Panel S2: Digital Health Revolution Improving Society

Cyber Security for Network-Connectable Devices

Joe Jarzombek, CSSLP, PMP
Global Manager, Software Supply Chain Management
Synopsys Software Integrity Group

Previously

Director, Software and Supply Chain Assurance
U.S. Department of Homeland Security
& Deputy Director, Information Assurance
OCIO, U.S. Department of Defense

Joe.Jarzombek@synopsys.com
+1 (703) 627-4644
SYNOPSYS®
Silicon to Software™

Sept 19, 2016

An ever-more connected world . . .

Goods & Services
- Track materials
- Speed distribution
- Product feedback

Homes
- Utilities control
- Security monitoring
- Structure integrity

Environment
- Pollution checks
- Resource status
- Water monitoring

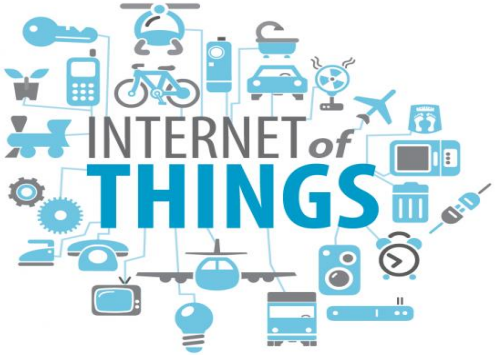
Communities
- Traffic status
- Pollution alerts
- Infrastructure checks

People
- Wellness monitoring
- Medical case management
- Social needs

SYNOPSYS®

Growing Concern with Internet of Things (IoT)

- Lax security for the growing number of IoT embedded devices in appliances, industrial applications, vehicles, TVs, smart homes, smart cities, healthcare, medical devices, etc.

