Feature

The Criticality of Security in the Internet of Things

Rebecca Herold, CISA, CISM, CIPM, CIPP/US, CIPT, CISSP, FLMI, is founder and chief executive officer of The Privacy Professor and cofounder and chief visionary officer of SIMBUS360. She has more than 25 years of information security, privacy and compliance experience; has published 17 books; and is an adjunct professor for the Norwich University (Northfield, Vermont, USA) Master of Science in Information Security and Assurance (MSISA) program.

For the past several years, a lot of research, writing and speaking has been focused on the Internet of Things (IoT) and the smart devices that are used within it. The technology is evolving faster than most can keep up with all the reports that are published. It is also a misnomer to keep referencing it as the IoT when, in progressively more instances, the Internet is not even involved. It is becoming more like the Network of All Things (NoAT), with more capabilities that are emerging for smart devices to communicate directly with each other in ways that go beyond the long-standing peer-to-peer (P2P) communications. And as these new technologies emerge, many are not being designed under any existing legal requirement to include security and privacy controls. For example, wearable fitness devices, home energy controllers, driverless and Internet-connected cars, smart watches, and many others seem to be designed with an ultimate goal of being newsworthy for how much data they can collect, analyze and share, without the auspices of virtually any regulatory authority to establish a minimum set of security and privacy controllers. Establishing security and privacy requirements for these growing numbers of personal smart devices is needed yesterday.

With all these new smart technologies and devices, most of them collecting, storing and communicating data without any action necessary by the individuals using them, it becomes more important than ever to build security and privacy controls into the devices.[1] While the technologies are new, the information security concepts that should be applied are not new; data security concepts that have been used for five to six decades or more can be applied within these gadgets, as can the comparably newer privacy control concepts.

In addition to the need for the engineers creating smart devices to build in data security and privacy controls, those businesses that have their employees using such gadgets, and businesses whose employees are using their own such gadgets while working, also need to establish parameters and rules around that use.

SMART DEVICES ARE INCREASINGLY BEING USED

How many of us are aware of any smart device development going on in our organizations? How many of us are aware of the smart devices that may soon be introduced within our environment or may already be in use? This is something on which all information security and privacy professionals and IT auditors, collectively referenced here as information assurance (IA) professionals, need to stay up to date. Here are just a few examples of some of the smart devices that have emerged over the past 15 years:

- **Mobile phones, which evolved into smart phones**—Smart phones were introduced in January 2007, with the introduction of the iPhone.[2] This was arguably the first type of widely used IoT device. Smart phones are now pervasive,[3] and the reach of data accessible from and to them is now significantly greater since they have applications (apps) and/or global positioning systems (GPS) installed. Do organizations know how many of their employees are using smart phones while also performing business activities? Employees could be bringing significant risk to the organization if their mobile devices are not properly controlled.
- **Medical devices**—Interest in these devices gained significance in 2007 when then-US Vice President Dick Cheney had his doctors disable the wireless connection to his pacemaker because he feared terrorists would hack into it and turn it off to kill him.[4] Many, and perhaps most, medical device manufacturers do not build any or, quite frankly, build negligible security and privacy controls into their devices.[5]
- **Smart meters and other smart devices within the smart grid**—One topic that comes up frequently in the group discussions of the US National Institute of Standards and Technology (NIST) Smart Grid Privacy Group[6] and the Smart Grid Interoperability Panel (SGIP)[7] (which the article's author has led since 2009) is how the smart devices being introduced into the smart grid will impact privacy,[8] particularly

those devices that are used by consumers and communicate directly with a wide number of smart device vendors without any regulations or industry standards.[9] It is likely that the evolution of smart meters and smart devices in this space will accelerate in the coming years, bringing with it privacy and security issues that have not yet been imagined.

