Global Forum
Shaping the future 2017

DIGITALIZATION:
INTELLIGENT PATHWAYS

SYNOPSYS®
Silicon to Software™

Software Supply Chain Management:
Enabling Cybersecurity Assurance for Network-Connectable Medical Devices

Joe Jarzombek, CSSLP, PMP
Global Manager, Software Supply Chain Solutions
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

Software Supply Chain Risk Management:

Technological Advances in Network-Connectable Medical Devices and Systems

Global Forum
Shaping the future

Before

Devices were physically connected to patients

Data obtained from devices was stored locally on paper

Devices were physical products

Care was hand-administered at the health care location

Physical access was needed to view health data

Now

Devices are connected wirelessly to patients and other devices

Data obtained from devices are stored in the cloud

Devices include software and databases of health information

Care is available to patients in the palm of their hand through apps

Health data can be accessed anywhere on earth

SYNOPSYS®

Software Supply Chain Risk Management:

Network-Connectable Medical Devices are Source Vectors for Exploitation

Sloppy manufacturing ‘hygiene’ is compromising privacy, safety/security;

– IoT risks provide vectors for exploitation of privacy & financial data

– IoT risks range from virtual harm to physical harm

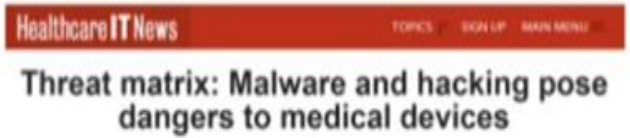
Medical devices & heath data systems provide hackers with vital information:

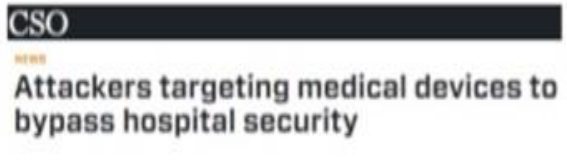
-- Lack of timely software updates/patches

-- Compromised devices infecting other systems and exposing patients to increased risks attributable to cyber exploitation

Software Supply Chain Risk Management:

Healthcare Concerns for Network-Connectable Medical Devices and Systems





Lax medical device security needs urgent action

Hospital Drug Pump Can Be Hacked Through Network, FDA Warns

Key points:

1. **Connected medical end-points**
2. **One stop treasure-trove of data**
3. **Cost of a data breach**
4. **Loss of reputation**
5. **Cyber exploitation -> physical harm**

FDA Warning Wire: Faulty Devices Used in Patients

Software Supply Chain Risk Management:

Healthcare Concerns for Network-Connectable Medical Devices and Systems

Ponemon Institute research reveals risks to medical devices and why clinicians & patients are at risk:

- Medical devices are very difficult to secure
- Accountability for medical device security is lacking
- Mobile devices usage is affecting security posture in healthcare
- Medical device security practices are not the most effective
- Testing of medical devices rarely occurs

https://www.synopsys.com/blogs/software-security/synopsys-report-finds-medical-device-industry-vulnerable/

SYNOPSYS®

Software Supply Chain Risk Management:

Healthcare Concerns for Network-Connectable Medical Devices and Systems

Ponemon Institute research reveals risks to medical devices and why clinicians & patients are at risk:

"How likely is an attack on one or more medical devices built or in use by your organization?"

- 67% of *device makers* believe attack is likely
- 56% of *device users* believe attack is likely

