



# The time to address medical device cybersecurity is now

**Corporate reputations,  
hospital operations,  
and patient safety  
are all at stake.**

June, 2016

---

[kpmg.com](http://kpmg.com)



# Table of contents

**02**

**A call to action**

**03**

**The cyberthreat landscape**

**04**

**A regulatory imperative**

**06**

**Who's in charge?**

**07**

**Where to start?**

**08**

**What does good look like?**

**09**

**How KPMG helps organizations**



# A call to action

In recent years, television shows and movies have memorably portrayed incidents involving hacked medical devices and artificially intelligent medical equipment harming unsuspecting patients.<sup>1</sup> Although these story lines are often exaggerated, the underlying threat is real. In fact, the frequency and severity of medical device risks are escalating as devices proliferate and cyber attackers turn their attention to vulnerable environments.

Medical devices represent a ripe target for cyber threats due to a combination of two factors:

- New technology-enabled, networked, and interconnected medical devices are being introduced. These advanced devices increase clinical effectiveness, but open up new attack vectors and cyber risks.
- Despite these innovations, there are still a significant number of older medical devices in use today. These are often not secure, and poorly managed.

The industry is not in the dark about these problems. According to a 2015 KPMG LLP (KPMG) report, 32 percent of health care organizations surveyed consider medical device security to be their top information security concern.<sup>2</sup> This apprehension is more than justified. A compromised or *sick* medical device, e.g., one infected by malware, can potentially shut down hospital operations,<sup>3</sup> reveal sensitive patient information to unauthorized persons,<sup>4</sup> compromise connected technologies, or harm patients.

**The current state of vulnerable medical devices is unacceptable and requires an immediate, industrywide call to action.** In order to address ever mounting cybersecurity threats, organizations must take a programmatic approach to identification, mitigation, and remediation of risk. The approach we recommend is fundamentally different from the current state approach. It requires all parties (from manufacturers to health care providers) to communicate and work in collaboration to actively identify cyber risks and related threats, plan for mitigation and remediation, and ensure the ongoing safety and security of patients.

---

1 <http://www.cnn.com/id/100306578# The Terrorist Hack that Shocked America – and Why it Matters>

2 <https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf>

3 <http://www.latimes.com/business/technology/la-me-in-hollywood-hospital-bitcoin-20160217-story.html>

4 <http://www.washingtontimes.com/news/2015/dec/24/100-million-hacked-healthcare-records-makes-2015-s/>

# The cyberthreat landscape

KPMG's 2015 cybersecurity report found that 81 percent of health care organizations surveyed have been compromised by a cyber attack in the last two years.<sup>5</sup> This is due in large part to the value of health care information on the black market, which carries an estimated value of ten times credit card information.<sup>6</sup> More recently, cyber attacks at health care organizations have involved "ransomware," whereby threat actors use malware to encrypt information in compromised environments and demand digital currency to unlock information and restore operations.<sup>7</sup> In addition to the recent wave of ransomware attacks, medical device companies and health care organizations face a wide variety of cyber threats, which vary in sophistication and include:

- Disruption of service
- Malware
- Insider threat
- Theft and/or loss of assets
- Unintentional exposure of data
- Espionage
- Web application attacks
- Point of sale (POS) intrusions

Medical devices in their current state are often vulnerable to cyber attacks, and may contribute to the likelihood that not only the device itself, but critical health care services or an entire organization, will be compromised. This is due to inadequate cybersecurity practices and governance across the life cycle of most medical devices, including:

- Poor software coding standards<sup>8</sup>
- Insecure data transfer channels
- Weak access controls
- Insufficient monitoring processes
- Insecure disposal practices<sup>9</sup>
- Delayed maintenance and update of processes
- Minimal cross team and cross organization communication

The bottom line with respect to cybersecurity threats is that any device configured to connect with another device is at risk of an attack. These risks will only escalate in number and severity as organizations and consumers adopt the "Internet of Things";<sup>10</sup> introduce wearable technologies into their everyday lives; continue to take advantage of smart computing devices such as portable electrocardiogram monitors, continuous glucose monitors, and wearable defibrillators; make further use of big data capabilities; and transmit patient data to different sources over multiple networks.

