Business Horizons (2016) 59, 615—622

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY
www.elsevier.com/locate/bushor

Wearing safe: Physical and informational security in the age of the wearable device

Adam J. Mills [a,*], Richard T. Watson [b], Leyland Pitt [c], Jan Kietzmann [c]

[a] Loyola University New Orleans, 6363 St. Charles Avenue, Box 15, New Orleans, LA 70118, U.S.A.
[b] Terry College of Business, University of Georgia, Athens, GA 30602-6269, U.S.A.
[c] Beedie School of Business, Simon Fraser University, 500 Granville Street, Vancouver, BC V6C 1W6, Canada

KEYWORDS
Wearable technology;
Wearables;
Information security;
Cybersecurity

Abstract Wearable computing devices promise to deliver countless benefits to users. Moreover, they are among the most personal and unique computing devices of all, more so than laptops and tablets and even more so than smartphones. However, this uniqueness also brings with it a risk of security issues not encountered previously in information systems: the potential to not only compromise data, but also to physically harm the wearer. This article considers wearable device security from three perspectives: whether the threat is to the device and/or the individual, the role that the wearable device plays, and how holistic wearable device security strategies can be developed and monitored.

1. The rise of wearables

In 1903 at the Royal Institution in London, physicist John Ambrose Fleming was preparing the setup of a primitive projection device intended to display Morse code messages from his colleague Guglielmo Marconi, the inventor of wireless telegraphy. Supposedly, this method of transmitting information was secure. Yet before the demonstration had even started, the audience was surprised, baffled, and amused to hear a series of messages being tapped out. The first messages were simply the word "rats" being tapped, but what followed was more complex and insulting to Marconi. A limerick began, "There was a young fellow of Italy, who diddled the public quite prettily. . . " The damage had been done; wireless telegraphy was clearly nowhere near as secure as Marconi had claimed. A few days later, the magician and inventor Nevil Maskelyne claimed responsibility for this first recorded instance of the hacking of an information system (IS) (Marks, 2011).

Whether for mischief or for malice, no system has ever been completely immune from hacking or compromise since Maskelyne's trick. In the 1960s, John Draper (aka Captain Crunch) used a toy whistle from a Cap'n Crunch cereal box to trick AT&T's telephone system into allowing him to place free long distance calls. In 1965, the Compatible Time-Sharing System on IBM's 7094 machine was hacked for the first time.

* Corresponding author
E-mail addresses: ajmills@loyno.edu (A.J. Mills), rwatson@terry.uga.edu (R.T. Watson), lpitt@sfu.ca (L. Pitt), jan_kietzmann@sfu.ca (J. Kietzmann)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.08.003

Mainframe systems were targeted from then on, and the first PC virus, Brain, was accidentally created by Pakistani programmers Basit and Amjad Farooq Alvi in 1986. Keeping systems, networks, and individual devices secure became a critical part of the IS professional's role. These cybersecurity issues have escalated at an exponential rate as massive data breaches at firms such as Target and Sony grabbed headlines, identity theft became a nightmare for thousands of individuals, and the security of smartphones also came under threat. Even technologies traditionally regarded as 'not IT' showed their vulnerability: distraught parents found their baby monitoring devices were exposed, and hackers brought a Jeep Cherokee to a standstill on a highway by remotely compromising its control systems. Now the most personal information technologies of all are under threat; we have entered the age of the wearable computer.

Wearable computers, or wearable information technologies ('wearables'), represent a huge future market. By the end of 2015, 6.1 million U.K. citizens (13% of the population) owned a wearable, and the product category on Amazon has enjoyed a triple-digit sales increase year-over-year since the company launched its first wearable offerings. The consulting firm IDTechEx predicts the wearables market will grow from $20 billion in 2015 to almost $70 billion in 2025. In November 2015, according to the analyst firm Canalys, sales of Apple's watch had reached nearly 7 million since its April launch (Lamkin, 2015). Wearables are arguably the most personal and intimate IT devices of all, portending enormous benefits of all kinds for individuals and organizations alike. However, being more personal and more intimate makes their security even more critical. Protecting the security of wearable devices and highly personal data will pose enormous challenges to organizations in general, and to IS practitioners in particular. We address these issues in this article.