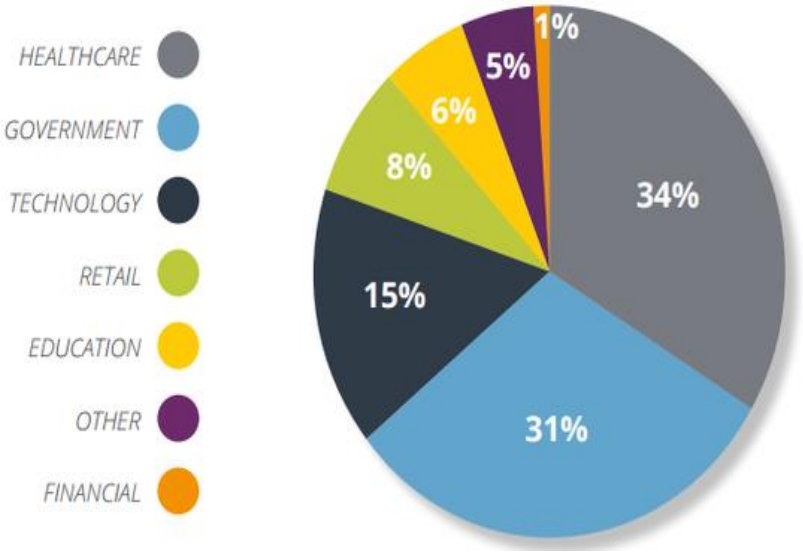
Patients have already suffered adverse events and attacks:

- 38% of device users are aware of inappropriate therapy or treatment due to an insecure medical device
- 37% - an attacker took control of the device

Software Supply Chain Risk Management:

Need for Cybersecurity Assurance: Healthcare is target-rich for breaches

Number of Records Breached by Industry:



Cyber intrusions will likely increase due to:

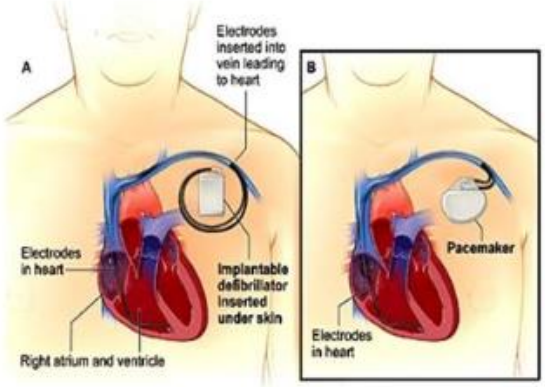
- Higher financial payout for medical records in black market
- Mandatory transition from paper to electronic health records (EHR)
- Lax cyber security standards

SYNOPSYS®

Software Supply Chain Risk Management:

Examples of Hacking Network-Connectable Medical Devices

Pacemaker/Implantable Cardioverter Defibrillator (ICD)



WIRED

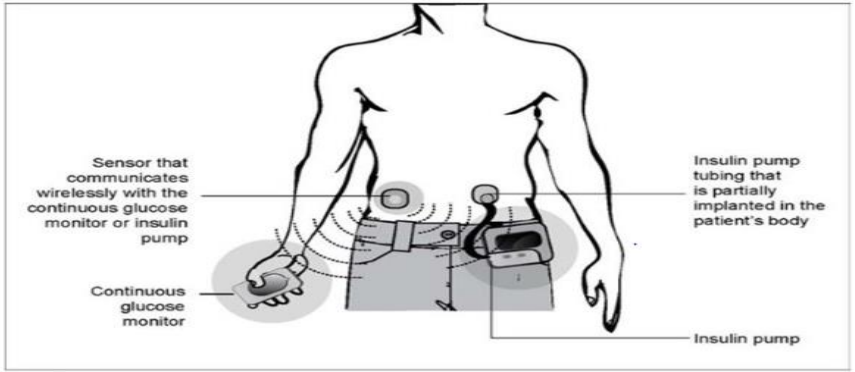
HACKER CAN SEND FATAL DOSE TO HOSPITAL DRUG PUMPS

"We are potentially looking at a worm with the ability to commit mass murder," Barnaby Jack added.

...the software I developed allows the shutting off of the pacemaker or ICD, reading and writing to the memory of the device and, in the case of ICDs, it allows the delivering of a high voltage shock of up to 830 volts.