- **Wearable fitness monitoring devices**—There are some wearables that are prescribed by health care providers[10] but do not fall under the traditional definition of a medical device that is regulated in the US by the Food and Drug Administration (FDA). There are also increasing numbers of fitness and health monitoring devices sold directly to consumers to help them keep track of exercising and specific types of health data, such as blood sugar levels and heart rate. The great success these wearables have had with helping their users to lose weight[11] is very seductive and leads those using them to become lax or nonchalant with regard to making sure they have appropriate security and privacy controls in place. Businesses are now even providing fitness monitoring devices to their employees to wear, with the businesses monitoring them to provide compensation incentives, which opens up a huge realm of privacy concerns.[12]
- **Smart home devices**—These include such devices as Amazon's Echo,[13] home security and baby monitors,[14] smart televisions (TVs),[15] and a wide range of home environment controllers.[16] These, too, are generally unregulated, and the data collected could be going to a very large number of third parties[17] of which the users have no knowledge. And, as the hack of the home security monitor that occurred in 2013[18] demonstrated, the need to build in security controls is great, and the possible privacy harms to those using the devices could be catastrophic, not to mention the fines and sanctions to the company providing the device.[19] In the US, lawmakers are looking to adopt new laws to secure these gadgets.[20] It is important for readers to know whether their countries are also considering such laws.
- **Smart cars**—Having computers perform various functions in cars is nothing new; the first computers were put into cars in the late 1970s to provide some engine controls.[21] However, beginning around 1995, it became common for cars to have a controller area network (CAN) to connect with and gather data from various types of sensors about different areas and parts of the car using wires and software protocols known collectively as the CANbus.[22] Today, microcomputers control a wide range of functions within automobiles such as braking, air bags, the horn, the locks and the ignition. They also track such things as location of the vehicle using GPS, the inflation of tires using sensors, the speed of the car at any given time and the path that is driven. These computers are wirelessly connected to more third parties than most drivers realize: Internet services providers (ISPs) enabling in-vehicle Internet access; OnStar and similar services that support emergency help; and, increasingly, auto insurance companies, individual US state transportation agencies, social media sites and a wide range of others.[23] And now there are confirmed instances of being able to hack into automobiles, such as when hackers demonstrated that they could take over a Jeep Cherokee, changing the cooling settings, the heating of the seats, the radio, the windshield wipers and disabling the accelerator.[24] US senators reacted quickly, proposing new legislation on the same day the news broke that would require the US National Highway Traffic Safety Administration (NHTSA) to set standards to ensure that all wireless access points of a vehicle are secured and built with technology to detect and stop a hack in real time. The proposed legislation also includes rules to force car companies to make customers aware of the data collected about them and their use of the car.[25] IA professionals need to stay on top of this to ensure that the automobiles they use for work have such connectivity appropriately secured.

> "Security is typically not even considered during the architecting and design of IoT devices."

SMART DEVICE MANUFACTURERS ARE NOT BUILDING IN SECURITY

Many of the hundreds of clients of information security and privacy services are start-ups, or small to mid-size technology companies, and many of them offer services and devices for the IoT. It is disappointing, and alarming in many ways, that most are not following long-standing systems engineering and programming design due diligence and testing rigor. One start-up technology company even explained they did not need change control procedures because they "use Agile Programming."[26]

In fact, security is typically not even considered during the architecting and design of IoT devices. At a discussion of the design of IoT devices at the 2015 US Consumer Electronics

Week show, a panel member stated that, "Security is not prevalent in the minds of the [IoT] architects."[27] But given that a Hewlett Packard 2014 IoT survey found that 70 percent of IoT devices were found to have significant security vulnerabilities,[28] this should not really be a surprise, should it?

The following discussion took place between a privacy professional and a medical device engineer after the engineer advised the privacy professional that the implantable device he engineered and maintains, which sustains the lives of hundreds of those using it, has absolutely no security controls built in.

Privacy professional: Are you not concerned that those using your medical device, with no access controls and no encryption and no antimalware, could be accessed inappropriately and bring harm to the patient wearing it?

Engineer: No. The data transmission and control are using short-range radio frequency identification (RFID). You would have to be right next to the patient to even access the device.

Privacy professional: But how is that near-vicinity access made?

Engineer: Using an app. It collects the data, changes controls, and a bunch of other stuff to maintain the device.

Privacy professional: How do you do maintenance on the devices then? Do you visit each patient? That seems time-consuming and nearly impossible considering all the patients who use your device.

Engineer: Oh, I can do that remotely. I go to a web site that communicates with the app to access the devices, based on the device number and/or patient name, depending upon how it is set up.

Privacy professional: So, I could access the device if I could get into the web site and find a device name or number.

Engineer: Yes, that is just what I said.

Privacy professional: So then I would not need to be right next to the patient to change the controls, would I?

A long, productive discussion followed.