We proceed as follows: First, we provide a brief overview of the unique nature of wearables. Then we argue that security in the case of wearables is different from other devices, and even more important. Next, we suggest two frameworks managers can use to think about device security and shape their strategies accordingly. We suggest the use of the McCumber cube (McCumber, 2004) as a lens through which to view and consider wearable technology security strategy. The article concludes with an integration of the three frameworks.

1.1. When we wear computers

Humankind has long worn the products of technology. Early warriors wore animal skins in order to protect themselves from clubs and arrows, and the Greeks and Romans wore metal body armor long before the knights of medieval times. The first wristwatch was made for the queen of Naples in 1810. However, it was not until the 1960s that people began to experiment with the wearing of computerized devices. Among the first of these was the Gambling Shoe in 1961. Built by MIT students, this wearable device applied mathematical theories to attempt to beat the roulette wheel in casinos. A computer strapped to the player's waist translated a signal from a sensor in the player's shoe, used to track the timing of the roulette wheel, into an audio-based result that was sent to his earpiece.

Today, wearables are no longer reserved for such special applications. Wearable technologies (Table 1) now refer to a concept that describes

Table 1. Where is the technology worn?

Anatomy	Device Examples	Application Examples
Head	Cap, eyes, glasses, ears	Monitor fatigue, portable computer
Neck	Necklace, chain, tie	Smartphone control, camera
Torso	Shirt, jacket, band	Monitor health, posture
Waist	Belt, fob	Monitor activity, identification and location
Upper arm	Band	Monitor activity, enhance lifting strength
Lower arm/wrist	Band, watch	Monitor fitness activity, interact with smartphone, portable computer
Hand	Ring, glove	Unlock doors, connect people, interact with touch screens in winter, SIRI/Cortana/Google Now enabled
Upper thigh	Band, pants	'Smart jeans' enable smartphone interaction, enhance physical strength
Lower leg	Socks, band	Pressure sensors monitor foot injury, posture
Foot	Sock, shoe	Navigation, fitness

how people can wear a wide range of information technology devices (e.g., watches, glasses, shoes) on almost any part of the anatomy (Robson, Pitt, & Kietzmann, 2016). There are now many hundreds of wearable devices, and the list grows by the day. These technologies can monitor, control, optimize, and even become autonomous (Porter & Heppelman, 2014) in a wide range of functions and behaviors.

Wearables can be relatively simple both in their technology and their application. For example, Air New Zealand now gives unaccompanied minors a bracelet to wear when they check in for a flight. The bracelet is scanned at various checkpoints on their journey, including check in, boarding, landing, and handover. Up to five nominated parents or guardians are alerted when the child passes a checkpoint, and in this way updated with the child's step-by-step progress on their journey. Other wearables are more complex. In 2014, Google unveiled a prototype smart contact lens to monitor the blood glucose levels contained in human tears. This promises a solution to the problem of effective blood glucose monitoring and control for people with diabetes.

2. Why wearable device security is different

While security is obviously important to all information systems, in the case of wearable devices the nature of the security challenge is sufficiently different and warrants special attention. First, wearables are by far the most personal computing devices. While the settings might be slightly different, it is easy for one person to use the desktop or laptop computer of another. Indeed, it turned out that the personal computer wasn't nearly as personal as other devices. While mobile phones, for instance, are a lot more customized to the individual, it is still relatively easy for one person to use the smartphone or tablet of another. However, most wearables are, or will be, unique (e.g., Watson, Pitt, Berthon, & Zinkhan, 2002, 2004) to the wearer. They are close and personal, intimate devices that will fit the particular wearer's anatomy. These devices monitor, control, and in many cases optimize tasks ideally and only for that individual. They become part of the anatomy, as in the case of the diabetic contact lenses, or robotic arms that afford the wearer far greater lifting strength.

Second, because people will wear these devices, fashion becomes very important. One of the major criticisms of Google's Glass spectacles was that they made wearers look like geeks and behave like 'glassholes.' Fashion comes at a price, however. Expensive wearables that are worn visibly might represent attractive targets for thieves. For example, the Brikk's Lux Watch Omni costs $114,995. It is an 18-karat gold Apple Watch with multiple rows of 11.30-carat diamonds around the face, buttons, and strap clasps.