5 <https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf>

6 <http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924>

7 <http://www.nbcnews.com/tech/security/three-u-s-hospitals-hit-string-ransomware-attacks-n544366>

8 <http://www.tripwire.com/state-of-security/vulnerability-management/medical-device-security-forget-everything-thought-knew/>

9 <http://searchsecurity.techtarget.com/opinion/McGraw-on-assessing-medical-devices-Security-in-a-new-domain>

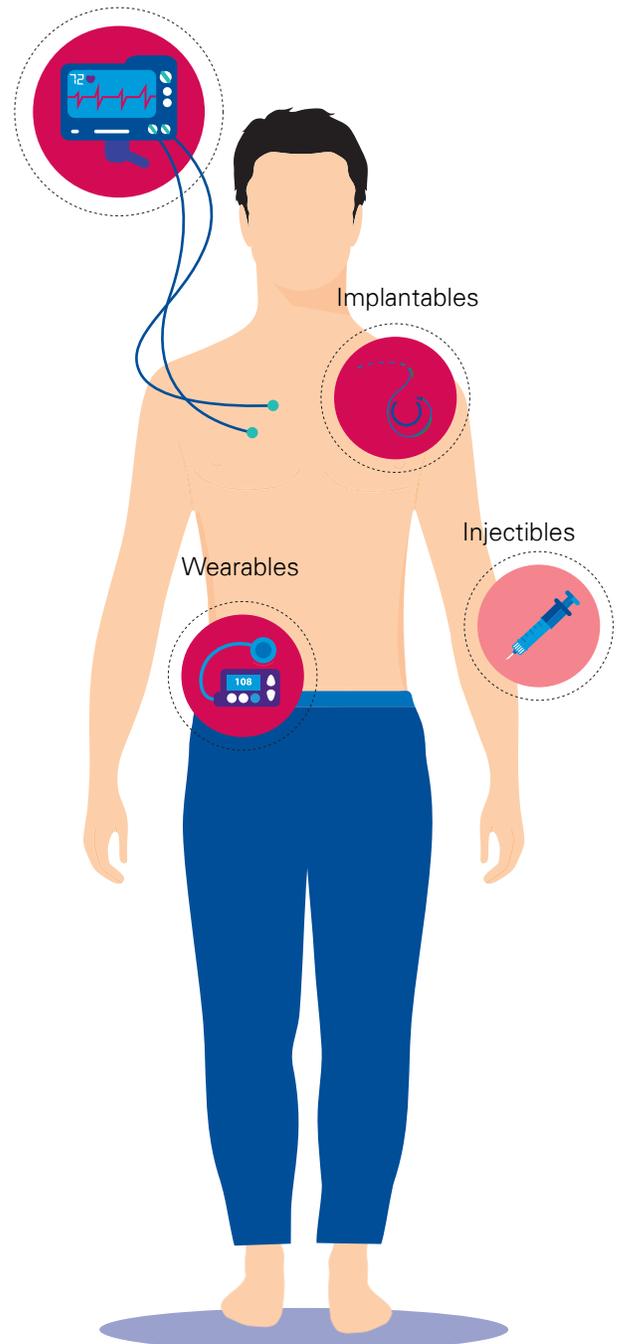
10 [http://en.wikipedia.org/wiki/Internet\\_of\\_Things](http://en.wikipedia.org/wiki/Internet_of_Things)

# A regulatory imperative

Governments, health care industry advocates, medical device manufacturers, and patients have been concerned with cybersecurity for quite some time. In 1976, the U.S. government required medical device and diagnostics manufacturers to follow quality control procedures to ensure device safety and effectiveness. In 1990, the U.S. government passed the Safe Medical Device Act, requiring providers to report medical device incidents to the U.S. Food and Drug Administration (FDA). (Note: This Act did not address cybersecurity incidents.) In 2014, the U.S. FDA enhanced the safeguards put in place by the Safe Medical Device Act by including the recommendation that medical device manufacturers fully identify and understand cybersecurity risks.<sup>11</sup> In early 2016, the FDA issued draft guidelines for medical device manufacturers that call for cyber threat intelligence sharing.

The FDA's more recent guidance stipulates that an effective cybersecurity risk management program is necessary at both the premarket and postmarket stages, and suggests that medical device manufacturers apply the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. The FDA also appeals to and incentivizes medical device manufacturers to practice cyber threat intelligence sharing via an Information Sharing and Analysis Organization (ISAO) and Information Sharing and Analysis Centers (ISACs).