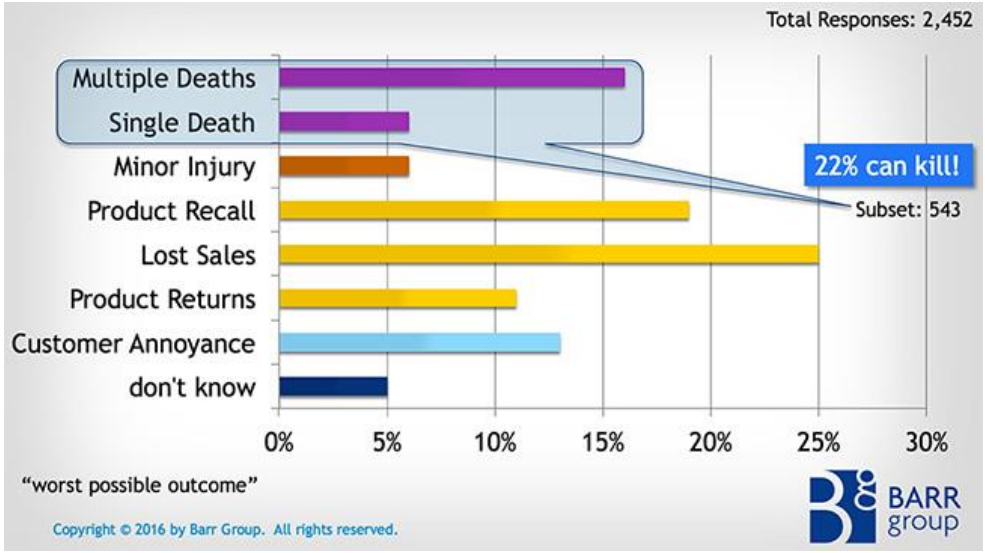


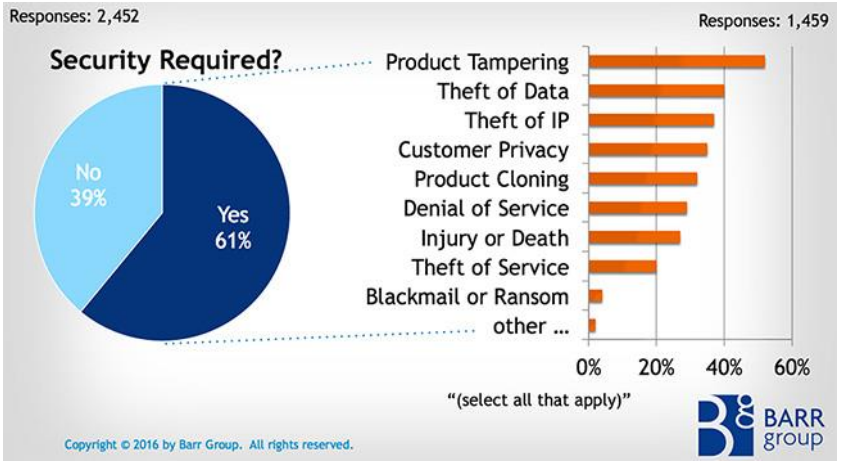
  - Sloppy manufacturing ‘hygiene’ is compromising privacy, safety and security – incurring risks for faster time to market
  - IoT risks provide source vectors for privacy/financial exploitation
  - IoT risks range from virtual harm to physical harm
    - Cyber exploitation with physical consequences;
    - Increased risk of bodily harm from hacked devices

Safety/Security Risks with IOT embedded systems

Engineering Community concerns:

- Poorly designed embedded devices can kill;
- Security is not taken seriously enough;
- Proactive techniques for increasing safety and security are used less often than they should be.





Barr Group: "Industry is not taking safety & security seriously enough"

Based on results of survey of more than 2400 engineers worldwide to better understand the state of safety- and security-aware embedded systems design around the world (Feb 2016).

Shifting Business Concerns: Increased Software Liability

1980's 1990's 2000's 2010's

Quality

Quality / Security

Quality / Security / Safety & Privacy

Financial Liability

SYNOPSYS®

90%

of all reported security incidents result from exploits against defects in software

SYNOPSYS®

Have Healthcare Network-Connectible Devices been Tested?

- **for Exploitable Weaknesses (CWEs)?**
  - If suppliers do not mitigate exploitable weaknesses or flaws in products (which are difficult for users to mitigate), then those weaknesses represent vectors of future of exploitation and ‘zero day’ vulnerabilities.
- **for Known Vulnerabilities (CVEs)?**
  - If suppliers cannot mitigate known vulnerabilities prior to delivery and use, then what level of confidence can anyone have that patching and reconfiguring will be sufficient or timely to mitigate exploitation?
- **for Malware (MAEC)?**
  - If suppliers do not check that the software they deliver does not have malware (typically signature-based), then users and using enterprises are at risk of whitelisting the malware.

CVE, CWE, MAEC & CAPEC are part of the ITU-T CYBEX 1500 series

Underwriters Labs Cybersecurity Assurance Program:
proving consumer protection for network-connectable devices

- UL Cybersecurity Assurance Program (**UL CAP**) will be **Product Oriented & Industry Specific** with these goals:
  - Reduce software vulnerabilities
  - Reduce weaknesses, minimize exploitation
  - Address known malware
  - Increase security awareness
- Product service offerings apply to:
  - Connectable Products
  - Products Eco-Systems
  - Products System Integration
  - Critical IT Infrastructure Integration

UL 2900-3: Organizational Process

UL 2900-2-1, -2-2:
Industry Specific Requirements
(for ICS & Medical Devices)

UL 2900-1: CAP General Requirements/

SYNOPSYS®

Digital Health Revolution Improving Society

Cyber Security for Network-Connectable Devices

Consumers of software-reliant IoT systems should demand safety and security be ‘built in’ as a responsibility of suppliers.

Health-care providers’ buying can send a strong market signal for cybersecurity in network-connectable devices.

[sample procurement language is available]

Panel S2: Digital Health Revolution Improving Society

Cyber Security for Network-Connectable Devices

Joe Jarzombek, CSSLP, PMP
Global Manager, Software Supply Chain Management
Synopsys Software Integrity Group

Previously

Director, Software and Supply Chain Assurance
U.S. Department of Homeland Security
& Deputy Director, Information Assurance
OCIO, U.S. Department of Defense

Joe.Jarzombek@synopsys.com
+1 (703) 627-4644
SYNOPSYS®
Silicon to Software™

Sept 19, 2016