Third, wearables are the first category of IT devices where there is not only danger to data, but also the real potential to cause physical harm to the wearer. Hacking a person's PC or laptop, or their smartphone, might enable a wrongdoer to steal data, or in some way impede the device's ability to function. However, it is unlikely that this could result in physical injury to the owner. Mischievous or malicious hacking of a wearable device can have consequences that might vary from annoying to severe. A smart watch might be programmed to emit a series of irritating but meaningless pulses for no reason at all. Hacking a diabetic's smart contact lenses to give erroneous readings could cause the wearer to either not receive warning signals or to overreact to exaggerated readings of glucose levels. This might not only have serious consequences, but it could also prove fatal. In the following section we suggest two frameworks that IS decision makers can use to consider the issues surrounding wearable device security.

3. Wearable device security: Questions and frameworks

The unique nature of wearables and the implications this has for security discussed above require that the manager consider three distinct, but related sets of issues. The first question pertains to *who or what* is threatened: The wearer or the wearable? This question is addressed by means of the 4Ds grid discussed below. The second question considers whether the wearable device focuses on the wearer's physical or mental capacities, and specifically what abilities of the wearer the device enhances. Managers and security professionals can explore the different *roles* that wearables can play, and how wearable technology security can be breached by using the 4Ms matrix, introduced later. The third question concerns *how* managers can develop a security strategy to address the potential vulnerabilities of wearables. We suggest the McCumber cube as a suitable device for achieving this.

3.1. Threats to the individual and to the device: The 4Ds grid

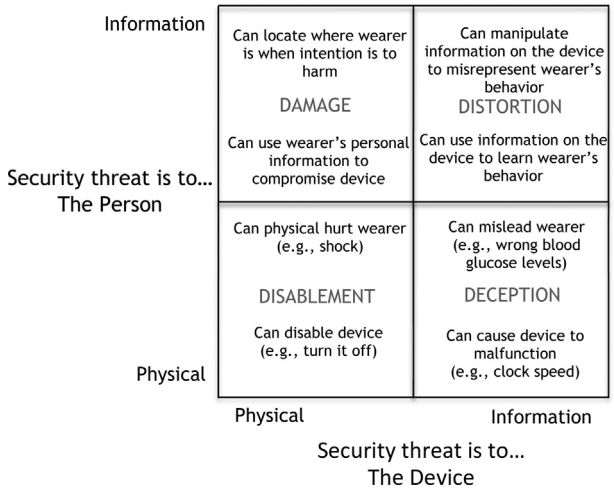
Throughout their relatively short history, information devices—such as PCs, laptops, tablets, and smartphones—have been vulnerable to two kinds of security threats. First, if compromised, the data

stored on or via the device (e.g., downstream, in the cloud) can be destroyed, stolen, or changed with negative consequences for the owner. Second, it is technically feasible that malicious hackers could also cause physical damage to the computing device itself. A program that over-exerted the central processing unit (CPU) could eventually damage the CPU. Stressing the graphics-processing unit (GPU) could have similar consequences. Flashing the BIOS and/or firmware could effectively 'brick' a computer's motherboard, making it impossible to turn on; smartphones have been vulnerable to similar issues. Historically, people have been at minimal physical risk when the security of their computing devices has been breached. The fact that wearable devices are worn on the anatomy changes that. While wearers have long been at informational risk—their data could be destroyed, changed, or stolen—they are likely also at physical risk in the age of the wearable.

The 4Ds grid (Figure 1) summarizes this situation with regard to threats and serves as a tool for IS decision makers and security experts to explore the various threats breaches in security of a wearable device represent. It asks, what is the nature of the threat: disablement, damage, deception, or distortion?

In the bottom left quadrant of the grid is the *disablement* threat, because the effect of a security breach on both the wearer and the device is that the physical attributes of either one or both can be compromised. The device could be disabled by a hacker, either by impairing it or by simply turning it off remotely so that it no longer operates. Alternatively, the device can be breached in such a way that it can disable the physical performance of the wearer, even to the point of injury. Examples of this could vary from initiating a sudden shutdown in a powered exoskeleton arm that makes the wearer suddenly drop what they are carrying to causing injury through a smart watch that delivers a shock through its haptic apparatus.

Figure 1. The 4Ds grid — Threats to individuals and devices



The *damage* quadrant encompasses security threats where the device is compromised physically, but the wearer's information—rather than physical well-being—is now at risk. Simple hacking of the device could cause a person to either lose all of their data, or have it stolen or changed. Since many wearable devices will be connected to a wearer's other information systems, such as smartphones and computers, they might possibly be used as gateways to the larger data stored on this kind of equipment. The wearable might also be used to locate a particular wearer, with the intention to harm them or their devices, or to breach their property.

