THE HEALTHCARE INTERNET OF THINGS

REWARDS AND RISKS

Jason Healey, Neal Pollard, and
Beau Woods

Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

in partnership with

intel Security

Atlantic Council
1030 15th Street, NW, 12th Floor
Washington, DC 20005

ISBN: 978-1-61977-981-5
Publication design: Krystal Ferguson; Photo courtesy of Intel Security.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its funders do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

March 2015

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Internet of Things (IoT) of digital, networked technology is quickly moving to the forefront of society, the global economy, and the human experience.

The IoT sometimes refers to colossal, impersonal concepts like connecting electricity grids to the Internet for economic or environmental considerations. But the IoT can be intensely personal as well. In the world of healthcare, software engineers are weaving networked medical devices into the fabric of the IoT. These devices, which can be worn or even implanted inside the body, are used to medicate, treat diseases, and maintain general health and wellness.

This report, a collaboration between Intel Security and Atlantic Council's Cyber Statecraft Initiative at the Brent Scowcroft Center on International Security, explores security risks and opportunities that networked medical devices offer to society. It also provides recommendations for industry, regulators, and medical professionals to maximize value to patients while minimizing security risks arising from software, firmware, and communication technology across these devices.

Individuals wear networked devices to learn more about themselves, their diet, their exercise regimen, and their vital signs. Doctors can adjust and optimize implanted medical devices, such as pacemakers, quickly and accurately—and often with no need for intrusive medical procedures. In hospitals, new devices network to provide more effective and less expensive monitoring and treatments. According to one estimate, these technologies could save $63 billion in healthcare costs over the next fifteen years, with a 15-30 percent reduction in hospital equipment costs.[1]

This is the second report in a series by the Atlantic Council in partnership with Intel Security to examine the rewards and risks of key emerging technologies and the importance of getting security right in order to unlock technologies' true potential.

The first paper in the series, *Online Voting: Rewards and Risks*, assessed the amazing possibilities that online voting and e-voting could unlock for participatory democracies, while analyzing equally difficult obstacles to ensuring their security.

For this paper, the Atlantic Council's Cyber Statecraft Initiative convened a roundtable of specialists from government, academia, think tanks, and the security and medical industries, to develop some guideposts on sustaining trust, innovation, and effectiveness in the world of networked medical devices.

The analysis in this report draws attention to the delicate balance between the promise of a new age of technology and society's ability to secure the technological and communications foundations of these innovative devices.

The rewards of networked healthcare come with four main overlapping areas of concern, including accidental failures that erode trust. Should any high-profile failures take place, societies could easily turn their backs on networked medical devices, delaying their deployment for years or decades. Protecting patient privacy and sensitive health data is a second immediate concern, as malicious online hackers consider healthcare information especially valuable. A case in point: the number of information security breaches reported by healthcare providers soared 60 percent from 2013 to 2014—almost double the increase seen in other industries—according to

1 Peter C. Evans and Marco Annunziata, Industrial Internet, Pushing the Boundary of Mind and Machines (GE, November 26, 2012), http://www.ge.com/sites/default/files/Industrial_Internet.pdf.

PricewaterhouseCooper's (PwC) Global State of Information Security Survey 2015.[2]

Intentional disruption is also a concern because networked medical devices face the same technological vulnerabilities as any other networked technology. Hacktivists, thieves, spies, and even terrorists seek to exploit vulnerabilities in information technologies (IT) to commit crimes and cause havoc. However, when a networked device is literally plugged into a person, the consequences of cybercrime committed via that device might be particularly personal and threatening.

Even more dangerous than the potential for targeted killings, though also far less likely, is the threat of widespread disruption. Theoretically, a piece of targeted malware could spread across the Internet, affecting everyone with a vulnerable device. Such a scenario has materialized in business IT and industrial control systems; the sophisticated Stuxnet attack against Iran's nuclear program is one example of this.

The current focus in medical device development and production is on manufacturers' preferences and patients' needs. Industry and government should also focus on implementing an overarching set of security standards or best practices for networked devices to address underlying risks.

Several recommendations will help foster innovation while minimizing security risks. This report makes the case that industry must build security into devices from the outset, rather than as an afterthought. As McAfee's then-CTO Stuart McClure testified before the US House Committee on Homeland Security in 2012, "Cybersecurity has to be baked into the equipment, systems and networks at the very start of the design process."[3]

The report recommends continued improvements to private-private and public-private collaboration. More coordination, not more regulation, is warranted. Regulators do not always keep pace with technological progress. They should have feedback from a full set of stakeholders through *transparent* collaborative forums that assure the regulator's independent functioning without creating concerns of collusion with industry. Likewise, industry officials should continue to improve communication among themselves.

The ultimate aim of enhanced cooperation is to change the current approach to the security elements of these devices. Security considerations, along with the devices' ability to improve patients' lives, must become an integral part of the process of conceiving and manufacturing these devices.

The report also recommends an evolutionary change to the regulatory approval paradigm for medical devices in order to encourage innovation while meeting regulatory policy goals and protecting the public interest.

Some medical device makers continue to push old technologies and resist innovation because they know regulators will approve the old technology. A more streamlined regulatory approval process could remedy this problem. An improved process should encourage security by design, as well as the ability to patch systems after they are deployed.

Lastly, this report recommends an independent voice for the public, especially patients and their families, to strike a better balance between effectiveness, usability, and security when devices are implemented and operated.