Automated equipment



<sup>11</sup> <http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf>

Many organizations are struggling to understand the FDA's recent guidance and how to implement recommended changes. The matrix below summarizes key considerations:

Pre-Market Guidance (2014)		Post-Market Guidance (2016)	
<b>Availability</b>	Ensure data is available when required.	<b>Structured, systematic approach to cyber risk and quality management systems</b>	Develop a programmatic, holistic, cross team, and recurring approach to cybersecurity risk assessments and quality issues.
<b>Integrity</b>	Validate that data is accurate and complete.	<b>Vulnerability management, device performance and risk acceptance criteria</b>	Conduct routine assessment of vulnerabilities to determine device performance, if compromised, along with agreed cyber risk acceptance criteria.
<b>Confidentiality</b>	Ascertain that data is protected and only available to authorized persons, on a need-to-know basis	<b>Ongoing process to identify, mitigate, and remediate cybersecurity risks</b>	Establish a risk assessment program with agreed risk criteria to continuously evaluate medical devices throughout their life cycle.
<b>Cybersecurity</b>	Consider cybersecurity from the concept and design phase through end of life and disposition of assets	<b>Vulnerability management, risk acceptance, and impact and severity to health criteria</b>  <b>Programs: vulnerability, patch, change and configuration management including compensating controls</b>	Understand and document how vulnerabilities could potentially impact medical devices and patient health.  Establish program and processes for facilitating timely and routine updates, system and software patches, and bug fixes, including configuration reviews and compensating controls assessments.

# Who's in charge?

Many organizations have a multistakeholder team responsible for medical device cybersecurity. This often includes corporate IT; product security; product engineering; research and development; risk; legal; compliance; and trusted third parties. The problem is that many different policies, procedures, and controls are referenced when making design, control, and governance decisions, and there is no lead owner to mediate among them.

We recommend that organizations adopt a “one-policy” view of cybersecurity. This policy should be based upon a thorough evaluation of the specific cyber threats to a medical device manufacturer, including threats to its products, business processes, supply chain, IT infrastructure, software development, and relationships with third parties. We use the ISO/IEC 27005 Information Security Risk Management standard<sup>12</sup> to guide stakeholders through the threat identification and analysis process.



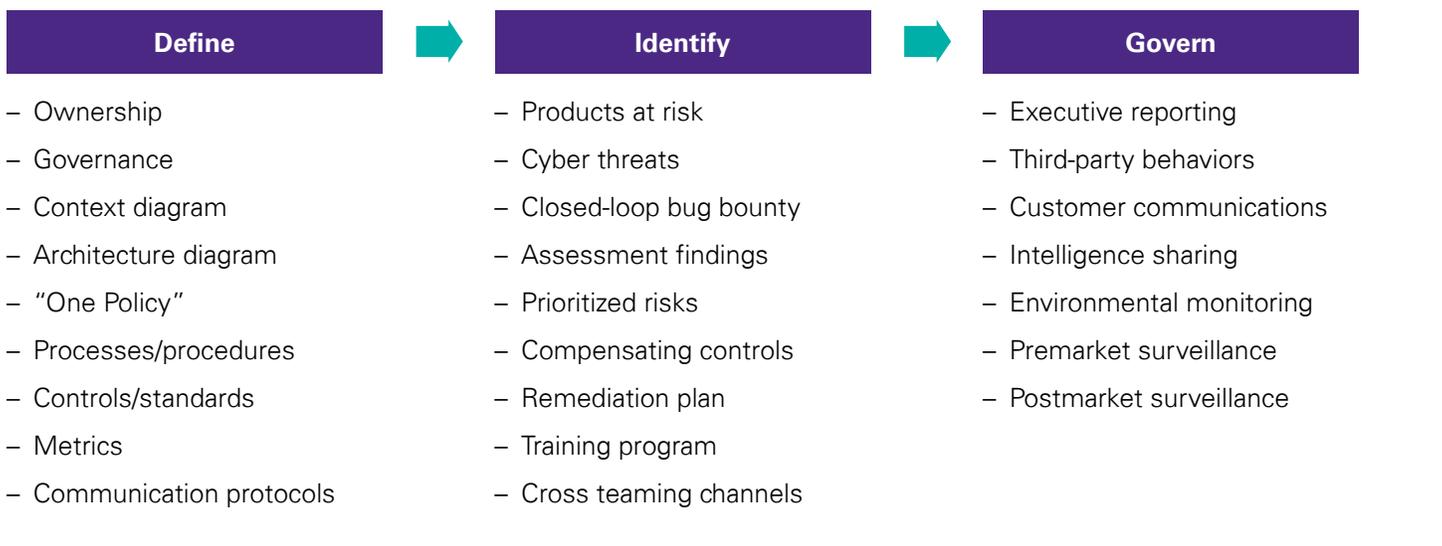
<sup>12</sup> <http://www.iso27001security.com/html/27005.html>

