The Next Wave: The Internet of Things and Security

F. Christian Byrnes
Twitter: @cbyrnes
Let's Get the Big Story Out of the Way Right Now

WE'RE ALL GONNA DIE

... but probably not from cyber security compromise
Digital Business Moment: Renting a Car
1974
Customer Experience:
Call three rental companies on the phone; wait on hold, eventually find one with a car available. On check-in fill out reams of paperwork with a dozen signatures. Insurance is included in the rental automatically. If an accident occurs call for a tow truck and the rental company brings out a replacement car. When returning wait on line to process car back in.

IT experience:

Risks:
Lost business due to incorrect inventory. Unhappy customers due to long waits in line, doing paperwork and then eventually getting a car.
Digital Business Moment: Renting a Car
1994
**Customer Experience:**
Still call on the phone, but now the agent has a terminal with past customer profiles and a more accurate inventory. On check-in forms are printed partially filled out. A few signatures and initials suffice. Accident: no change. Return: no change.

**IT experience:**
Mainframe OLTP system handles basic transactions and updates inventory.

**Risks:**
Loss of leased communications lines stops reservations. Check-in agent has fall-back to paper as option. Re-entering manual transaction can take days, creating old inventory problems. Most serious risk is database corruption which can take up to a week to repair.
Customer Experience:
Reservation made via the web. Fast, clean, minimal effort. No check-in; go straight to car, even pick your car. Show license on exit from parking lot. Insurance costs extra; post-accident services slow to non-existent. On return wait for agent to come to the car and check you out. Email confirmations followed by endless marketing emails.

IT experience:
Mobile, networking, cloud and social support built on reliable infrastructure.

Risks:
DDOS, client data loss due to security breach, fallback to paper virtually impossible, in part due to reduced staffing that improved profitability. Reputational risk, negative social reviews,
Digital Business Moment: Renting a Car

2034
Customer Experience:
“Siri, I need a car in Dubai next week.”
Siri: “Human driver or self driving?”
Siri checks for airline tickets, arranges car according to preference profile.
Pickup: walk to car and drive away.
Drop-off: Get out of car and walk away.

IT experience:
Hundreds of sensors in the car and in the lot. Physical security, car maintenance, etc. Robots service the car in preparation for the next renter.

Risks:
Your competitors want your sensor data as well as your client data. Some geographies mandate human drivers; others do not allow them. Cyber-gangs and corporate fiefdoms.
Did I say 2034?

We do not have that long.
SECURITY SCENARIO

2020

The External Environment
FORCE 1:
Target

Enterprise ← Enterprise
Individual → Individual
The Third Industrial Revolution

- The first industrial revolution – 1780-1850
- The second industrial revolution – 1870-1930
- The third industrial revolution – 1940-2025(?)
  - In Germany the result is called “Business 3.0”

If history provides any guidance:

Industrial revolutions end with a game changer.

Of the five pillars of a stable society, prosperity is always threatened at the end of an industrial revolution. That threat leads to major changes in the economy.
The Nexus of Forces is a game changer

Mobile, social and cloud create massive data and shift control away from the enterprise.

This is the largest change since 1966.

Its next phase technical implementation is embodied in the Internet of Things (IoT).
The Internet of Things: 15 Billion or One Trillion Things by 2020?

- Smart Meters
- Light Bulbs
- Smart Hubs
Internet of Things Hype Cycle, 2014

- **Innovation Trigger**
- **Peak of Inflated Expectations**
- **Trough of Disillusionment**
- **Slope of Enlightenment**
- **Plateau of Productivity**

**Plateau will be reached in:**
- less than 2 years
- 2 to 5 years
- 5 to 10 years
- more than 10 years
- obsolete before plateau

As of July 2014
What Can We Learn From “Legacy” IoT?

Over the past five years changes in
- Capability
- Deployment
- Connection
- External environment

of operational technology have forced changes within enterprises to secure OT.

What can we learn from them as we approach securing the Internet of Things?
Hype Cycle for Operational Technology

expectations

- Intelligent Lighting
- Big Data
- Operational Technologies for Government
- Networking IT and OT
- UAS for Business
- IT/OT Convergence in Life Sciences
- IT/OT Integration
- IT/OT Impact on EA
- IT/OT Alignment
- Data Science
- High-Performance Message Infrastructure
- IT/OT Convergence in Manufacturing
- IT/OT Skilled Workforce
- Decisions and Recommendations as a Service
- ITAM Processes for OT
- Exploiting Sensor Grids
- Lidar
- Enterprise Manufacturing Intelligence
- Vehicle-to-Infrastructure Communications
- Enhanced Network Delivery
- Remote Diagnostics
- Public Telematics and ITS
- Intelligent Electronic Devices
- Process Control and Automation
- Vehicle-to-Vehicle Communications
- Machine-to-Machine Communication Services
- Operational Technology Platform Convergence
- Real-Time Infrastructure
- Hardware Reconfigurable Devices
- Asset Performance Management
- Operations Intelligence
- Open SCADA
- Complex-Event Processing
- Facilities Energy Management
- System Engineering Software
- Integrated and Open Building Automation and Control Systems
- Event-Driven Architecture
- Commercial Telematics
- Process Data Historians
- Fleet Vehicle Tracking

As of July 2013

Innovation Trigger  Peak of Inflated Expectations  Trough of Disillusionment  Slope of Enlightenment  Plateau of Productivity

Plateau will be reached in:
- ○ less than 2 years
- ○ 2 to 5 years
- ○ 5 to 10 years
- △ more than 10 years
- ⚫ obsolete before plateau

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved.