---

2 Peter Harries, "The Prognosis for Healthcare Payers and Providers: Rising Cybersecurity Risks and Costs," PricewaterhouseCoopers, December 17, 2014, http://usblogs.pwc.com/cybersecurity/the-prognosis-for-healthcare-payers-and-providers-rising-cybersecurity-risks-and-costs.

3 Stuart McClure, statement delivered to the United States House of Representatives Committee on Homeland Security Subcommittee on Oversight, Investigations, and Management, April 24, 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-McClure.pdf.

THE HEALTHCARE INTERNET OF THINGS
REWARDS AND RISKS

THE PROMISE OF A NEW AGE OF MEDICAL TECHNOLOGY

The medical industry is evolving rapidly. Not only do more kinds of devices exist today, but they are increasingly interconnected. Almost half (48 percent) of healthcare providers polled in a PricewaterhouseCoopers survey said they have integrated consumer technologies such as wearable health-monitoring devices or operational technologies like automated pharmacy-dispensing systems with their IT ecosystems.[1]

Though the underlying technology in many of these devices overlaps, as graphic 1 shows, the devices generally fall into four main groups: consumer products for health monitoring; wearable external medical devices; internally embedded medical devices; and stationary, but networked, medical devices.

These technologies hold the key to unlocking both individual and society-wide benefits in three ways: they can improve outcomes and quality of life, empower patients, and cut skyrocketing healthcare costs.

Across the board, these powerful and customizable medical technologies offer the patient improved outcomes and quality of life. Medical staff, or even the users themselves, can monitor their health more responsively, receive feedback and alerts more quickly, make adjustments less intrusively, and deliver benefits more precisely.

According to one study on remote care management, the online monitoring of patients' blood pressure, body weight, and oxygen saturation led to a 64 percent drop in hospital readmissions. Regular videoconferencing checkups meant "patients and their nurses were able to recognize any 'red flags' and help address health problems before they became serious enough to require re-hospitalization."[2]

At the same time, wearable devices individualize medicine by empowering patients to meet their own goals for health and quality of life.

Health-monitoring products provide real-time feedback about nutrition, fitness, pulse, blood pressure, and other vital signs. In fact, according to an eight-nation survey sponsored by Intel, more than half of respondents would trust a test they personally administered as much as, or more than, one performed by a doctor.[3] For better health, patients seem willing to embrace networked medical technology. More than 70 percent of survey respondents were open to using "toilet sensors, prescription bottle sensors, or swallowed [health] monitors."[4]

Though the direct costs associated with the development, testing, and production of medical devices are high, they hold the promise of helping to cut skyrocketing medical costs. It is hard not to be beguiled by the promise of easier health monitoring and self-treatment

1 Michael Compton and Kevin Mickelberg, "Connecting Cybersecurity with the Internet of Things," PricewaterhouseCoopers, October 15, 2014, http://usblogs.pwc.com/cybersecurity/connecting-cybersecurity-with-the-internet-of-things/.

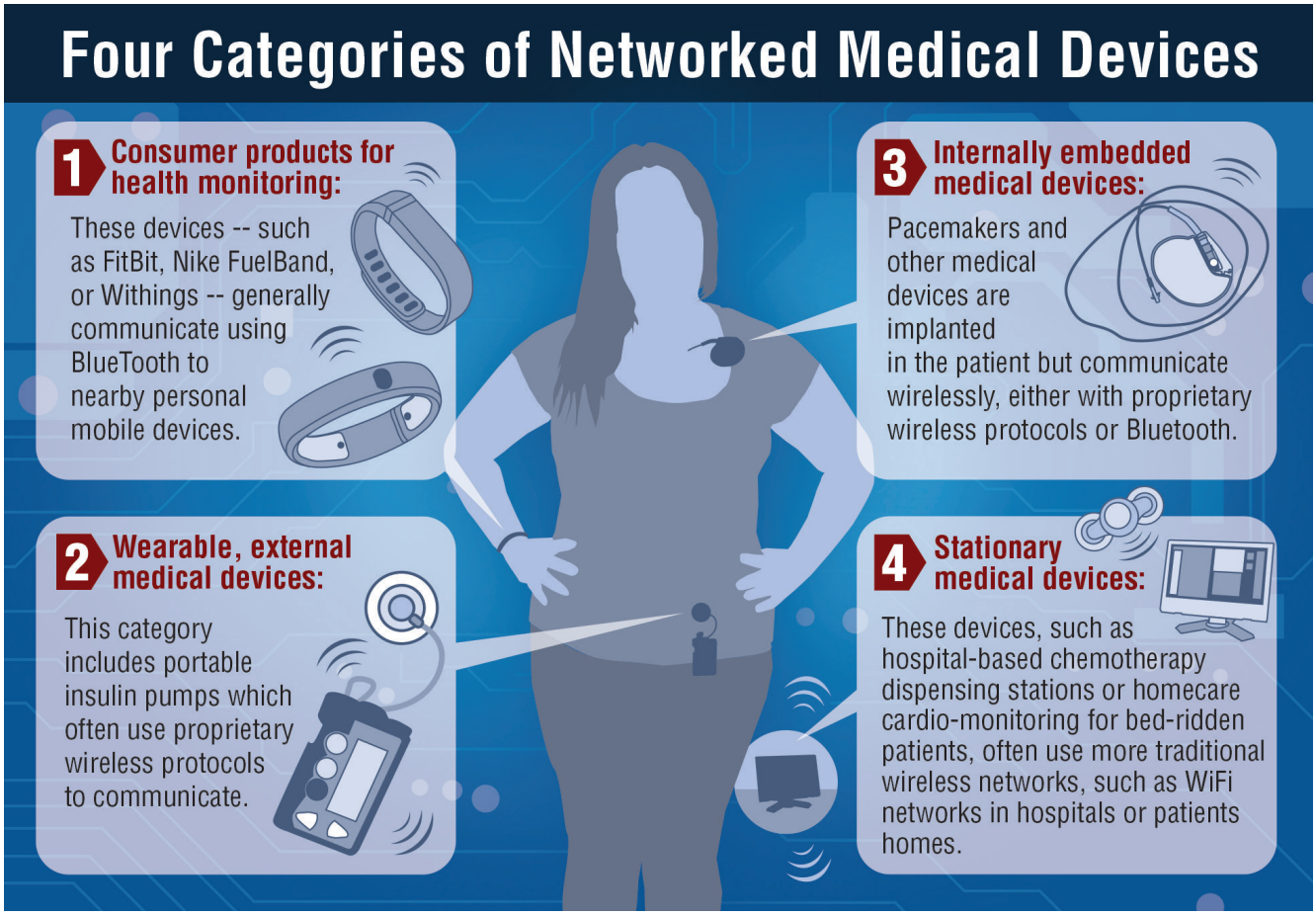
2 Intel, "The Internet of Things and Healthcare Policy Principles," http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/iot-healthcare-policy-principles-paper.pdf.

