Security Proof your Healthcare Environment and Platforms

Michael McNeil
Royal Philips
November 2015
Objectives

• Discuss Philips’ unique perspective and positioning it faces as a medical device manufacturer

• Review emerging and established drivers for increased focus and resources on medical device security and safety

• Understand how manufacturers and healthcare delivery organizations are responding to the emergence of cybersecurity risk

• Discuss Security by Design, responses to / working with the Researcher Community
Philips: A strong industrial company leading in health and well-being

<table>
<thead>
<tr>
<th>Businesses(^1,(^2)</th>
<th>Geographies(^1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>Western Europe</td>
</tr>
<tr>
<td>Consumer Lifestyle</td>
<td>North America</td>
</tr>
<tr>
<td>Lighting</td>
<td>Other Mature Geographies</td>
</tr>
</tbody>
</table>

- **45%**
- **23%**
- **32%**
- **25%**
- **33%**
- **7%**
- **35%**

Since **1891**
€**21.4 billion** sales in 2014, **70%** B2B
~**106,000** employees in over 100 countries

50% of the portfolio has global leadership positions
€**1.6 billion** R&D spend in 2014 and ~71,000 patent rights
More than 1/4 of revenues from recurring revenue streams

---

\(^1\) Based on sales last 12 months September 2015.  
\(^2\) Excluding Central sector (I&G&S).  
\(^3\) Growth geographies are all geographies excluding USA, Canada, Western Europe, Australia, New Zealand, South Korea, Japan and Israel.  
Note - Prior-period financials have been restated for the treatment of the combined businesses of Automotive and Lumileds as discontinued operations.
# Healthcare

**What we do. Where we are.**

<table>
<thead>
<tr>
<th>Businesses</th>
<th>Geographies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imaging Systems</td>
<td>Western Europe</td>
</tr>
<tr>
<td>Healthcare Informatics, Solutions &amp; Services</td>
<td>North America</td>
</tr>
<tr>
<td>Patient Care &amp; Monitoring Solutions</td>
<td>Other Mature Geographies</td>
</tr>
<tr>
<td>Customer Services</td>
<td>Growth Geographies</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Imaging Systems</td>
<td>36%</td>
</tr>
<tr>
<td>Healthcare Informatics, Solutions &amp; Services</td>
<td>6%</td>
</tr>
<tr>
<td>Patient Care &amp; Monitoring Solutions</td>
<td>31%</td>
</tr>
<tr>
<td>Customer Services</td>
<td>27%</td>
</tr>
<tr>
<td>Western Europe</td>
<td>20%</td>
</tr>
<tr>
<td>North America</td>
<td>44%</td>
</tr>
<tr>
<td>Other Mature Geographies</td>
<td>11%</td>
</tr>
<tr>
<td>Growth Geographies</td>
<td>25%</td>
</tr>
</tbody>
</table>

- **€9.2 Billion sales in 2014**
- **39,000+ People employed worldwide in 100 countries**
- **9% of sales invested in R&D in 2014**
- **450+ Products & services offered in over 100 countries**

---

1. Based on sales last 12 months September 2015.
2. Growth geographies are all geographies excluding USA, Canada, Western Europe, Australia, New Zealand, South Korea, Japan and Israel.
We target healthcare customer and consumer needs along the Health Continuum

Healthy living
Help people to live a healthy life in a healthy home environment

Prevention
Enable people to manage their own health

Diagnosis
Ensure first time right diagnosis with personalized and adaptive care pathways

Treatment
Enable more effective therapies, faster recovery and better outcomes

Home care
Support recovery and chronic care at home

Monitoring, informatics and connected care
Improve population health outcomes and efficiency through integrated care, real-time analytics and value-added services
Industry Challenges

Patient Safety
- Potential threats demonstrated from ethical hackers

Data Integrity
- Demands from customers and patients for accurate and available data

Legal/Regulatory Obligations
- Meeting the privacy and security needs of our customers in the healthcare delivery industry
- Stringent laws around securing data and the transfer of data throughout the world

Protecting Intellectual Property
- Nation State attacks to gain network access and critical assets
- Ensuring security during expansion in emerging markets
Product Security Increasing complexity

Only a few years ago medical devices were standalone systems using proprietary hardware/software and when connected then often only in isolated networks.

