Presented to the Interdisciplinary Studies Program:

UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Best Practices to Address Security Concerns with Employee Wearable Technologies

CAPSTONE REPORT

Steven Sconce
NERC Compliance Manager
EDF Renewable Energy

University of Oregon
Applied Information
Management
Program

Spring 2016

Academic Extension
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Kara McFall
Director, AIM Program

Best Practices to Address Security Concerns with Employee Wearable Technology

Steven Sconce

EDF Renewable Energy

Abstract

The great popularity of wearable computers offers many benefits and opportunities to businesses, but widespread use of wearables in the workplace creates serious security challenges for employers. Thus, managers of both civilian and military operations need a heightened awareness of these issues and of best practices for addressing them. This annotated bibliography, intended for employers and managers, explores relevant literature from 2010- 2016 about the nature of these security problems and best practices for addressing them.

Keywords: wearables, security, privacy, identity theft

Table of Contents

Best Practices to Address Security Concerns with Employees and Wearable Technologies: An Annotated Bibliography

Problem Statement

Recent developments in communication technology, especially the increased use of small portable devices, create new opportunities for businesses. A subset of these small computers are referred to as wearable computers and are noted by their mobility, portability, ability to amass large amounts of data and their ability to transfer data wirelessly across computers. A wearable computer is "a device that is worn on the body for long periods of time on a daily basis, which has processing and wireless capabilities" (Castellet, 2016, p. 63). These wearable computers prove to be extremely useful and popular (Schadt, Linderman, Sorenson, Lee, & Nolan, 2010). According to many authors, wearable computing may be the next step in the evolution of the IT industry with such devices finding increasing applications in both civilian and military organizations of all types, including hospitals, factories, schools, and every kind of workplace (Beltramelli, 2015; Brooks, 2013). The most popular forms of wearable devices are smartwatches and fitness trackers (Beltramelli, 2015). Vendors who currently market wearable devices include Apple, Google, Samsung, Garmin, and Fitbit (Austen, 2016; Brooks, 2015; Malanik & Jasek, 2016). The wearable market growth is estimated at 25-50% each year for the near future (Federal Trade Commission, 2015; Malanik & Jasek, 2016).

While wearable devices to date keep the individual in mind, employers are exploring ways to leverage wearable devices with their employees (Austen, 2015). For instance, some organizations encourage employees to wear fitness trackers such as Fitbits as part of employer sponsored wellness programs in order to lower employee insurance rates (Redmond, Lovell,

Yang, Horsch, Lukowicz, Murrugarra & Marschollek, 2014). Other organizations are pondering the use of wearable technology to track the location of employees and their productivity (Austen, 2015).

Despite the growing popularity of wearable devices and new uses for the technology, these devices pose security concerns that include: (a) theft by unauthorized parties of data that is being transmitted to or from the device; (b) theft of data generated by wearable devices that is stored in cloud networks; and (c) theft of the wearable devices themselves (Popat & Sharma, 2013). Since Bluetooth is the primary method of data transmission, rather than via cable or a secure Internet connection, it is very vulnerable to capture by unauthorized persons during transmission. Since wearables tend to use relatively simple processors compared to those of a desktop, laptop computer, or even an ordinary smart cell phone, these unsophisticated processors tend to be much more readily hacked than the equipment involved in standard Internet connections (Malanik & Jasek, 2016).

The very features that make wearables convenient also contribute to the security risks the devices pose (Beltramelli, 2015). In contrast to most other forms of memory, information contained in wearable systems is intended for broadcast and/or remote access. While this feature does make these devices functional and convenient for their intended purpose, it simultaneously increases their vulnerability to access from unauthorized or malicious users (Bangia, 2010). Depending on the nature and application of the specific device, the information collected, stored, and/or transmitted can be of virtually any type. However, the common types of information held within wearables can include GPS-location data, activity and motion records, physiological information, medical information, emails, phone numbers, data from social media sites, or other personal information. However, once a hostile user is able gain access to the wearable device,

they can potentially gain access to any other computer it is linked into - including those in the wearer's home or workplace - and thus sensitive information such as credit card numbers, passwords, social security numbers, banking information, strategic military data, proprietary business information, and all other information a targeted database might contain is under risk of theft. Therefore, assuring the safety of data collected from wearables and/or transmitted to and from them is a challenging but essential task (Safavi & Shukur, 2014; Malanik & Jasek, 2016).