3 Intel Newsroom, "The World Agrees: Technology Inspires Optimism for Healthcare," December 9, 2013, http://newsroom.intel.com/community/intel_newsroom/blog/2013/12/09/the-world-agrees-technology-inspires-optimism-for-healthcare.

4 Ibid.

Jason Healey is the Director of the Atlantic Council's Cyber Statecraft Initiative at the Brent Scowcroft Center on International Security. **Neal Pollard** is a Director at PricewaterhouseCoopers and Senior Fellow at the Cyber Statecraft Initiative. **Beau Woods** is the CEO of Stratigos Security.

GRAPHIC 1. Networked Medical Devices



using devices like insulin pumps, which provide cheaper alternatives to an overtaxed medical system. If used as tools of preventive medicine, they can also decrease the rate of hospitalization.

The US National Institute of Standards and Technology, quoting one estimate by General Electric, says deploying cyber-physical systems could save $63 billion in healthcare costs over fifteen years, with a 15-30 percent reduction in hospital equipment costs and a 15-20 percent increase in patient throughput.[5]

THE RISK LANDSCAPE

Society's ability and desire to exploit networked technologies has always outpaced its ability to secure the underlying technology. Networked medical devices are no different with exposed security gaps in the integration of operational technology (e.g., medical devices), consumer technology (e.g., smartphones), and networked information technology (e.g., hospital networks).

Malicious actors could soon have the same hold here as they do elsewhere so that we could soon see a booming market in medical zero-day exploits, a security hole known to the attackers and for which there is no defense. This is what the future will look like if security officials and healthcare organizations do not take the correct steps today.

Networked medical devices raise four main and overlapping areas of concern: accidental failures, privacy violations, intentional disruption, and widespread disruption.

The first concern is **accidental failures**, which erode trust and could stop these promising technologies in their tracks. Even a single negative incident, repeated endlessly in the

5 Peter C. Evans and Marco Annunziata, *Industrial Internet, Pushing the Boundary of Mind and Machines* (GE, November 26, 2012), http://www.ge.com/sites/default/files/Industrial_Internet.pdf.

media, might stop an entire class of promising technologies from ever becoming a reality.

Networked medical devices are vulnerable to more than just criminal intent. Like any other technology, they are prone to failure. The complexity of connecting IT to consumer or operational technology which controls physical processes, such as pumps, creates exponential opportunities for flaws in design, implementation, or operation, any of which can lead to accidental failure. This is as true for pacemakers as it is for point-of-sale terminals and toasters—yet given the potentially fatal consequences of a medical device malfunctioning, there's little room for failure when it comes to these devices compared to other networked technologies. Should any high-profile failures take place, societies could easily turn their backs on networked medical devices, delaying their deployment for years or decades.

A second immediate concern is **protecting patient privacy** and the sensitive health data inside these devices.

Vulnerabilities in a networked medical device pose obvious privacy risks, since these devices access patients' most personal biological data. The devices' wireless networking function is central to their effectiveness, though as with any wireless network, users and technicians must ensure that they don't transmit unencrypted personal data across open networks. Additionally, if these devices interface with medical billing records, then patients risk losing both medical and financial information.

According to the Identity Theft Resource Center, 44 percent of all registered data breaches in 2013 targeted medical companies.[6] Furthermore, the number of information security breaches reported by healthcare providers soared by 60 percent from 2013 to 2014—more than double the increase seen in other industries—with financial losses up by a stunning 282 percent, according to PwC's Global State of Information Security Survey 2015.[7]

Since the IoT is still in its infancy, no one yet knows all the ways this information can be used for malicious purposes. For example, one could imagine how many unethical gamblers would want access to key athletes' medical or health data before or during sporting events. What if extortionists took over devices or medical equipment until the patient or hospital paid a hefty ransom? Who knows what other examples we can't yet imagine?

Given the potentially fatal consequences of a medical device malfunctioning, there's little room for failure when it comes to these devices compared to other networked devices.

Intentional disruption is also a concern, because networked medical devices face the same technological vulnerabilities as any other networked technology.