FALSE ARGUMENTS AGAINST SECURITY AND PRIVACY CONTROLS

There are many other false arguments that can be heard, in person as well as in print and online, for why IoT device engineers and manufacturers cannot, should not and/or will not build in the necessary data security controls. Some of the most common false arguments include:

- **Nothing bad, related to security or privacy, can happen with the IoT device.** Wrong. Oftentimes, the engineers and manufacturers do not consider all the access paths that exist to the device. They often consider only the access point in the device itself. Once they thoughtfully consider all the ways in which access can be made, they should then understand the ways in which bad things can happen with regard to security, privacy and even safety.
- **Addressing security and privacy kills innovation.** Wrong. Actually, if privacy is purposefully addressed within new innovations, it expands and improves innovations. It does not inhibit them. The public is demanding that privacy be protected.[29] Privacy should be viewed as not just a differentiator or something to be done if legally required, but a standard requirement for any new technology or service involving personal data. It takes more innovation to create secure devices that mitigate privacy risk than it does to simply leave out such controls.[30]
- **Security is too expensive to build in.** Wrong. A medical device manufacturer once told this author how much he paid for marketing: "Somewhere in the mid-six-figures." When asked how much he spent on security, he replied, "As little as possible. If we stay below five figures we are happy." It is easy to see where his priorities lie, which is alarming considering an unsecured medical device can have dire health consequences for the patient using it.
- **Privacy cannot be built in.** Wrong. This is a widespread conundrum for IoT device engineers. And no wonder, considering privacy is a very fuzzy topic with a history of no specific actions provided for engineers to follow. This is changing. More instruction is being provided in various university[31] and professional classes, such as those provided at ISACA® conferences.[32] And more tools are being created, such as the upcoming *ISACA® Privacy Principles and Program Management Guide* (expected in early 2016).
- **Consumers do not care about privacy.** Wrong. Most people do care about privacy. A Pew research study reported that 91 percent of adults surveyed care about their privacy, but feel as though they have no control over how their personal information is collected and used by companies.[33] More consumers will be demanding that the devices they use have security and privacy controls built in.[34]

SMART DEVICES NEED TO HAVE SECURITY AND PRIVACY BUILT IN

IoT devices act as:

- Data collectors
- Data storage devices
- Data processors
- Data servers
- Access paths between devices

The risk associated with each device and all these different actions must be considered and appropriately addressed and mitigated.[35] The storage capabilities of the tiniest microchips are increasing by leaps and bounds and new storage warehouses are being built specifically for IoT devices.[36] All these data can provide insights into the individuals' lives who are using the devices. These data need to be protected and deleted when no longer necessary. And the data collected should be limited to only what is necessary to support the purpose of the device.[37] A large portion of smart devices are controlled by apps, which themselves typically have a multitude of security and privacy vulnerabilities. According to a 2015 study, 90 percent of mobile banking apps are vulnerable.[38] The banking industry is one of the most highly regulated and audited industries. If the apps it uses are this bad, think how much worse other apps are in industries with less, or no, regulation.

Additionally, the privacy harms that can result from the devices must also be considered and appropriately mitigated.[39]

Another problem is that architects who do try to build in security controls are constraining themselves to consider only existing and past types of security controls, which often do not lend themselves well to IoT devices. These new and different types of user interfaces require new solutions for the long-existing security concepts and risk that must be mitigated. For example, biometrics could be used in ways it currently is not. Location-based controls, which seem to have fallen out of favor as a viable security control in the past couple of decades, could also be used in a wide range of ways to provide security to smart devices.

Considerations for including security and privacy controls into IoT devices often stop at legal requirements. And considering there are few laws and regulations that are written in such a way that they would apply to IoT devices, this is another reason why those devices predominantly lack effective security and privacy controls.

The recent ISACA IoT survey[40] revealed that 49 percent of survey participants viewed wearables and other IoT devices as security threats to the workplace, and 25 percent were concerned with the privacy risk associated with them. However, 56 percent of those responding to the survey did not have policies and procedures covering the use of IoT devices. IA professionals need to address this.

WHAT TO DO GOING FORWARD?

In January 2014, an ISACA webinar titled "Where Do You Draw the Creepy Line?"[41] was attended by several thousand participants. It described the basic risk involved with IoT and with using big data analytics on all the data collected by the devices. Those basic risk factors and concerns are expanding.