Employers have special security concerns regarding employees using wearable devices which include: (a) unauthorized use of the recording features to record company proprietary information (Beltramelli, 2015); (b) employees who believe an employer has overstepped legal bounds in accessing sensitive employee data generated by the devices may raise data privacy concerns (Austen, 2015); and (c) employees of employers who make employment decisions based upon productivity and other data generated by the devices worn by employees may file discrimination claims (Scheinberg, 2015).

The fact that many employees take wearable devices into the office substantially increases security concerns for employers and leave enterprise networks vulnerable to hackers. Unlike desktops and laptops kept within a designated and protected location and can therefore be easily managed, wearables tend to go wherever their users go. Therefore, once these devices move beyond the safety provided by walls, locked facilities, human guards, and physical or electronic security measures, wearables receive none of the protection that afforded by such methods. (Popat & Sharma, 2013).

Given the fact that wearable devices are relatively new, the information security field is still formulating best practices in addressing threats posed by this technology (Beltramelli, 2015; Brooks, 2015; Malanik & Jasek, 2016; Scheinberg, 2015). Employers wishing to mitigate the

threats posed by the wearable technology of their employees will need guidance in best practices for both technology solutions and policies related to the use of these devices at work.

The increasing number of identity thefts and related crimes is a serious concern. A study focused only on cybercrimes involving medical data reported that at least 4.5 million Americans have their medical records illegally accessed and/or stolen each year (Magsan, 2014). Commenting on the apparent inability of medical security systems to counter this problem, another set of authors express that "current healthcare cyber security systems do not rival the capabilities of cyber criminals" (Luna, Rhine, Myhra, Sullivan & Kruses, 2016, p.#). One US federal government study estimates that 17.6 million Americans were the victims of identity theft during the previous year (Bureau of Justice Statistics, 2015). Another study by Malanik and Jasek (2016) also claims the number of (reported) identity thefts in the US during 2014 was 17,576,200, representing an increase of 84% over the number of such thefts in 2012. Malanik and Jasek (2016) attribute this recent increase to the rapidly rising popularity of smart devices which have only nominal security systems.

While it seems that the advantages of the wearable computers come at a negligible price, employers wanting the benefits of using wearable computers in the workplace must do so at the expense of having to pay greater attention to the security risks created by such devices. Thus, employers encounter the following problem: How to maximize the benefits of wearable computers while simultaneously minimizing the security risks created by their presence. In other words, employers want to know, in terms of both technology and policies, how to address security concerns related to the use of wearable computers by their employees.

Purpose

The purpose of this annotated bibliography is to present selected literature that defines the security threats to employers posed by the use of wearable technologies by their employees, clients, and customers. It follows the assumption that a clear understanding of the problem and its various aspects is the first step towards *eventually* discovering best practices in technology and policies to mitigate these threats. The annotated bibliography also examines literature that explores and/or proposes various the technological or policy-related best practices regarding these matters.

Research Question

Question. What are the best practices for employers in technology and policies to address security concerns related to employee wearable devices?

Audience

This project focuses on the challenges and opportunities associated with wearable technology, the data collected by such devices, and the special challenges that the use of wearable devices raises for employers when workers use such technologies. Its intended audience includes: (a) civilian employers, as well as military and government officials, whose employees, contractors, coworkers, and subordinates may be using wearable technologies as part of their duties; (b) employers of workers who use wearable technology to collect, process, and store data using wearable technology; and (c) professionals in the fields of IT and information security with an interest in the design, development, marketing, and use of wearable technologies.