Hacktivists, thieves, spies, extortionists, and even terrorists seek to exploit vulnerabilities in IT to commit crimes and cause havoc. However, when a networked device is literally plugged into someone, the consequences of cybercrime committed using that device might be particularly personal and threatening. Both Hollywood and the real world offer scenarios showing the potentially lethal consequences of terrorists or madmen hacking into pacemakers or insulin pumps.[8] A James Bond movie featuring such attacks surely cannot be far behind.

The US Department of Homeland Security (DHS) is investigating two dozen cases of suspected cybersecurity flaws in medical devices that criminals could exploit, such as forcing an insulin pump to overdose a patient, or instructing a heart implant to "deliver a deadly jolt of electricity."[9]

Even though almost half of respondents polled by PwC had integrated medical devices into their enterprise IT, they had not been as quick in

6 Meg Whitman, "10 Big Tech Trends in Healthcare," *HP Matter*, January 7, 2015, https://www.linkedin.com/pulse/10-big-tech-trends-healthcare-meg-whitman.

7 PricewaterhouseCoopers, "PwC Global State of Information Security Survey 2015," September 30, 2014, http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml.

8 See for example *Homeland* episode no. 10, "Heartbroken," which originally aired on Showtime on December 2, 2012, and Daniel Halperin et al., "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," IEEE, 2008, http://www.secure-medicine.org/public/publications/icd-study.pdf.

9 Jim Finkle, "U.S. Government Probes Medical Devices for Possible Cyber Flaws," Reuters, October 22, 2014, http://www.reuters.com/article/2014/10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022?utm_content=buffer9c60e&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

ensuring the security of these connected devices. More than one-third (37 percent) said they had contacted device manufacturers to learn more about the equipment's security capabilities and risks, and only 59 percent had performed even a rudimentary risk assessment of the devices or technologies. Only 56 percent had implemented security controls, demonstrating a lack of foresight that can have real consequences.[10]

Two prominent security researchers, Jay Radcliffe and Barnaby Jack, have exposed flaws in insulin pumps, which are one of the more widely deployed networked medical devices. In 2011, Radcliffe discovered that access to an insulin pump's serial number would allow him to remotely communicate with the device from up to one hundred and fifty feet away. As these devices have little to no security, he could turn off the pump or cause an insulin overdose with just $20 worth of equipment. Jack soon improved upon Radcliffe's hack by finding a way to compromise an insulin pump even without the serial number, and expanding the range to three hundred feet. This would let a hacker scan for any nearby devices instead of having to target a specific device identified in advance.

As dramatic as these risks are, scant evidence exists that criminals or terrorists are motivated or able to exploit them. In the report referenced earlier, DHS acknowledged it is not aware of any criminals or terrorists trying to exploit the vulnerabilities the department is investigating. This should not, however, be reassuring. That these attack tools have not been widespread could just mean they have not yet appeared in the black market for sale. They almost certainly will.

Even more dangerous than the potential for targeted killings—though also far less likely—is the threat of **widespread disruption**.

Theoretically, a piece of targeted malware could spread across the Internet, and only take action when it confirmed it was in a medical device. Such malware could affect everyone with a vulnerable device. This far-fetched but possible scenario has materialized in business IT systems and industrial control systems, like the sophisticated Stuxnet virus which targeted Iran's nuclear program.

BOX 1. REWARDS AND RISKS IN CONTEXT: BIOINSTRUMENTATION

Great Lakes NeuroTechnologies, a company based in Cleveland, Ohio, developed "bioinstrumentation" products to better measure health. One set of these products tracks how symptoms change in response to treatment for patients with Parkinson's disease through "physiological monitors and patient-centered diagnostic and therapy systems integrated with wireless, remote, and web-based applications," according to the company.

Of course, these Internet-enabled devices are at risk of an attack, but the results demonstrate the upsides of improved outcomes at reduced cost:

- "Clinicians use the real-time data collected by IoT-enabled devices to help optimize their patients' treatment and observe their response to treatment."
- "Pharmaceutical companies working on developing new therapies…use the information gathered through [these networked] devices to aggregate patient data from multiple locations around the world for clinical studies."
- "The Internet of Things also helps Parkinson's patients get affordable access to quality care" via telemedicine.

Source: Jasper, "Great Lakes NeuroTechnologies Turns to Jasper to Automate Telemedicine for Parkinson's Disease—IoT Enables Connectivity for Remote Sensing to Optimize Patient Treatment," https://www.jasper.com/sites/default/files/downloads/GL-NeuroTechnologies-IoT-Success-Story.pdf.

10 Michael Compton and Kevin Mickelberg, "Connecting Cybersecurity with the Internet of Things," PricewaterhouseCoopers, October 15, 2014, http://usblogs.pwc.com/cybersecurity/connecting-cybersecurity-with-the-internet-of-things/.