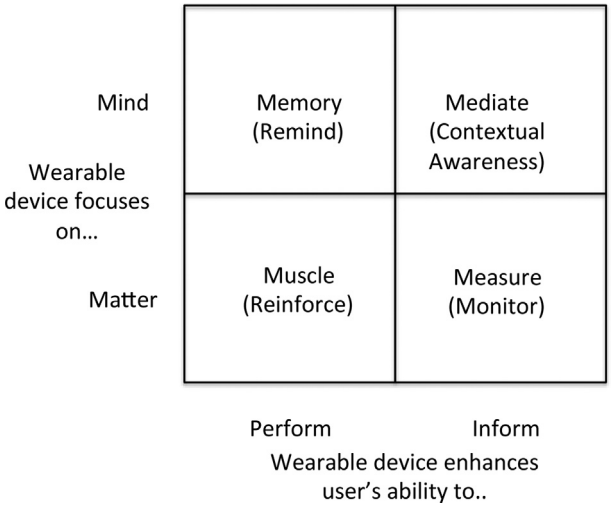
The bottom right cell of the grid has to do with *deception*, where the security breach on the device is informational but the effect on the user is physical. For example, the malicious changing of the data on a medical wearable might cause it to give the wearer wrong information with regard to measures such as blood glucose or blood pressure. This might either cause the wearer to be lulled into a false sense of security or to overreact to an erroneous reading—perhaps by changing the dosage of their medication—when, in fact, nothing was wrong at all.

Distortion is at the heart of the top right quadrant, where—in the case of both wearer and device—the breach is informational. By breaching a device's information security, a third party might learn a lot about a wearer's behavior for malevolent purposes. Alternatively, the information on a wearer's device could be manipulated to relay false information about a person's behavior, such as that they were complying with a medical regimen when they were not, or causing a physician to prescribe additional medication when the patient did not need it.

3.2. The roles that wearables play: The 4Ms matrix

The next decision tool for managers to use in their consideration of wearable device security asks two questions. First, what is the focus of the wearable? Is it on cognitive ability, and how this can be enhanced; or is it on the physical? Is the focus on the mind or the matter? Second, what ability does the wearable enhance—to better inform the wearer, or to better perform tasks? This enables us to identify four distinct roles wearable technology can play. We term these roles the 4Ms, illustrated in Figure 2. Understanding these roles should give managers a good perspective on exactly how a

Figure 2. Understanding the roles of wearables



wearable device can have its security compromised and how this could, in turn, affect the wearer.

The *muscle* quadrant is the one in which the wearable device focuses on physical things (i.e., the matter) such as lifting or moving objects, or performing fine tasks at much higher accuracy. These devices—such as exoskeleton arms, which give laborers the ability to lift a lot more weight, or smart gloves that permit surgeons to work with enhanced precision—enable the wearer to perform tasks better than they would be able to without the device. The focus is on reinforcing muscles, enhancing strength, extending endurance, or augmenting the ability to work more finely and accurately. Where muscle is the focus of the wearable, the main security threat would come from attempts to make the device perform in ways other than intended. This could either injure or hurt the wearer, or cause them to be unable to perform the task the device was intended to reinforce. A hacked exoskeleton lifting arm could be made to stall mid-lift and cause the wearer to be left holding a burden that was much heavier than they could ordinarily carry. A surgical smart glove's fineness and precision could be turned off in mid-operation, or its accuracy could be altered in a way that causes the surgeon to make mistakes and put the patient at risk.

The remaining quadrants focus on the mind. One of the main applications of wearables is to remind wearers. Captured in the *memory* quadrant, this might be something as simple as a smart watch reminding a sedentary office worker to stand up and move about if they have been inactive for too long, or it might be a more complex function, such as using smart spectacles or a headset to access a database while on the job. Disabling, or changing the frequency of 'stand up' reminders on a smart watch might merely be annoying to the wearer. However, when the data being fed to a smart headset is tampered with in a way that misleads or confuses the wearer, the consequences can be far more serious.