Barnaby Jack

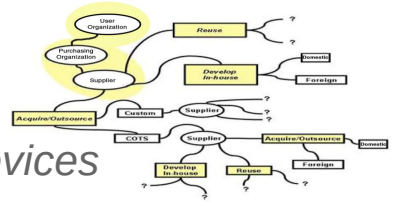
Continuous Glucose Monitoring System and Insulin Pump



SYNOPSYS®

Software supply chain risk management

Mitigating third-party risks attributable to exploitable software in medical devices



Increased risk from supply chain due to:

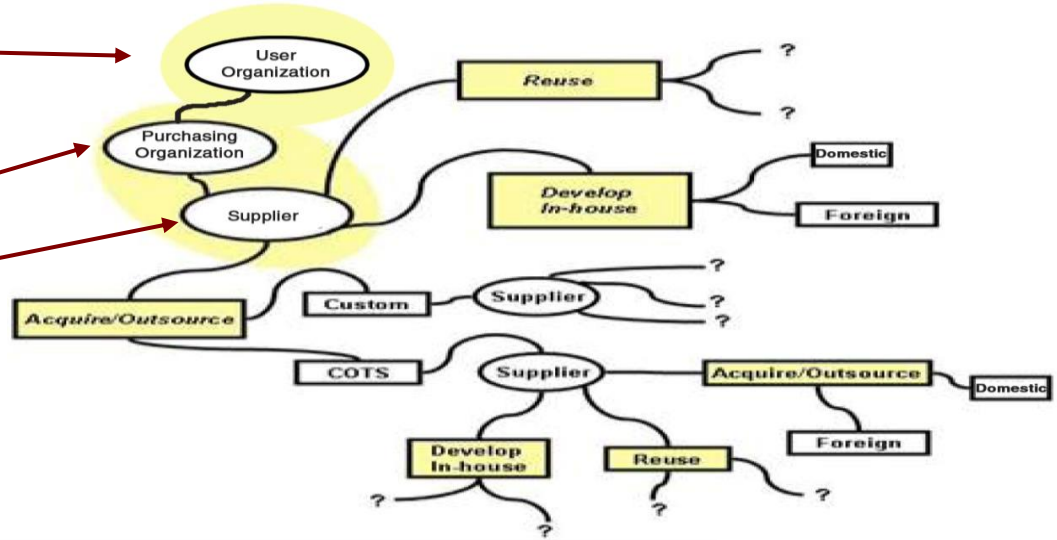
Increasing dependence on globally sourced medical devices and software	• Varying levels of development/outsourcing controls • Lack of transparency in process chain of custody • Varying levels of acquisition ‘due-diligence”
Residual risk	• Tainted products with malware, exploitable weaknesses (CWEs) and vulnerabilities (CVEs) • Defective and unauthentic/counterfeit products
Growing technological sophistication among adversaries	• Internet enables adversaries to probe, penetrate, & attack remotely • Supply chain attacks can exploit products and processes

Software in the supply chain is often the vector of attack

Software supply chain risk management

Mitigating third-party risks attributable to exploitable software in medical devices

- Enterprise-level:
  - Regulatory compliance
  - Changing threat environment
  - Business case
- Program/project-level:
  - Cost
  - Schedule
  - Performance



Who makes risk decisions?
Who determines 'fitness for use' criteria for technical acceptability?
Who "owns" residual risk from tainted products?

Note: "Tainted" products: corrupted with malware, or exploitable weaknesses and/or vulnerabilities

SYNOPSYS®

Software Supply Chain Risk Management:

Testing Software & Enabling Cybersecurity Assurance for Network-Connectable Devices

Software is buggy

How many exploitable weaknesses and vulnerabilities are in your systems and devices?

Input processing

Any software processing input can be attacked**:** network interfaces, device drivers, user interface, etc..