BOX 2. REWARDS AND RISKS IN CONTEXT: INSULIN PUMPS

Insulin pumps, among the most widely embedded devices, illustrate the balance between the benefits and risks of networked medical devices. Convenient and effective, they undoubtedly improve peoples' lives. One user, Melissa Ford, explains:

> *My insulin pump allows me to be a person with diabetes, not an autoimmune disorder with a pet human. For 7 years now, an insulin pump has given me the freedom to do the things I couldn't have done as confidently on injections. I eat just about whatever I want, when I am hungry; I drink alcohol in moderation; I travel at will; and I exercise to good effect. I can spend long hours in the library or at the pub. Reduced diabetes-related frustration and depression freed me to discuss things other than my blood sugars—campus events I had attended, what I was learning in my classes, and fun with friends.*[11]

SOURCES OF RISK IN NETWORKED MEDICAL DEVICES

The software and firmware underlying networked medical devices have evolved in much the same way as other technologies: as an uneven and inconsistent mix of different versions, standards, and approaches to implementation. The developments were driven by manufacturers' preferences and patients' needs, as opposed to an overarching set of security standards or best practices.[12]

No one standard operating environment, architecture, communications method, or networking backend exists as a widely accepted standard for any class of networked medical devices. Where mobile phones or tablets operate on a relatively small set of standard technologies (Android or Apple, WiFi only or WiFi and 3G or 4G), medical device manufacturers tend to assemble a grab-bag of technologies, depending on the size of the device.

Large devices are typically more standardized, with commodity off-the-shelf hardware and software components not much different from what might be on the doctor's desk. An MRI, for instance, might run a UNIX subsystem on the device, with a Windows front-end for controlling and viewing images. Smaller devices tend to be more specialized. For example, since a pacemaker needs an extremely long battery life and a low-consumption processor, it would more likely use a custom operating environment.

The communication technology may be more standard than other components of the device. A bedside infusion pump might link to the hospital's WiFi and connect to a system at the nurses' station, which in turn is linked over the local network to the hospital's medical records system. A pacemaker is more likely to use a shorter-range technology such as Bluetooth, the same technology that connects a mobile phone to a wireless earpiece or a tablet to a wireless keyboard.

Connectivity is powered by network systems, through which speedy electronic data transfers occur. The Internet, the world's most iconic network, consists of a multitude of other networks that differ in many aspects including size, topology, and access technology, bringing extreme complexity to the system. Known as the perimeter of a connected system, a network is subject to specific risks that network specialists address with constantly evolving security solutions.

Whereas a local health network with sharply defined boundaries might seem watertight, the very fact of being connected to the Internet via e-mail, or to a supplier via a private network, exposes the ecosystem to network-based risks. Simply blocking traffic or shutting down ports affords insufficient protection and are counterproductive mechanisms, which merely serve to hinder access to information or interrupt service delivery. For networked devices to run smoothly, the networks that support them require full-time management with the capacity to inspect traffic, apply appropriate security policies, and exercise a bird's eye view on activity across the hybrid links that populate them. However,

11 Melissa Ford, "'No, It's Not a Beeper, It's My Insulin Pump': Reflections on the Use of Continuous Subcutaneous Insulin Infusion Pump Therapy," *Medscape*, http://www.medscape.com/viewarticle/458714.

12 For a case study of this process going horribly wrong, read Nancy Leveson's analysis of the Therac-25 computer-controlled radiation therapy machine http://sunnyday.mit.edu/papers/therac.pdf.

sophisticated technology is not always accessible, and security vendors face the daunting challenge of juggling the genuine business needs of saving time, keeping costs down, and simplifying administration.

Device and application software disparities are common due to the lack of standard programming language across the industry. In most cases, companies continue to improve on older devices while using similar components and languages, as the costs of switching are high, and keeping "legacy code" might ease the burden of getting the FDA approval required for new devices.

Access control and credential-management controls present a particular dilemma, as these control permissions allow direct access to a patient's most personal data, or to the device's underlying control code.

Medical devices need to be *secure enough* to protect against tampering, yet still *accessible enough* to be accessed by medical personnel. Imagine a patient with a networked pacemaker who naturally wants the strictest controls, then falls unconscious after heart trouble while traveling overseas. That patient would want a local doctor or emergency medical technician to have immediate access to the pacemaker, yet the patient is incapacitated and cannot grant that authorization.

Different manufacturers have different solutions to this dilemma. Some favor "hard-coded" passwords that are built into the system and can't be readily changed. The upside is that these passwords can be listed in the device's user manual, easily found by emergency medical professionals who might need them to treat a patient. Unfortunately, hackers can also easily find the passwords and misuse them. The US Computer Emergency Readiness Team (US-CERT) recently disclosed that several defibrillators had this vulnerability, noting the default password "allows physically proximate attackers to modify device configuration and cause a denial of service with adverse human health effects."[13]

Other manufacturers stress security by avoiding such hard-coded credentials, but at the risk of keeping out legitimate medical personnel during a dire emergency.

Finally, there is the challenge of fixing vulnerabilities after they are discovered. If, for example, a device has been surgically implanted, patching the software or firmware is not always possible.

In the United States, some manufacturers fall back on a longstanding concern that any change, even security patches, requires FDA re-approval. Although this is not accurate, patching medical devices remains costly and cumbersome, as manufacturers must prove that the patched device still meets all medical intended-use claims.[14]

Consequently, less patching is done on medical devices than on other IT systems.