As discussed during the webinar, actions need to be taken to address the risk associated with IoT. Here are some recommended actions:

- **Look forward.** Make sure someone in the organization is monitoring IoT developments, notices whenever a department or team within the business starts using them and when employees start bringing them into the business environment. One tool that should be of interest to IT personnel who are keeping an eye on this is Shodan, a search engine for IoT.[42]
- **Look at the emerging IoT standards.** There are many to consider, and many more in the works. Here are just a few:
  - Institute of Electrical and Electronics Engineers (IEEE): The Privacy and Security Architecture for Consumer Wireless Devices Working Group (COM/SDB/P1912 WG) initiative kicked off in July 2015.[43]

  - Open Web Application Security Project (OWASP): Internet of Things (IoT) Top 10 project, "designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies."[44]
  - NIST: The NIST Engineering Laboratory Cyber-Physical Systems (CPS) and Smart Grid Program Office is leading the Cyber-Physical Systems Public Working Group (CPS PWG) "to help define and shape key aspects of CPS to accelerate its development and implementation within multiple sectors of our economy." Through its five subgroups, the CPS PWG is preparing a CPS Framework.[45]
- **Address long-standing data security core concepts.** Make sure change controls, access controls, and other long-time information security practices are implemented not only within the IoT devices, but also in the rules for using IoT devices for business and within business environments. Build in controls from the beginning of device design and planning engineering.
- **Build in strong authentication.** Do not simply connect to specific IP addresses as a method of authentication. IP addresses can easily be spoofed. The risk of using IP addresses has already been demonstrated several times, such as for medical devices.[46] Always require default passwords to be changed before they are used for the first time.
- **Encrypt data.** Encrypt not only the wireless data transmissions, but also the data in storage. And, no, encryption does not take up that much of the IoT device resources to justify leaving it out.
- **Log access to the IoT device.** Log who accessed the device, what he/she did to the device and with the data, and when he/she did the accessing.
- **Embed antimalware within the device.** These smart devices are often more susceptible to malicious malware than other types of computing devices, as has been demonstrated by hacks into health care systems via unsecured medical devices using malware.[47]
- **Protect entry points.** Build in protection from port scans and other penetration tools.
- **Keep the devices updated.** Establish procedures to deploy firmware updates to fix discovered vulnerabilities. Yes, this can be accomplished.
- **Secure the IoT device perimeter.** This requires strongly securing the apps and clouds used in conjunction with the devices.
- **Watch third parties.** Establish oversight of third parties used to support the IoT devices and ecosystem.[48]
- **Consider privacy and safety harms.** IoT device makers must start looking at how their products could cause harm to those using them. Determine and mitigate the potential safety and privacy harm to those who will be using the devices.[49]
- **Establish IoT rules and boundaries.** For those businesses using smart devices, and where their employees are using IoT devices, establish policies and procedures that clearly describe the boundaries within which IoT devices can be used.[50] Organizations creating IoT devices need to create the rules for the necessary data security and privacy controls that must be built into the devices.

ENDNOTES

1 Brownlee, Lisa; "The $11 Trillion Internet of Things, Big Data and Pattern of Life (POL) Analytics," *Forbes*, 10 July 2015, *www.forbes.com/sites/lisabrownlee/2015/07/10/the-11-trillion-internet-of-things-big-data-and-pattern-of-life-pol-analytics/*

2 Arthur, Charles; "The History of Smartphones: Timeline," *The Guardian*, 24 January 2012, *www.theguardian.com/technology/2012/jan/24/smartphones-timeline*

3 In September 2014, the number of unique mobile users passed 3.6 billion, or 50 percent of the world's population. The number of mobile devices surpassed the world's population in December 2014. In 2015, for the first time, more than one quarter of the global population will use smart phones. By 2018, more than one-third of consumers worldwide, or 2.56 billion people, will use smart phones, according to eMarketer. That figure represents more than half of all mobile phone users. FIPP, *www.fipp.com/news/fippnews/is-the-importance-of-mobile-exaggerated*

4 Franzen, Carl; "Dick Cheney Had the Wireless Disabled on His Pacemaker to Avoid Risk of Terrorist Tampering," The Verge, 21 October 2013, *www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007*

5 See: Herold, Rebecca; session at the 201410X Medical Device Conference, *https://www.youtube.com/watch?v=_aqOOPUwJhE*

[6] National Institute of Standards and Technology, NIST Smart Grid Collaboration Wiki for Smart Grid Interoperability Standards, USA, *http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy*