Hackers use binary analysis & fuzzing techniques to find vulnerabilities

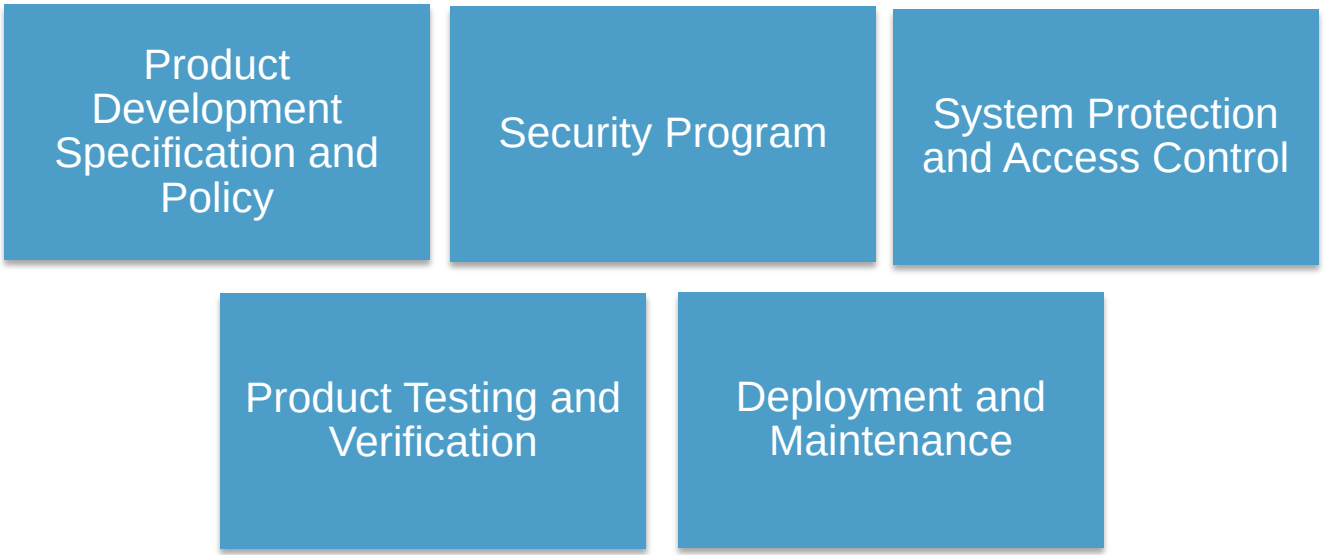
These are used to exploit or launch attacks

These can also be discovered & mitigated by suppliers; should be used in test criteria for acceptance testing

SYNOPSYS®

Software Supply Chain Risk Management:

Proactive Control with Procurement Language for Supply Chain Cyber Assurance



SYNOPSYS®

Procurement Language for Supply Chain Cyber Assurance

Exemplar
(freely available for download; used by other organizations)

https://www.synopsys.com/software-integrity/resources/white-papers/procurement-language-risk.html

SYNOPSYS®

Software Supply Chain Risk Management:

Underwriters Labs Cybersecurity Assurance for Network-Connectable Devices

- UL Cybersecurity Assurance Program (**UL CAP**) provides independent testing and certification of network-connectable devices
- UL CAP uses Synopsys Software Integrity tool suite to comprehensively address software issues in systems and devices
- UL CAP is **Product Oriented & Industry Specific** with these goals:
  - Reduce software vulnerabilities
  - Reduce weaknesses, minimize exploitation
  - Address known malware

UL 2900-3: Organizational Processes

UL 2900-2-1, -2-2: Industry Specific Requirements (currently for ICS & healthcare systems & devices)

UL 2900-1: CAP General Requirements/

SYNOPSYS®

Software Supply Chain Risk Management:

Enabling Cybersecurity Assurance for Network-Connectable Medical Devices

Software security tools and services can be used in assisting:

- Governments and industry in establishing certification labs for medical devices;
- Healthcare service providers in testing network-connectable medical devices and equipment; and
- Manufacturers in implementing best practices for securing medical devices and mitigating risks to patients and health care providers.

Cybersecurity Assurance: It's an multi-team effort!

Global Forum
Shaping the future 2017

DIGITALIZATION:
INTELLIGENT PATHWAYS

SYNOPSYS®
Silicon to Software™

Thank You

Joe Jarzombek – Global Manager, Software Supply Chain Solutions
Joe.Jarzombek@synopsys.com | 703.627.4644
Synopsys Software Integrity Group | www.synopsys.com/software

Join us in our online Software Integrity Community for software security and quality assurance
See State of Fuzzing 2017 to gain insight in software development where further testing remains
Synopsys named a Leader in AppSec Testing in Gartner's 2017 Magic Quadrant