RECOMMENDATIONS FOR BETTER SAFETY, SECURITY, AND EFFECTIVENESS IN NETWORKED MEDICAL DEVICES

As with security challenges accompanying other new technologies, open collaboration and communication are key to managing and reducing risk. This includes collaboration and communication among regulators, as well as between regulators, industry, and medical and healthcare practitioners. Several recommendations will help foster innovation while minimizing exposure to security risks:

- Stress security at the outset, rather than as an afterthought
- Improve private-private and public-private collaboration
- Move toward evolutionary change of the regulatory approval paradigm for medical devices
- Introduce an independent voice for the public

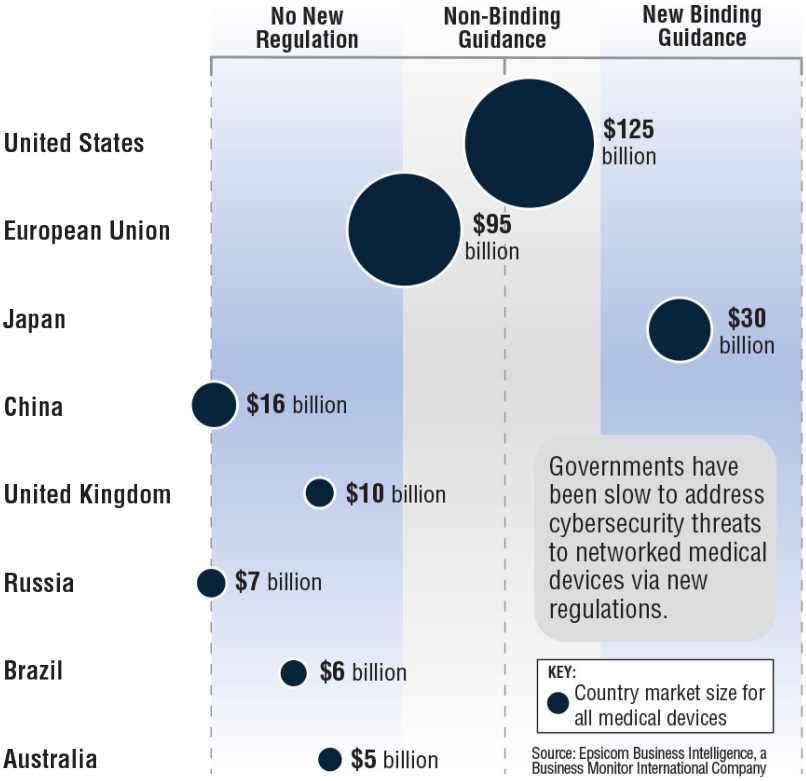
13 US-CERT, "Vulnerability Summary for the Week of August 11, 2014," August 2014, https://www.us-cert.gov/ncas/bulletins/SB14-230.

14 For evidence that the concern is not true, refer to FDA guidance and communications such as http://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm; http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm189111.htm; and http://www.fda.gov/RegulatoryInformation/Guidances/ucm356186.htm.

GRAPHIC 2. Regulatory Spectrum for Networked Medical Devices Worldwide

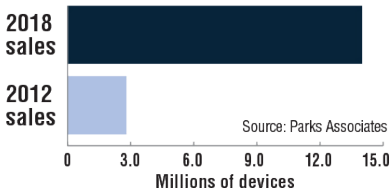
The Evolving Global Market for Networked Medical Devices

Regulatory Spectrum for Networked Medical Devices



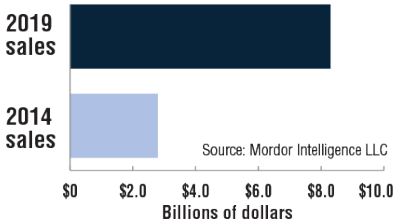
Unit sales set to grow five times

Parks Associates predicts unit sales of networked medical devices will exceed 14 million units by 2018, more than five times the sales from 2012.



Revenue expected to triple by 2019

The global medical wearable electronics market was worth more than $2.8 billion in revenue in 2014 and is expected to cross $8.3 billion in 2019, growing at a healthy CAGR of 17.7% from 2014 to 2019.



United States: The FDA's latest regulatory guidance is non-binding, and many countries are waiting for more definitive US action before updating their own regulations. eHealth in the US will be big business, but the current focus is largely on wearable fitness monitoring devices, which represents a small fraction of the potential market.

European Union: A slate of proposed regulations are currently being considered by the European Parliament, and the EU put out new revised guidance on software as a medical device in late 2014. Look for something definitive in the short term, which will likely spurn more aggressive investment into the European eHealth space.

Japan: Connected software programs will now be treated under the same regulatory regime as other medical device hardware, though the exact implementation is yet to be determined. Japan is the country with the second largest market for medical devices, and the next generation of medical technology will likely be shaped in Tokyo.

China: Despite a major overhaul of Chinese medical device regulation in 2014, the government did not address networked medical devices. China remains a relatively small player in the eHealth space, but growth could be explosive over the medium-term. However, government policies that favor domestic device manufacturers over foreign competitors could limit investor appetite.

United Kingdom: In their latest guidance, the UK Medicines and Healthcare Products Regulatory Agency made clear that software, including apps, with an explicit medical purpose that meets the definition of a medical device in the Medical Devices Directive will be regulated as devices and will have to undergo a conformity assessment.

Russia: Russia currently pursues its own product testing on all medical devices, and does not recognize CE marking, FDA 510(k) clearance or other national approvals. Russia's medical device registration process continues to be mired in an opaque bureaucracy (Roszdravnadzor), and major overhauls to the regulatory framework of networked medical devices are unlikely.

Brazil: Despite expectations of a major overhaul in 2014, the National Health Surveillance Agency of Brazil failed to move forward with new regulatory requirements specifically for medical device software. Analysts predict that demand for networked medical devices will only grow Brazil's position as the largest market in Latin America.

Australia: Since 2011, there have been no major updates to the Australian Regulatory Guidelines for Medical Devices, leaving a hole in the regulations regarding networked medical devices. Australia has a history of following the lead of the US and EU, so look for more of the same as the technology continues to develop.