G00246894
Operational Technology Exists in All Industries …

Operational technology is technology used in the running of a business that senses or controls physical assets.
The Things of OT & the Lesson of Target

Native IP Equipment

Legacy SCADA

IP Connectors
# Strategic Planning Assumption

By 2017, half of global enterprises responsible for OT will have integrated IT/OT cybersecurity planning practices.

## Reasons why SPA will be true:
- The budget for increasing complexity in IT and OT security requires cost savings moves.
- IT security technology is being applied increasingly to OT security problems.
- OT is the first of several integration phases for security and risk in the enterprise — stay tuned for physical security and the securing the Internet of Things.

## Reasons why SPA may be false:
- Differences in mission, culture and process will keep IT and OT apart longer.
- Progress delays in technical standards for OT security will slow market adoption.
- Skills shortages will take longer to overcome.
Part 3

How can organizations prepare for the IoT?
Understand your new role in the IoT security universe

Cybersecurity

Information Security

IT Security

OT Security

Physical Security

IoT Security

Digital Security
Map the role of IoT security into the 2020 security scenario

- **AUTHORITY**
  - Coalition Rule
  - Neighborhood Watch

- **TARGET**
  - Regulated Risk
  - Controlling Parent

- **Enterprise**

- **Individual**

- **Tribal**

- **Monolithic**

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved.
Embrace secure IoT practice as part of the new digital workplace
Ensure your IoT strategy has privacy and trust as foundations.

Privacy
Buy It and Give Control to Customer

Digital Security
Build It

Trust
Earn It

Great products, services, experiences
Ensure that IoT and cloud security are part of the same framework
Leverage Written Guidance, Frameworks and Methodologies

- ISO/IEC 27001
- IEC 62443/ISA-99
- NIST SP Guides
- ES-ISAC
- DHS-TSA

- DHS-CFAT
- NERC CIP
- RG 5.71

- CERT
- CPNI
- ENISA
- SANS
- UCA

- USA NIST Cybersecurity Framework
- Gartner EISA Framework
- Langner RIPE Framework
- ENISA Protecting ICS

- ISACA SCADA Cybersecurity Framework
- NSA Framework for Assessing and Improving Security Posture for ICS
- ENISA Good Practices for an EU ICS
- Testing Coordination Capability

Strategy and Governance Management and Operations
Organizations Must Address the Security Skills Shortfall

Relationship and Relative Availability

IT

OT Security

OT Engineering

Source: Protecting Industrial Control Systems from Electronic Threats, by Joseph Weiss

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved.
Security Architecture Becomes Critical

- Identify the constituencies – in the IoT constituencies are not just people
- Determine the number of different security baselines (2-5)
- Define baselines as control sets
- Map the constituencies, their boundaries and their shared functional requirements
- Define the connection requirements between constituencies – specify proxies to support them with filtering and monitoring controls as appropriate
- Design a network architecture that creates zones, each at or above a defined baseline, to contain each constituency.
Deploy an Adaptive Protection Architecture

- Threat Intelligence
- Community Intelligence
- Vendor Labs
- Policy
- Vulnerability Insights
- Context

Next-generation security protection platforms

Continuous Monitoring  Embedded Analytics
Design for new security challenges in a world of ‘zones’

“Back office”

The World
Recommendations

✓ Engage your business — make sure you know how they are developing IoT-related business initiatives.

✓ Actively increase awareness to the business of IoT security and risk implications and impact.

✓ Plug into industry initiatives and standards development around secure embedded systems and M2M communications.

✓ Establish education and training for selected security planners in IoT principles and concepts.
Recommended Gartner Research

- **Forecast: The Internet of Things, Worldwide**
  Peter Middleton, Peter Kjeldsen, and Jim Tully (G00259115)

- **What Securing the Internet of Things Means for CISOs**
  Earl Perkins (G00259020)

- **Cool Vendors in the Internet of Things, 2014**
  Alfonso Velosa and others (G00262623)

- **The Impact of the Internet of Things on Data Centers**
  Fabrizio Biscotti and others (G00250562)

- **Hype Cycle for the Internet of Things**
  Hung LeHong (G00252763)

For more information, stop by Gartner Research Zone.