[7] Smart Grid Interoperability Panel, Smart Grid Cybersecurity Committee, *www.sgip.org/SGCC*

[8] Smart Grid Interoperability Panel, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, September 2010, *www.nist.gov/smartgrid/upload/nistir-7628_total-2.pdf,* and NISTIR 7628 Revision 1, 2014, *http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf*

[9] Herold, R.; C. Hertzog; *Data Privacy for the Smart Grid*, CRC Press, 2015, *www.crcpress.com/Data-Privacy-for-the-Smart-Grid/Herold-Hertzog/9781466573376*

[10] *Corporate Wellness Magazine*, "Wearable Devices are Coming to a Doctor Near You," 3 April 2015, *www.corporatewellnessmagazine.com/technology/wearable-devices-coming-to-a-doctor-near-you/*

[11] Rosenbrock, K.; "Do Fitness Trackers Really Work for Weight Loss?" *The Active Times*, 19 March 2015, *www.theactivetimes.com/do-fitness-trackers-really-work-weight-loss*

[12] Young, E.; "Do You Want Your Company to Know How Fit You Are?" BBC News, 17 July 2015, *www.bbc.com/news/business-33261116*

[13] Your Security Resource, "How Private Is the New Amazon Echo?" *www.yoursecurityresource.com/expertqa/how-private-is-new-amazon-echo/index.html#.Va_rdPlViko*

[14] Associated Press, "Hackers Post Webcam, Security Camera, Baby Monitor Video Online," CBC News, November 2014, *www.cbc.ca/news/technology/hackers-post-webcam-security-camera-baby-monitor-video-online-1.2841770*

[15] Phillips, C.; "Privacy Fears Over Samsung's 'Orwellian' Smart TV," *Newsweek*, 9 February 2015, *www.newsweek.com/privacy-fears-over-samsungs-orwellian-smart-tv-305532*

[16] Christian, S.; "British Gas Works to Address New Security Threats and Conquer the Smart Home," Verimatrix, 30 June 2015, *www.verimatrix.com/blog/201506/british-gas-works-address-new-security-threats-and-conquer-smart-home*

[17] Howard, P.; "The Internet of Things Is Poised to Change Democracy Itself," Paxtechnica, 1 July 2015, *http://paxtechnica.org/?p=789*

[18] O'Brien, J.;"Police Warn Monitors Susceptible to Hackers After Middlesex Centre Incident," 23 July 2015, *www.lfpress.com/2015/07/23/police-warn-monitors-susceptible-to-hackers-after-middlesex-centre-incident*

[19] Federal Trade Commission,"Marketer of Internet-connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy," USA, 4 September 2013, *www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles*

[20] *Brooklyn Daily Eagle*, "Schumer Warns of Webcam, 'Smart' TV, Baby Monitor Hackers," December 2014, *www.brooklyneagle.com/articles/2014/12/1/schumer-warns-webcam-%E2%80%98smart%E2%80%99-tv-baby-monitor-hackers.*

[21] Chipsetc, "Computer Chips Used in Cars," *www.chipsetc.com/computer-chips-inside-the-car.html*

[22] *Popular Mechanics*, "How it Works: The Computer Inside Your Car," 21 February 2012, *www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/*

[23] Massachusetts Department of Transportation, How E-ZPass Works, USA, *www.massdot.state.ma.us/highway/TrafficTravelResources/EZPassMAProgram/HowEZPassWorks.aspx*. Lanctot, R.; "Losing Facebook," 28 June 2015, *www.linkedin.com/pulse/losing-facebook-roger-c-lanctot*

[24] Greenberg, A.; "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, 21 July 2015, *www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/*

[25] Trujillo, M.; "Senators Seek Privacy, Anti-hacking Safeguards in Cars," *The Hill*, 21 July 2015, *http://thehill.com/policy/cybersecurity/248636-senators-want-privacy-hacking-safeguards-in-cars*

[26] Herold, R.; "Change Controls Are Still Necessary," *The Privacy Professor*, Dell Insight Partners, *http://privacyguidance.com/blog/change-controls-are-still-necessary/*

[27] CE Week New York 2015, "Tackling Connected Car Security and Privacy Concerns Highlights" panel discussion, *https://youtu.be/w8ShDE6RE6M*