This changed when standard platforms were used and systems become more often connected to exchanged data such as medical images and workflow management, remote support and the introduction of vendor managed services.
Product Security Increasing complexity

And now we use personal health apps on mobile devices, connect more health systems, sometimes using cloud based solutions, while also moving more healthcare functions to the patient home.

Furthermore we develop and open up standardized medical device platforms for shared rapid application development and access to health data.
What products and environments are at most risk?

• To ensure Philips develops products and services that:
  
  ▪ Reduce unauthorized access of medical devices and patient information

  ▪ Prevent compromise or loss of patient data

  ▪ Ensure medical device functional integrity and service availability for safe and reliable patient care

  ▪ Enable security patching to remediate unsecure systems and vulnerabilities in response to new threats
What products and environments are at most risk?

Portable & Mobile Devices
Could someone walk out with the device?
Could the device be found in an openly accessible area in your facility?

Malware Protection
Concerns about anti-virus definition updates on medical devices?

Then is your storage medium encrypted?
Then is the storage medium physically secure so it cannot be removed without tools?

An application whitelisting solution takes away the need for daily updates.
What products and environments are at most risk?

**Access to Devices & Settings**
- Does your device store or display ePHI and could non-authorized users potentially access this?
- Is the device only used by clinical users on a daily basis, without a need to access outside of the application?

**Firewall Controls**
- Can your network and device user be fully trusted to never make an unauthorized connection to the outside world?

**Pointers**
- Bring authentication up to your enterprise IT standards, where possible through Active Directory account management integration.
- Prevent access to the Operating System for non-administrator accounts.
- Use a firewall and close all non-essential ports.
# Medical Device Challenges

## Medical Device’s – large & small

<table>
<thead>
<tr>
<th>Big Iron</th>
<th>Mobile</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Image" /></td>
<td><img src="image2.png" alt="Image" /></td>
<td><img src="image3.png" alt="Image" /></td>
</tr>
<tr>
<td><img src="image4.png" alt="Image" /></td>
<td><img src="image5.png" alt="Image" /></td>
<td><img src="image6.png" alt="Image" /></td>
</tr>
<tr>
<td><img src="image7.png" alt="Image" /></td>
<td><img src="image8.png" alt="Image" /></td>
<td><img src="image9.png" alt="Image" /></td>
</tr>
</tbody>
</table>

12 April 6, 2015 Philips HealthTech Confidential
# Medical Device Challenges

## Medical Device’s – large & small

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Big Iron</td>
<td>High Capital Cost</td>
</tr>
<tr>
<td>Mobile</td>
<td>Driver support</td>
</tr>
<tr>
<td>Software</td>
<td>Support / updates</td>
</tr>
</tbody>
</table>
# Medical Device Challenges

## Medical Device’s – large & small

<table>
<thead>
<tr>
<th>Category</th>
<th>Medical Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Big Iron</strong></td>
<td>![Medical Device Image]</td>
</tr>
<tr>
<td><strong>Mobile</strong></td>
<td>![Medical Device Image]</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>![Medical Device Image]</td>
</tr>
</tbody>
</table>

- **Long lifecycle**
- **Software patches**
Responding to the Challenge

Ongoing risk assessment and management determines the security controls.
Responding to the Challenge

Defense-in-depth strategy

- **Firewall**
  - Blocks unnecessary ports
  - Limits the attack profile

- **Malware protection**
  - Whitelisting
  - Allows only known and trusted applications and libraries
  - Requires fewer updates

- **Operating system hardening**
  - Three levels
  - Customizable

- **Access controls**
  - At rest and in transit
  - Based on your requirements

- **Patient data encryption**
  - Three levels
  - Customizable

Disables unnecessary services
Reduces the attack surface
Product Security Requirements
Product Security Requirements

Customer regulatory requirements

Product Security requirements & constraints

Customer regulatory requirements

Standards

Contractual obligations

Manufacturer business requirements

Manufacturer regulatory requirements

Product Security must ensure that the appropriate security features are built into the products so that customers can comply with their obligations.

