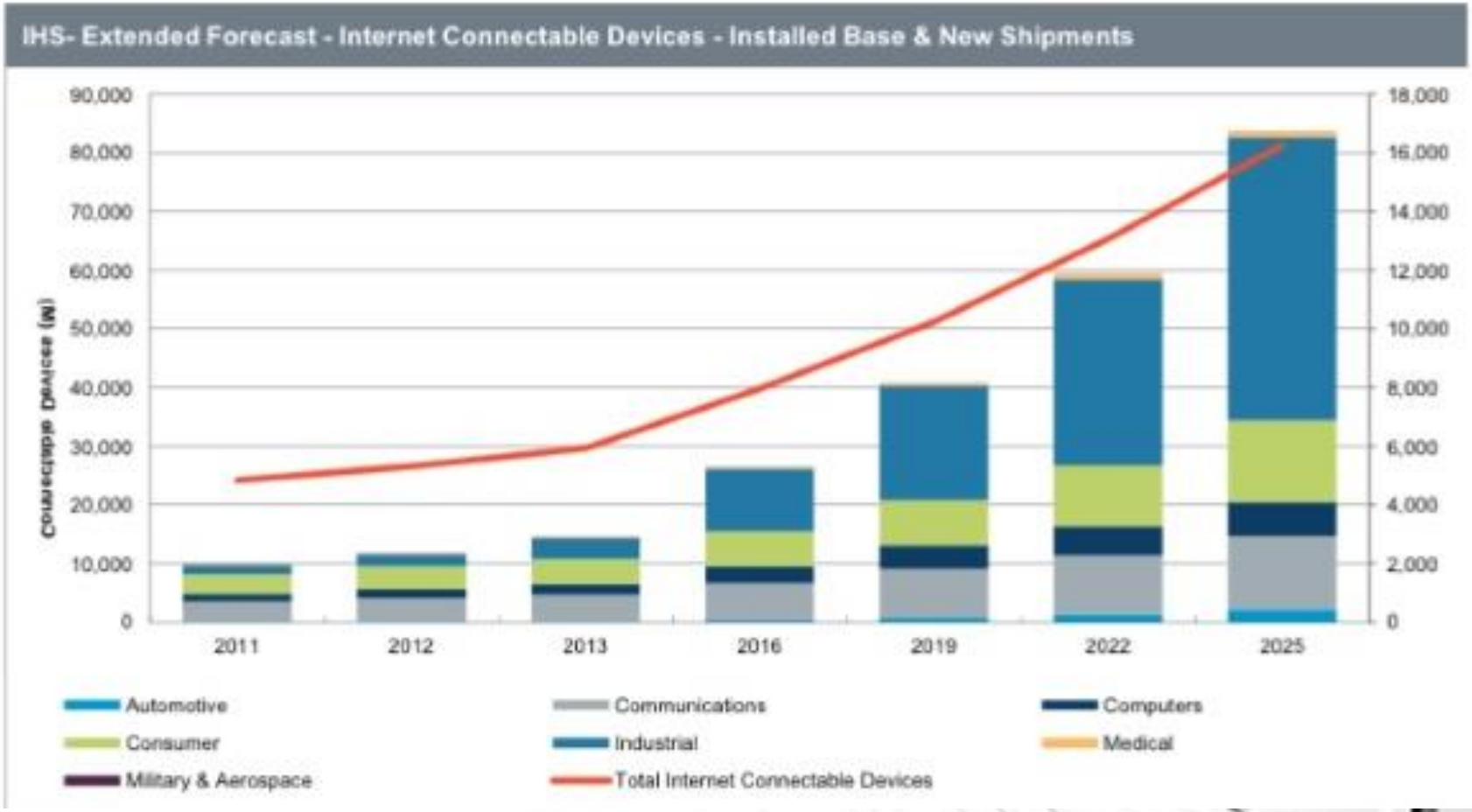
- EmeSec Incorporated
  - Founded in 2003
  - Core services are in cloud, security, and engineering
  - Compliance consulting
- An accredited FedRAMP 3PAO
- Hold 4 ISO certifications:
  - ISO 9001: 2008
  - ISO/IEC 20000-1: 2011
  - ISO/IEC 27001: 2013
  - ISO/IEC 17020: 2012

Today's Learning Objectives

- Attendees will explore, learn and discuss:
  - Cybersecurity planning and liability risks that may be better handled in development for cloud services and IoT solutions
  - The direct and indirect implications of CUI and GDPR on functional requirements
  - Specific data protections, data privacy and and PII considerations

IoT Market 2011 to 2025

- By 2020, 34B connected devices of which 24B are IoT*
- Market value is estimated at $883B in 2021
  - Compounded Annual Growth Rate of 23%



*Business Insider

Why focus on DevOps Compliance?