[28] Hewlett-Packard Development Company, *Internet of Things Research Study*, USA, 2014, *www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf*

[29] Madden, M.; "Public Perceptions of Privacy and Security in the Post-Snowden Era," Pew Research Center, November 2014, *www.pewinternet.org/2014/11/12/public-privacy-perceptions/*

[30] Thierer, A.; "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation," Social Science Research Network, 18 February 2015, *http://ssrn.com/abstract=2494382*

[31] Carnegie Mellon University, "Engineering Privacy in Software," course description, Pittsburgh, Pennsylvania, USA, *www.cs.cmu.edu/~breaux/teaching-08605sp14.html*

[32] ISACA, EuroCACS/ISRM 2015, November 2015, *www.isaca.org/ecommerce/Pages/eurocacs-isrm.aspx*

[33] *Op cit*, Madden

[34] Hulme, G. V.; "Want Good IoT Security? It's Up to Each and Every One of Us," CSC Blogs, 23 July 2015, *http://blogs.csc.com/2015/07/23/want-good-iot-security-its-up-to-each-and-every-one-of-us/*

[35] Sarma, S.; "I Helped Invent the Internet of Things. Here's Why I'm Worried About How Secure It Is," *Politico*, June 2016, *www.politico.com/agenda/story/2015/06/internet-of-things-privacy-risks-security-000096?cmpid=sf*

[36] M2X, IoT Cloud-based Data Storage Service and Management Tool, AT&T, *https://m2x.att.com/*

[37] Herold, R.; "Data Collection Must be Limited for Internet of Things Privacy," *The Privacy Professor*, 30 January 2015, *http://privacyguidance.com/blog/data-collection-must-be-limited-for-internet-of-things-privacy/*

[38] Chettri, S.; "'90% of Mobile Banking Apps Are Vulnerable' Study," *Hindustan Times*, 19 April 2015, *www.hindustantimes.com/business-news/90-of-mobile-banking-apps-are-vulnerable/article1-1338449.aspx*

[39] Herold, R.; "Organizations Must Consider Privacy Harms," *The Privacy Professor*, 2015, *http://privacyguidance.com/blog/organizations-must-consider-privacy-harms/*

[40] ISACA, *Internet of Things: Risk and Value Considerations*, USA, 2015, *www.isaca.org/knowledge-center/research/researchdeliverables/pages/internet-of-things-risk-and-value-considerations.aspx*

[41] ISACA, "Where Do You Draw the Creepy Line? Privacy, Big Data Analytics and the Internet of Things," webinar, 9 January 2014, *www.isaca.org/Education/Online-Learning/Pages/Webinar-Where-do-you-draw-the-creepy-line-Privacy-big-data-analytics-and-the-Internet-of-things.aspx*

[42] Shodan, *www.shodan.io/*

[43] IEEE Standards Association, Privacy and Security Architecture for Consumer Wireless Devices Working Group (COM/SDB/P1912 WG), *http://grouper.ieee.org/groups/1912/meeting_information.html*

[44] Open Web Application Security Project, OWASP Internet of Things Top 10, *www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project*

[45] National Institute of Standards and Technology, Cyber-Physical Systems, USA, *www.nist.gov/cps/*

[46] Bonderud, D.; "Do No Harm? Medical Device Vulnerabilities Put Patients at Risk," The MSP Hub, 28 May 2015, *http://themsphub.com/do-no-harm-medical-device-vulnerabilities-put-patients-at-risk/*

[47] Jackson-Higgins, K.; "Hospital Medical Devices Used as Weapons in Cyberattacks," *Information Week Dark Reading*, 8 June 2015, *www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751*

[48] Herold, R.; "Will Your Contractors Take Down Your Business?" *The Privacy Professor*, May 2015, *http://privacyguidance.com/blog/will-your-contractors-take-down-your-business/*

[49] Herold, R.; "Organizations Must Consider Privacy Harms," *The Privacy Professor*, 12 May 2015, *http://privacyguidance.com/blog/organizations-must-consider-privacy-harms/*

[50] Herold, R.; "How Businesses Can Reduce Wearables Security & Privacy Risks," *The Privacy Professor*, 12 March 2015, *http://privacyguidance.com/blog/how-businesses-can-reduce-wearables-security-privacy-risks/*