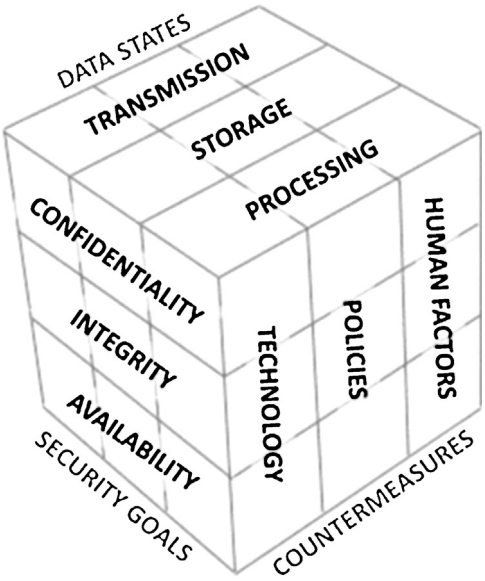
In the *measure* quadrant the wearable device enhances the wearer's ability to keep informed about physical attributes. Medical devices that measure and monitor physical signals on the human anatomy are an example of this. A band on a pregnant mother's abdomen can monitor a fetal heart beat and relay this to her obstetrician. It might be susceptible to malicious or mischievous hacking. If the device got a critical measurement wrong and reported incorrectly, the mother or the obstetrician could either overreact (e.g., adjusting their treatment) or underreact by doing nothing when they should take corrective steps. Both of these conditions could be injurious and, in some instances, fatal.

Finally, the main consequence of compromising a wearable in the *mediate* quadrant is that the device will fail in its task to inform the wearer when its focus is on the wearer's cognitive abilities. Stated differently, the device might fail in its task of optimizing the wearer's contextual awareness. The Safelet (http://www.safelet.com) is a smart bracelet that alerts others to the wearer's geographic presence when they might be alone in a potentially dangerous area at night, for example. If the device were to mislead the recipients of the signals into believing that the wearer was safe, when in fact they weren't, the consequences could be serious. The Lechal (http://www.lechal.com) shoe is a device that guides the wearer using GPS information and a series of pulses in the footwear to point direction. Its purpose is to prevent users from becoming lost in unknown terrain, particularly at night, and targets the visually impaired, police, and the military. By getting the user's context wrong, compromised footwear could cause them to become lost, or place them in a threatening environment.

3.3. The McCumber cube

A basic premise of cybersecurity is that organizations need to protect the confidentiality, availability, and integrity of their data (i.e., *security goals*) during its transmission, processing, and storage (known as *data states*) using technology, policy, and people appropriately (i.e., *countermeasures*). The McCumber cube (see Figure 3) allows managers to focus on each one of these elements individually before concentrating on their interconnectedness. Since the security of the information system relies

Figure 3. McCumber cube*



*Source: Based on McCumber (2004)

on the joint optimization of all these elements, the McCumber cube also reminds managers not to focus on one of the elements to the exclusion of others (e.g., on technology over people).

3.3.1. Security goals

Three security goals—confidentiality, integrity, and availability, also known as 'the CIA of data security'—are the main objectives that assure data is not lost when critical issues arise (e.g., natural disasters, technology malfunction, theft). Confidentiality refers to the goal that sensitive information is not intentionally or accidentally disclosed or made available to unauthorized individuals, entities, or processes. This is usually achieved through the encryption of data and password protection of wearables devices. Many wearables today, though, are completely unprotected. Integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means data cannot be modified in an unauthorized or undetected manner. Often, integrity can be achieved by keeping backup data or logging user activities to monitor whether data has been compromised. On wearables, this is hardly ever the case. Availability means that authorized individuals and processes need to have timely and reliable access to data and other resources for any IS to serve its purpose. Traditional enterprise information systems are backed up regularly and off-site, and organizations implement strong data recovery procedures to assure reliable access to data.

3.3.2. Data states

The three states of digital data are storage (i.e., data-at-rest), transmission (i.e., data-in-transit), and processing (i.e., data-in-use). Storage refers to inactive data-at-rest, whether this is on the wearable device itself, on a connected smart device, or in the cloud. On wearables, a lot of data are stored because of the interconnected nature of the backend databases and the need for historic reference (e.g., workout data over time). Transmission relates to data-in-transit between information systems, either over public or untrusted networks such as the internet or over more secure, private networks. For many wearables, this refers mainly to basic, unsecured Bluetooth connections or wi-fi networks that pair wearable devices with other technology, typically other mobile devices (e.g., smartphones). Both are relatively easy to breach with brute-force attacks.[1] Processing refers to data-in-use, to data in computer memory currently being processed by applications either on wearable devices, on mobile devices, or in the cloud. Data-in-use can contain digital certificates, encryption keys, and personally identifiable information, which makes it particularly attractive to hackers who can then use the compromised data to gain access to stored data.