- Cloud, IoT, hybrid, and traditional environments now converged
  - In-house and purchased code libraries and designs
- New software requirements
  - Demonstrable security and privacy controls
  - Holistic review of supply chain, communications, integration ,etc.
  - NIST SP 800-160
    - Focus on systems of systems and critical assets
- Evidence of software code analysis needed for compliance (and often times for purchase)
  - NIST SP 800-53, Rev. 4
  - FedRAMP

Regulatory Compliance

Regulations

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- Controlled Unclassified Information (CUI)
  - FAR 52.204.21
  - DFARS 252.204.7012
- Federal Risk Authorization and Management Program (FedRAMP)
  - Standardizes cloud security controls and control enhancements

Implications

- EU GDPR
  - Strengthens and unifies data protection for EU citizens
  - Requires specific handling for export of personal data outside of the EU
- CUI
  - Standardizes the protections and markings of government information including dissemination
  - Applies to all “Covered Contractor” systems
  - Imposes a set of Basic controls

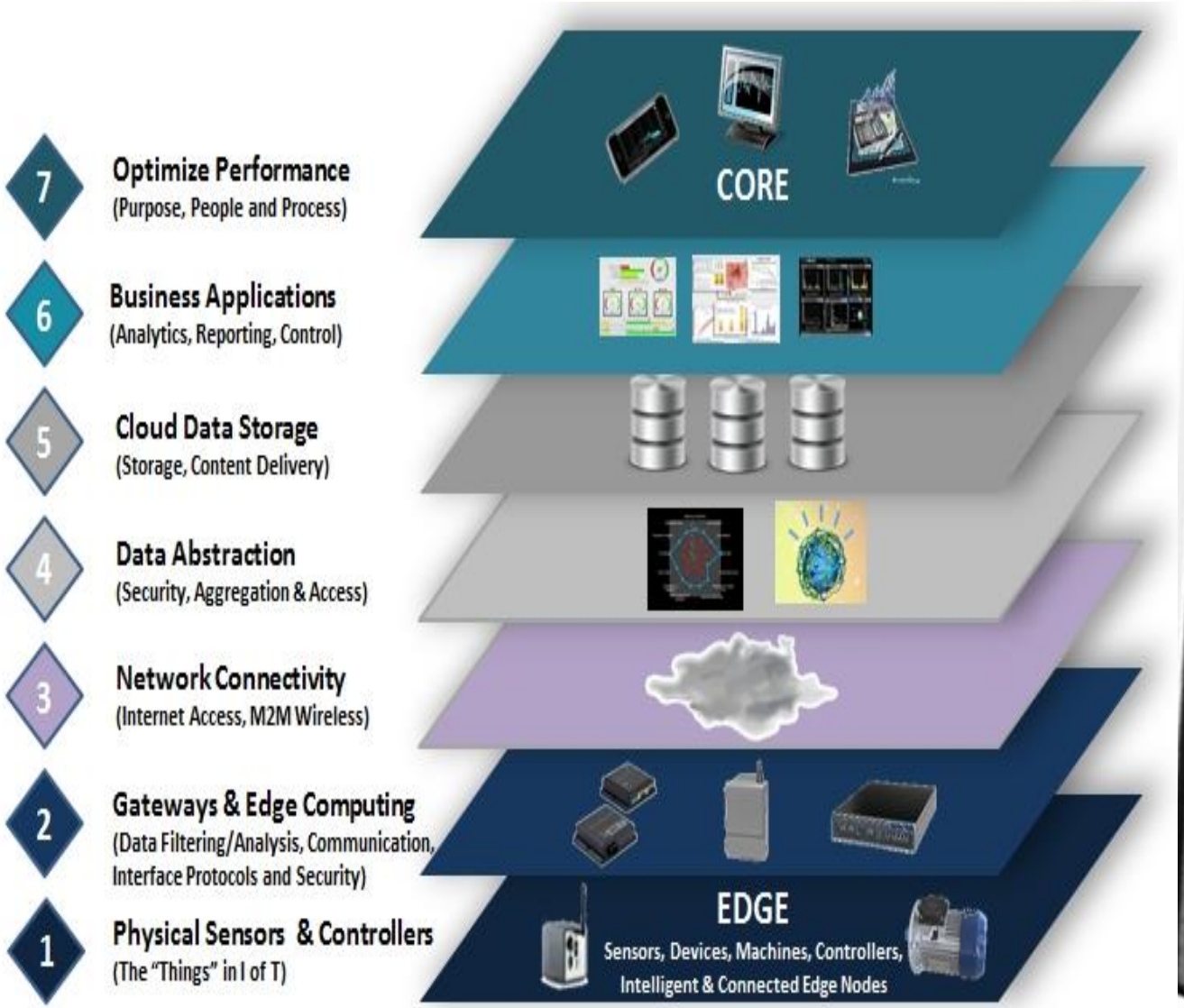
Compliance Risks in Dev Ops

- Understanding the Complexity
  - IoT exists outside of physical security perimeter
  - Vulnerability management practices are new
  - Changing requirements
  - Data decision points reflect potential risks
    - Too much data
    - Privacy and confidence
- Automated development processes
  - Virtual and physical
  - Artificial intelligence
  - Incident response