These include medical device specific regulations (e.g. FDA), local privacy and healthcare specific laws (e.g. HIPAA),

And many others...
Product Security Requirements
Contractual obligations

The customer can also force the manufacturer to comply with their needs to adhere to their local law, regulations and internal policies through contracts.
Product Security Requirements
Manufacturer regulatory requirements

Manufacturer regulatory requirements depend on the type of product (e.g. FDA, MDD, FTC) but there will also be touch points with privacy laws when processing personal data from the customer and/or his patients in services provided by the manufacturer.
Product Security Requirements
Manufacturer business requirements

Even in the case that certain regulatory requirements or contractual obligations might not exist for a specific product in a specific country then a manufacturer still needs to implement security controls and adhere to requirements and constraints as defined in internal policy and by business strategy.
Product Security Requirements Standards

The ability for a manufacturer to operate on a global level can be very complex when it comes to compliance to the specific details of the sometimes very diverse local laws and regulations.

The implementation of international recognized standards can often help to achieve an acceptable level of compliance.
In control
Security by Design

Key elements of the “security by design” best practices (from the Jan. 2015 FTC IoT report):

• Design security into the device at every stage of development, including detailed risk assessments, and consider utilizing multiple levels of security where a risk is identified.

• Take advantage of well-known security techniques, like encryption, salting, and rate limiting, to guard against well-known hacking methods.

• Train employees about the importance of security, and ensure that security is managed at an appropriate level in the organization.

• Fully test the security of products before they are released to consumers and incorporate “smart defaults,” such as requiring consumers to change a default password.

• Monitor connected devices throughout their expected life cycle, and take note of credible sources that identify security vulnerabilities. Where feasible, provide security patches to cover known risks.
Some Applicable Security Standards

• Many applicable NIST standards such as NIST SP 800–33, SP 800-82 and specifically SP 800-53; Recommended Security Controls for Federal Information Systems and Organizations

• ISO/IEC 27002; Information technology – Security techniques – Code of practice for information security controls (and the ISO/IEC 27000 series)

• ISO 27999; Health informatics - Information security management

• ISO/IEC 15408; Information technology – Security techniques – Evaluation criteria for IT security

• IEC 62443-3-3; Industrial communication networks - Network and system security - System security requirements and security levels

• IEC-80001; Application of risk management for IT Networks incorporating medical devices
Responsible Disclosure

Philips is committed to ensuring the safety and security of patients, operators and customers who use our products. Philips maintains a global network of product security officers for developing and deploying advanced best practice security and privacy features for our products and services, as well as for managing security events. Philips operates under a global product security policy, which guides our incident response and risk assessment activities relating to potential security and potential privacy vulnerabilities identified in our products and services. Philips supports coordinated vulnerability disclosure, and also encourages vulnerability testing by security researchers and by customers, with responsible reporting to Philips.

To this end, Philips maintains a product security page with information on software vulnerability testing and responsible reporting at www.philips.com/security.

When submitting reports of vulnerability findings, please ensure the following procedures are followed, for safe and efficient support.
Philips Healthcare Responsible Disclosure Positioning

• **Philips Healthcare and Responsible Disclosure**
  • Philips Healthcare recognizes the need for clear a Responsible Disclosure Policy and protocols as part of its Product Security function.
  • The company is developing a Responsible Disclosure Policy according to current industry best practices.
    – The policy will be publicly accessible, with clear communications channels for customers, researchers and other security community stakeholders.
    – The policy will be based on principles of transparency, accountability and responsiveness.
    – The policy will outline defined protocols for reporting and response, managed by the Philips Product Security Team.
      ▪ The policy protocols will encompass:
        • Monitoring and response of inbound communications
        • Managing confirmation receipt and follow-up communication with senders
        • Evaluation of vulnerability notifications and status tracking
        • Alignment with incident response, stakeholder notification, remediation and prevention protocols as required
  • Philips has actively sought out researcher and analyst input to help guide policy design and projected implementation.
    – The company has increasingly engaged with the security research community over the past year.
    – Philips is committed to ongoing dialogue with the security community and to productive partnerships.
The statement

Philips is committed to ensuring the safety and security of patients, operators and customers who use our products. Philips maintains a global network of product security officers for developing and deploying advanced best practice security and privacy features for our products and services, as well as for managing security events. Philips operates under a global product security policy, which guides our incident response and all risk assessment activities relating to potential security and potential privacy vulnerabilities identified in our products and services. Philips supports coordinated vulnerability disclosure, and also encourages vulnerability testing by security researchers and by customers, with responsible reporting to Philips.

To this end, Philips maintains a product security page with information on software vulnerability testing and responsible reporting at www.philips.com/security

When submitting reports of vulnerability findings, please ensure the following procedures are followed, for safe and efficient support.
Questions?

There are some viruses doctors can’t treat.