# Where to start?

As with most initiatives, organizations are best served by identifying what is at risk and then steering their investments to support a risk based approach. This requires that medical device manufacturers identify and prioritize cybersecurity threats to their product portfolios. To do this, organizations need to employ a number of review and assessment techniques that include statistical and dynamic code analysis; vulnerability assessments; penetration tests;

gap assessments; key control testing, and more. Further, organizations should collect and analyze threat intelligence to substantiate existing and emerging threats.

A “where-to-start” model that we reference when guiding clients through assessment, change, and remediation efforts is summarized as follows:



# What does good look like?

Many organizations do not have a strategy for identifying, remediating, and sustaining medical device cybersecurity capabilities. We advise a “crawl-walk-run” maturity development campaign that starts with the aforementioned “where-to-start” model.

## Crawl

- Engage cross-functional team
- Initiate “where-to-start” efforts

## Walk

- Govern/communicate
- Monitor cyber threats
- Engage third parties
- Engage customers
- Security by design/SDLC
- Share intelligence
- Align change initiatives
- Decommission products

## Run

- Attestation reporting
- Device ID management
- Threat correlation
- Auto patch/update
- IoT integration
- Device specific training

# How KPMG helps organizations

KPMG helps organizations through our programmatic approach to allocate their scarce resources to address cybersecurity threats and risks in a pragmatic and compliant way. Our recommended approach to helping organizations secure medical devices includes the following areas of focus:

## Product Considerations

1. Define, document, and prioritize cyber risk scenarios in accordance with medical device type, use, and purpose.
2. Design and implement comprehensive cybersecurity controls as per defined cyber risk scenarios.
3. Introduce and document consistent and secure software development and coding methods.
4. Perform penetration testing and vulnerability assessments to proactively identify issues.
5. Train stakeholders in methods of medical device protection that maintain security and patient privacy.
6. Assist with incident response processes.

## Program Considerations

1. Consolidate and optimize cybersecurity and privacy policies to clarify roles and controls, and to define target state for improved medical device security.
2. Design and implement improved maintenance programs related to medical device updates and patches.
3. Improve vendor risk management programs and related communications.
4. Introduce improved threat management capabilities.
5. Identify use and transfer of sensitive information (ePHI) and introduce compliant practices (e.g., HIPAA).
6. Assist with the design and collection of information related to cyber threat intelligence sharing.

## KPMG member firms are:

- Global – The network of KPMG member firms employs over 162,000 people in 155 countries. KPMG cybersecurity industry professionals have extensive knowledge and can offer insight to you wherever you operate.
- Award-winning – KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016 achieving the highest score for current offering.
- Shaping the cyber agenda – Through the International Information Integrity Institute (I-4), KPMG member firms help some of the world's leading organizations work together to solve today's and tomorrow's biggest security challenges.
- Committed to you – KPMG professionals build client relationships on mutual trust and long-term commitment to providing effective and efficient strategies.

## Contact us

### **Greg Bell**

**Principal, KPMG Cyber US Leader**

**M: 678-296-4327**

**T: 404-222-7197**

**E: rgregbell@kpmg.com**

### **David Remick**

**Partner, KPMG Cyber, Life Sciences Lead**

**M: 404-769-1096**

**T: 404-222-3138**

**E: jremick@kpmg.com**

### **Larry Mraz**

**Director, KPMG Cyber, Life Sciences**

**M: 908-528-1660**

**T: 973-912-6161**

**E: lawrencemraz@kpmg.com**

**KPMG's Cyber 24 x 7 Hotline at 855-444-0087**

[www.kpmg.com/us/cyber](http://www.kpmg.com/us/cyber)

[kpmg.com/socialmedia](http://kpmg.com/socialmedia)



The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 550344