http://www.businessinsider.com/internet-of-things-security-privacy-2016-8

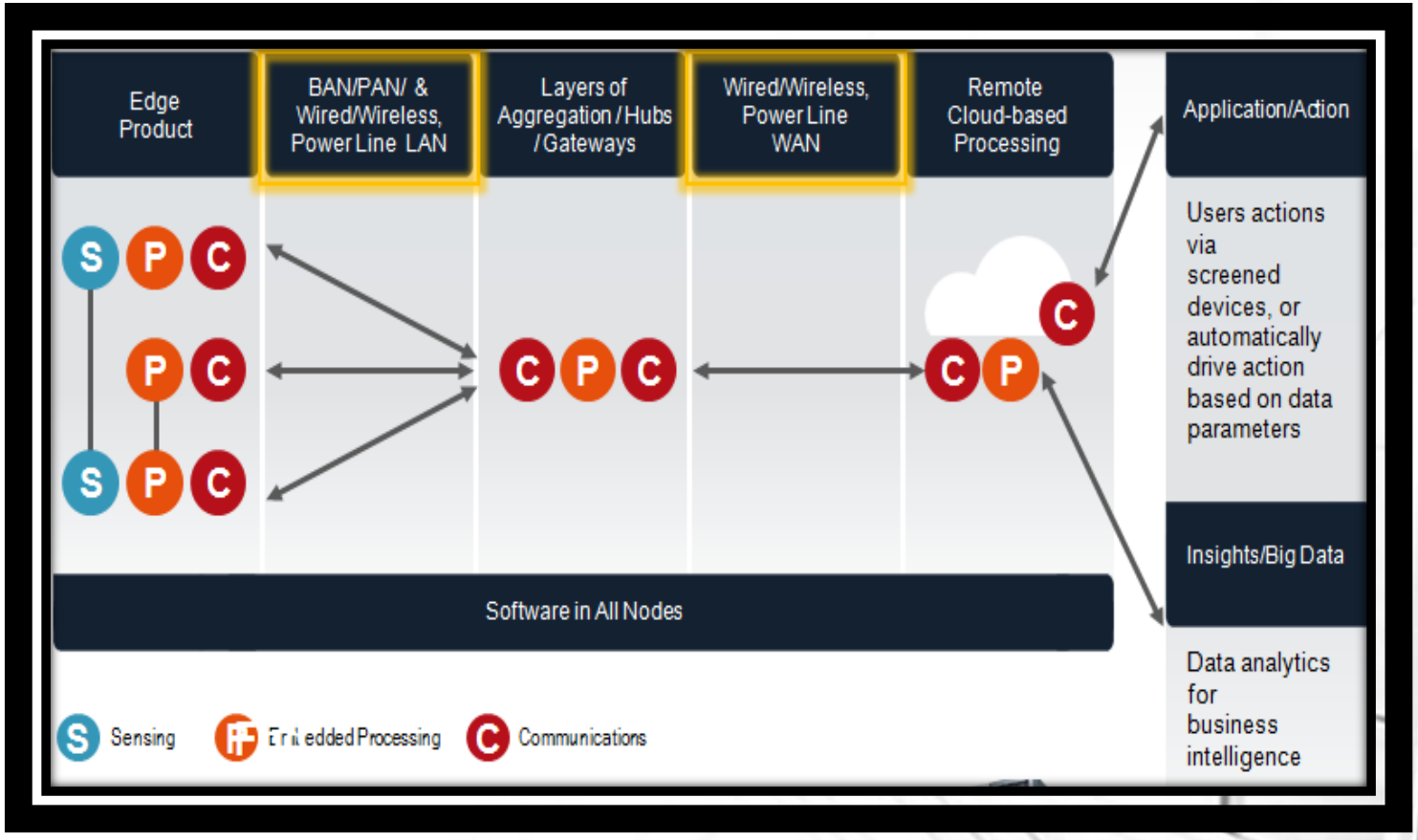
Cloud & IoT Threats

- Enlarged information supply chain in multiple directions
- Greater Numbers of interfaces and interconnections
  - Data ownership issues
- New privacy concerns
  - Global regulations
  - Data leakage responses
    - How is it defined?



Security Compliance from the Fog Inward

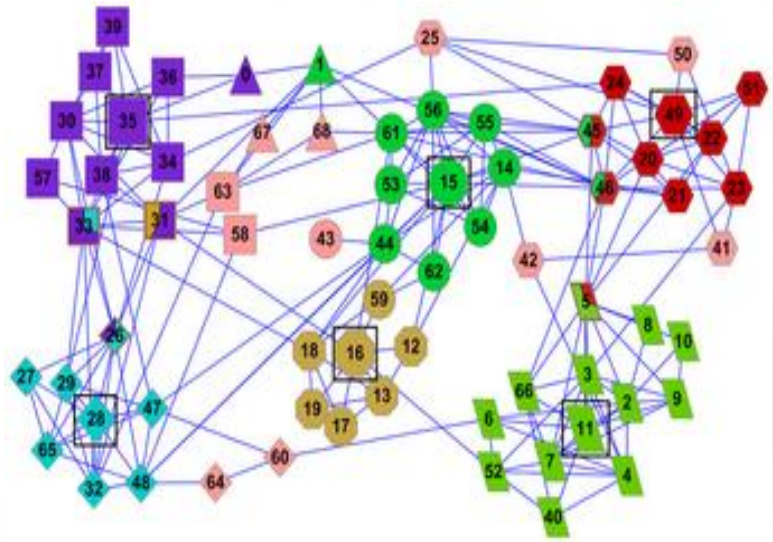
- Edge Issues
  - Sensing & Processing
- Transaction Issues
  - Communications
  - Further Processing
- Centralized Considerations
  - Remote (Cloud) Communications
    - Automated Device Actions
    - User Actions
  - Data Analytics & Processing



How are these documented for compliance? And maintained?

Compliance → Due Diligence

- Liability is the reasonable care taken to avoid harm
  - Compliance describes the degree of effort required by law or industry standard
  - Due diligence is the information needed to assess risk accurately
- IoT third and fourth party relationships create extended liability
  - See CUI, DFARS requirements
- **Supply chain protection is the hottest area of risk management**



DevOps Compliance Benefits

- Competitive advantages
  - High trust
  - Increased marketability and resale of code & code libraries
  - Enhanced accessibility into environments
    - Federal market access
    - Ability to support Federal market as third party suppliers (PaaS, SaaS)
- Reduced liabilities
  - In extended performance of sensors & gateways
  - Related to data ownership

Recommendations

- Seek Available Guidance (NIST, IIoT, ISO)
- Development capabilities & design
  - Encryption
  - IoT configurations & technology refresh
  - Device authentication/tightly mapped interconnections
  - Consider how data flows – including segregation of networks
    - Understand them for reconfiguration as appropriate
- Incorporate Compliance, IT, and Marketing into design and discussions
  - Consider scope, depth and rigor of design

Continue the Conversation

- @EmeSec
- @mariahorton
- Phone: 703.429.4492/4491
- Email: info@emesec.net

emēsec™