3.3.3. Countermeasures

Security countermeasures aim to eliminate or prevent threats by minimizing their probability and/or reducing the harm attacks can cause. In the McCumber cube, these countermeasures are divided into human factors, organizational policies and practices, and security solutions embedded in technologies. Human factors refer to those individuals who use and administer information systems. In many cases, employees are the weakest link in organizational information systems (e.g., passwords kept on Post-it notes, sensitive data stored on unprotected USB drives). Measures are put in place to mitigate these risks, including narrowly-defined roles (e.g., read/write permissions) and responsibilities for everyone, end-user training for device use, and the education of potential threats and how to circumvent or report these.

Policy and practices refer to organizational, administrative controls that govern how data and information security are to be managed within a firm. They include policies for managing risks related to the use, storage, and transmission of data, and acceptable use policies users must agree to before

[1] See http://www.itbusinessedge.com/slideshows/five-potential-security-concerns-related-to-wearables-05.html

they can gain access to corporate devices, networks, or the internet. Some firms maintain a formal computer emergency response team (CERT) or computer security incident response team (CSIRT), while many others maintain flexible BYOD (bring your own device) practices for wearable devices, making their use particularly challenging to manage. Especially since many wearables include cloud-based services, the contractual agreements with third parties are also of tremendous importance. Technology refers to the software- and hardware-based solutions designed to protect information systems, including anti-virus software, firewalls, and intrusion detection systems. Wearables are complex systems. Sensors capture signals from users and their environment to translate them into data. Micro-processors then turn the data into a transmittable format, where transmitters send the data on to other processing or storage technologies. All of these phases need to be protected to minimize cyber threats.

Together, these three elements of cybersecurity—namely security goals, data states, and countermeasures—offer a structured approach to assessing and managing security risk in wearables information systems. The McCumber cube focuses on information (not on technologies), suggesting that the same method remains useful as technologies mature and change. More importantly, when these elements are combined, the McCumber cube reveals 27 individual cubes that offer help for managers who need to protect their wearables information system. For instance, for the combination of data confidentiality, data storage, and policies, managers ought to look very closely at contractual agreements between the wearable device vendor and any third parties they might use. How do these parties store data and how are these firms protected against breaches? Are they allowed to sell the data, either as part of their ongoing business model (e.g., to insurance companies) or in case they go out of business, like RadioShack tried when it put up consumers' personal data among the assets it tried to auction off to settle its bankruptcy (Federal Trade Commission, 2015)? In the combination of data confidentiality, data storage, and policy, how can managers ensure their employees choose strong and unique passwords in the first place? In reality, the majority of people use the same passwords across personal and corporate accounts, which is likely going to increase when personal devices such as wearables are used at work. People also frequently share passwords with team-mates, which introduces new problems when disgruntled employees leave with access to their colleagues' wearable device passwords.

Working through each of the 27 cubes allows managers to establish the information security of their wearables information system. They take into consideration how the key security goals (CIAs) related to various data states (processing, storage, and transmission) are addressed through the full range of available security measures (human factors, politics, and technology itself). The same framework can also be used to monitor and evaluate the information security of the wearables information systems over time—an important component of a firm's risk assessment and management practices. As wearables progress and people change their behavior, new threats emerge. These risk/security management practices need to be revised and improved, based at least in part on the insights gleaned through the use of the McCumber Cube. In this context, managers are advised to review the policies of their cyber liability and data breach insurances to ensure these cover breaches of wearable devices.

4. Conclusion: Are wearables a real concern?

Many of the situations described above sound like the material of conspiracy stories and science fiction novels. Hacking into wearables to change the reading of the wearer's vitals is the modus operandi of a James Bond villain rather than a target any black-hat hacker would really be interested in. But such is the world we live in today—people often violate ''computer security for little reason beyond maliciousness or for personal gain'' (Moore, 2005, p. 258). Serious vulnerabilities in several models of drug infusion pumps in hospitals have already been discovered, which allow a hacker to secretly and remotely change the amount of drugs administered to a patient (Zetter, 2015). Doing so indirectly, via wearables, is the next logical step.