Source: Emergo Group

1 Build Security into Devices from the Outset, Rather than as an Afterthought

Medical device manufacturers must adopt a "secure-by-design" approach to research and development.

In the past, security has always been an afterthought. Because of that approach, security experts have had to deal with the reckless shortcuts developers have taken to try to cram security in after the fact. Adding security features to products after their initial rollout is a losing battle. It is simply too costly and ineffective to try to secure systems already in the possession of the end user.

As Stuart McClure, McAfee's then-Executive Vice President and Worldwide Technology Officer explained to the US House Committee on Homeland Security, "Cybersecurity has to be baked into the equipment, systems and networks at the very start of the design process."[15] Admittedly, to get security right in the design process upfront is an investment both in time and resources. But by prioritizing security in its approach to product design today, the medical device industry will reap dividends tomorrow.

Maximizing the benefits of networked medical devices requires careful balance between the control that a secure-by-design approach might impose on devices and the flexibility needed by practitioners and patients in the field. Sometimes, flexibility, and adaptation in the field breeds security vulnerabilities, as device operators change configurations or security features, or combine technologies. A secure-by-design approach might include mitigating approaches such as automated logging and monitoring of device modifications in the field, to identify vulnerabilities and better manage them.

National governments, in partnership with an industry coalition, might make this secure-by-design approach easier by providing initial funding for an open-source, common-language software library for medical devices.

Since many medical device manufacturers write their own in-house code—and they are not software specialists—their customized code is more likely to be inefficient, specific to each company or project, or full of security holes just waiting to be discovered. Such small software operations also tend to make it difficult to find and patch those bugs.

This project could be a rare opportunity in which innovation, privacy, and security would be fully aligned, as it could reduce costs for manufacturers and accelerate innovation, all while allowing for better security. As security threats and other bugs are found, the fixes would be made available to the entire community.

Even the best secure-by-design products will still have bugs. The medical device industry should therefore adopt another best practice from other technology sectors and cooperate with computer security researchers. A grassroots organization of security researchers called "I Am The Cavalry" is an excellent example of collaboration between security researchers and companies, creating public awareness around areas where IT security affects public safety and human life, especially networked medical devices.

All too often, companies see such "hackers" as adversaries or villainous criminals looking for flaws in their products. Instead, many are driven by simple curiosity or public mindedness.

So-called "bug-bounty" programs offer modest financial rewards to these researchers who provide low-cost security testing for the software. An industry-wide bug-bounty program for medical devices, perhaps even initially co-funded by a partnership between government and industry, might drastically improve security at a low cost.

A new approach for risk management of networked medical devices begins with cooperation between the manufacturers of devices and software. Manufacturers need to work with the security industry and regulators to develop a comprehensive risk model to follow during product innovation, design, and delivery. This model would view the networked medical device as a platform, not a standalone delivery device. (The smartphone is another example of this model.) It would create corresponding industry coalitions around

15 Stuart McClure, statement delivered to the United States House of Representatives Committee on Homeland Security Subcommittee on Oversight, Investigations, and Management, April 24, 2012, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-McClure.pdf.

specific device lines, to consider the security of technologies connected to the device. The goal is to produce a medical device as a robust platform, upon which additional technologies and services can be added.

It is ineffective to apply existing risk models, developed for desktop security, to medical devices. The differences—such as in credential management, access control, and patching—are too great. As one participant in an Atlantic Council workshop pointed out, the tradeoffs between convenience and security can be particularly pronounced:

> *If you have an insulin pump and you're asking somebody over sixty to input a password every time that person gives a bolus, then either the person is going to choose 1-1-1-1 as the password, or they're going to find a way to deactivate it, or they're going to go for a competitor's device which doesn't have it [to avoid the irritation].*[16]

However, existing models for cybersecurity risk management can serve as a launching point. Within the United States, NIST's National Cybersecurity Center of Excellence (NCCoE) is working with industry to develop a use-case to secure wireless medical infusion pumps, and will then expand it into a practice guide using off-the-shelf solutions.[17]

NIST has also created a more targeted $7.5 million program to explore Cyber-Physical Systems (more or less, another name for the IoT), including networked healthcare devices. This has been an active and extensive project for developing a secure-by-design IoT, involving industry vendors, academia, and government.

Other jurisdictions, especially the European Union (EU), should be involved with these programs and extend them within their own borders.

2 Improve Private-Private and Public-Private Collaboration

Few would suggest that the industry needs more regulation. Rather, more coordination is crucial. In any government agency struggling to deal with rapid changes in technology, regulators are not always as agile as they would like to be. To respond effectively, regulators require feedback from everyone involved through *transparent* collaborative forums, which ensure the regulator's independent function without concerns of collusion with the industry.

Improving security almost certainly requires a safe place to talk about these issues, provide clarity on regulatory interpretation, reach agreement on how regulators can enable innovation and effectiveness, and serve as a safeguard of the public interest.

For discussion with government, one existing model is the National Health Information Sharing and Analysis Center (NH-ISAC) in the United States. The NH-ISAC itself is probably not appropriate for this function, as it focuses on threat response, but its role as a convener of multiple stakeholders makes it useful as a model.

Manufacturers should continue improving communications among themselves. The Industrial Internet Consortium (IIC)—formed by Intel, IBM, Cisco, AT&T, and Microsoft—is an example of how industry collaboration can help unlock business value while also bolstering security.