However, so far no massive data breaches based on wearables have made the news. Given the steep growth projections for the sales of wearable devices and their increasing interconnectivity with other wearables and existing information systems, this lack of bad news may have lulled consumers and firms into a false sense of security. In fact, when we think of wearables today, we mainly think about harmless devices that collect data about the person and their behavior; data that is of no interest to others (e.g., workout routines, run times, sleeping patterns). But other, more permanent and important data can also be accessed through wearables, including the wearer's date of birth and social

security number. These types of personal information are many times more valuable than a stolen credit card number on the black market (Overfelt, 2015).

From a firm's perspective, there is a real concern that wearables become the new weakest technological link through which existing security measures can be bypassed, especially when these devices connect to the cloud. As more and more wearables are used for work, it is no longer just personal data that may be exposed or compromised, "but also potentially operational data, that could be sensitive in nature" (Maddox, 2015).

In the race to be first-to-market, security on wearables has not been taken as seriously as it should be by the firms who develop them, the consumers who wear them, or by the firms who adopt them into their existing legacy systems and work processes. In order to reap the organizational benefits wearable devices offer, managers need to think through the entire wearables ecosystem and develop a holistic security strategy.

In this article we discussed how wearables introduce potential vulnerabilities to the device and/or the individual (in the 4Ds framework), we described the different roles the wearable device plays (in the 4Ms framework), and how holistic security strategies for such devices can be developed and monitored. For the latter, we argue that managers need to address security risks based on not only on the hardware and software of the device, but also those related to the data they generate, the networks used, the people who have access, and the procedures and policies that deal with processing, storing, and distributing information in an organization. The McCumber cube is a framework for developing such an information assurance strategy for enterprise risk management.

The need for such strategies keeps growing for a number of reasons. Typically, legal regulatory environments adapt to technological advancement after about five years. This suggests the laws today are not equipped to address many of the new threats that arise through emerging wearable technologies. Developers of wearable technologies keep moving ahead to create newer and more powerful technological devices, further increasing the gap between technology and the laws that govern them. In this process, ongoing support for older versions is not always assured by these developers. Firms, on the other hand, are reluctant to update all the time. Together, these two divergent interests further increase security concerns of wearable information systems. All of these trends suggest that it is up to the firm to determine the level of risk it is willing to take versus the benefit it gets from wearable devices. The responsibility to develop, implement, and monitor appropriate wearable technology security strategies lies with the firm.

References

Federal Trade Commission. (2015, May 18). *FTC requests bankruptcy court take steps to protect RadioShack consumers' personal information*. Retrieved from https://www.ftc.gov/news-events/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-radioshack

Lamkin, P. (2015, November 5). Apple sales hit 7 million. *Forbes*. Retrieved from http://www.forbes.com/sites/paullamkin/2015/11/05/apple-watch-sales-hit-7-million/#826b1645c9ac

Maddox, T. (2015, January 29). Experts discuss security, privacy, and fashion trends for wearables at CES 2015. *Tech Pro Research*. Retrieved from: http://www.techproresearch.com/article/experts-discuss-security-privacy-and-fashion-trends-for-wearables-at-ces-2015/

Marks, P. (2011, December 20). Dot-dash-diss: The gentleman hacker's 1903 lulz. *New Scientist*. Retrieved from https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/

McCumber, J. (2004). *Assessing and managing security risk in IT systems: A structured methodology*. Boca Raton, FL: Auerbach Publications.

Moore, R. (2005). *Cybercrime: Investigating high technology computer crime*. Newark, NJ: Matthew Bender & Company.

Overfelt, M. (2015, December 13). The price of the wearable craze: Less data security. *NBC News*. Retrieved from http://www.nbcnews.com/tech/innovation/price-wearable-craze-less-data-security-n479271

Porter, M. E., & Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review, 92*(11), 66–68.

Robson, K. E., Pitt, L. F., & Kietzmann, J. H. (2016). *Wearables, the internet of things, and the internet of people: Converging on the internet of everything*. Report of the Advanced Practices Council of the Society for Information Management.

Watson, R. T., Berthon, P. R., Pitt, L. F., & Zinkhan, G. M. (2004). Marketing in the age of the network: From marketplace to u-space. *Business Horizons, 47*(6), 33–40.

Watson, R. T., Pitt, L. F., Berthon, P., & Zinkhan, G. M. (2002). U-commerce: Expanding the universe of marketing. *Journal of the Academy of Marketing Science, 30*(4), 333–347.

Zetter, K. (2015, June 8). Hacker can send fatal dose to hospital drug pumps. *Wired*. Retrieved from: http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/