The EU might consider such models as part of its current debate on adopting new regulations. Current EU procedures for medical device approval are shorter and less restrictive than their US equivalents. The European Parliament is considering new regulations that would promote safety as well as innovation. However, some manufacturers worry that such rules would create unnecessary layers of bureaucracy and delay patient access to innovative technologies.[18]

As the various regulatory bodies (shown in graphic 2) continue deliberating, they will need

16 Quote from participant at Atlantic Council workshop on networked medical devices held on June 27, 2014.

17 NIST, "Cybersecurity Center Invites Feedback on Securing Medical Devices," December 22, 2014, http://www.nist.gov/itl/pumps-122214.cfm.

18 Angeliki Valsamidou, "Update on the European Proposal for a Medical Devices Regulation," *Inside Medical Devices,* May 30, 2014, http://www.insidemedicaldevices.com/2014/05/30/european-parliament-adopts-resolution-on-the-proposal-for-a-medical-devices-regulation.

to consider the transnational nature of data. Medical devices—especially in the consumer personal-fitness space—already stream data to cloud servers, which can be in another jurisdiction that might have significantly different health and privacy regulations.

These standards must be coordinated worldwide, following the examples of the Global Harmonization Task Force and the International Medical Devices Regulators Forum. Ideally, IT standards should vary as little as possible from one country to another. Not only would that cut manufacturing costs; it would allow security to scale among jurisdictions.

Movement to the cloud will continue to pose regulatory and business challenges, as data moves seamlessly across borders with profoundly different privacy regulations.

3 Evolutionary Change of the Regulatory Approval Paradigm for Medical Devices

The current regulatory paradigm must do more to encourage innovation, while still meeting regulatory policy goals and protecting the public interest.

Most regulatory processes, such as the FDA's 510(k) process, give the regulator an initial look at a new medical device before it goes to market. To determine whether the new device is similar to an existing one on the market—with the same risks and benefits for treating an identical problem—the FDA will classify the proposed product and review its risks and benefits, along with any available research. If a device is 510(k) cleared, it may then be sold in the United States, but cannot be referred to as "FDA-approved."

Yet some manufacturers push old technologies and stifle innovation because they know the old technology will obtain regulatory approval. As mentioned earlier, this can discourage manufacturers from innovating, which can actually result in decreased network security.

One possible incentive might be a streamlined approval process. Software security for nonmedical devices is a fairly mature field. Security experts already know the vulnerabilities of general commercial software, which allows a solid correlation for those in medical devices. Where the same or similar vulnerabilities exist, such as in a device running a vulnerable webserver or with an out-of-date operating system, regulators might not approve the product. The regulatory process should encourage security by design, as well as the ability to patch systems after they are deployed.

4 Independent Voice for the Public in Cybersecurity Discussions

It is fundamental that this model offers a voice in the debate to the public, especially patients and their families. In most countries, governments and private companies do not adequately represent the public's interest in medical issues. This applies specifically to striking a balance among effectiveness, usability, and security when the device is implemented and operated.

As the head of a medical device consortium testified before the US Congress:

> *Our entire healthcare system is shifting to a model that embraces shared decision-making by informed patients, whose views are valued and considered at every stage of treatment. It makes sense for innovators and regulators to consider patient perspectives as they develop and assess medical devices. After all, one of the most important questions we ask is whether the clinical benefit of a device outweighs its risk.*
>
> *Patients and their families have a deep and personal understanding of what it is like to live with a disease, and they often have valuable insights on how a device could affect their quality of life. In the end, it is patients who must take the risks of medical interventions to obtain the benefits, so their perspectives on benefit-risk tradeoffs should be central to the benefit-risk assessments that are the basis of regulatory approval.*[19]

Regulators have already recognized the value of public input, especially from patients.

19 Bill Murray, testimony delivered to the US House of Representatives Committee on Energy and Commerce Subcommittee on Health, July 9, 2014, http://democrats.energycommerce.house.gov/sites/default/files/documents/Testimony-Murray-HE-21st-Century-Cures-Modernizing-Clinical-Trials-2014-7-9.pdf.

Within the United States, guidance in 2012 from the FDA's Center for Devices and Radiological Health emphasized "patient tolerance for risk and perspective on benefit."[20] The FDA can embrace this approach further, applying it industry-wide and offering specific guidance on how feedback from patients, or the broader public, should be collected and presented into the regulatory process.

CONCLUSION

Networked medical devices have bridged the human-machine interface, delivering the most personal of benefits. They literally embed the Internet into people's lives, improving medical outcomes, offering better quality of life, and lowering healthcare costs. They also potentially introduce security flaws along with those benefits. However, these flaws can be managed and even reduced with a handful of steps: a focus on security by design; better collaboration among industry, manufacturers, regulators, and medical practitioners; a change in the regulatory approval paradigm; and encouraging feedback from patients and families who directly benefit from these devices.

The medical profession stands to benefit from networked medical devices in ways that are still unfolding. The practice of medicine is as old as human civilization, though it sometimes resists adopting new technology. To embrace this change, medical school curricula would do well to focus on this new set of tools. Health practitioners and physicians, working with patients and their families, are particularly well suited to drive the right balances among security, safety, effectiveness, and patient experience. If they embrace this technology, they will be uniquely positioned to observe and identify the causes of medical device failures—as well as the unintended consequences of efforts to strike these balances—and share those insights and lessons with all involved parties.

20 Ibid.

ABOUT INTEL SECURITY

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. www.intelsecurity.com.

ABOUT THE ATLANTIC COUNCIL

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.