There are countless ways that employers, workers, schools, hospitals, corporations, military organizations, and governments could improve services, performance, efficiency, and convenience by using wearables. However, the advantages of using wearables do not come without risks (Brooks, 2013; Connolly et al., 2014). Therefore, IT and information security professionals need to have a strong grasp of the particular challenges associated with data security in such devices, especially where this concerns the activities of their employees, subordinates and co-workers. While some firms involved in the creation, marketing, and implementation of wearable technologies have demonstrated a measure of concern for security issues, not all firms make this a priority (Malonic & Jacek, 2016). It remains unclear whether the level of concern is equal to the potential challenges and risks (Brooks, 2013; Pearson, 2011). Therefore, these professionals may be particularly interested in this project and in other emerging research on information security related to wearable technologies.

Finally, employers may find this research interesting if they have workers who use any form of wearable technology, e.g., fitness bands, smart watches, or smart glasses, which might communicate with the company's hardware or databases, and thereby unwittingly (or deliberately) compromise the security of the organization. It is important for such employers to understand how these devices operate, what they a capable of doing, what type of information they collect, how data owners can keep the information secure, and what policies need to be implemented in response to the existence and prevalence of wearable technologies.

Search Report

Search strategy. A search strategy for the topic of information security issues related to storing data collected from wearable technology in cloud-based databases requires a search

strategy that focuses on academic databases that publish journal articles on information and communication technology. To be specific, it involves a search strategy that covers two important concepts or areas of interest in information technology: (a) information security, and (b) wearable technology.

A search of the literature on the subject reveals a significant amount of research about information security issues related to data collected from wearable technology, and regarding security concerns for both civilian and military organizations. Most of the relevant articles were published within the last five years. Most of the articles are in the field of Information Technology and the Internet of Things.

Also, because wearable technologies and the potential security challenges associated with them intersects with similar security issues with cellphones, Wi-Fi, and other IT technologies, the review of literature includes some studies related to data storage issues and security challenges of a more general nature.

Key terms. The literature review uses the following keyword search terms:

- wearable technology;
- big data storage;
- big data;
- data integrity;
- data security;
- phishing;
- wearable gadgets;
- consumer data;
- information security;

- data breach;
- InfoSec
- cyber security;
- information assurance;
- online privacy;
- online information;
- biohacking;
- permission-less information; and
- hacking.

Search engines and databases. A search for peer-reviewed journal articles and research reports originate from reputable and reliable library databases and Google Scholar. The current search used the University of Oregon Library database and EBSCOhost Online Research database with both databases offering a wide variety of published scholarly research studies. My search strategy employs the use of Boolean terms and key words as a method of searching for relevant scholarly literature on the topic. The use of words such as *and, not, or* is used in the Boolean search strategy for these two library databases.

In addition, Google Scholar is part of the search strategy. Google Scholar does not have a Boolean search option; therefore, a search on Google Scholar requires using a combination of key term searches alone or in combination to research journal articles for the literature review.

Documentation approach. The documentation approach for this literature review is to collect the sources and create a mini-database using Microsoft Word and Microsoft Excel. Reference information for each of the sources is in MS Word document format. However, a

database table is used to organize the sources collected for this paper. The Excel database is in table form and contains information about the research reports including the following information:

- author's name;
- year of publication;
- title;
- general topic;
- abstract; and
- key words.

The information in the Excel database is saved in Excel file format.

Reference evaluation criteria. As noted by the Center for Public Issues Education (2014) not all information is equally valid, useful or accurate, and each reference is evaluated in terms of authority, timeliness, quality, relevancy, and bias. Furthermore, each of the evaluation categories is applied to the references cited.

***Authority*.** Resources are given validity if the article is peer-reviewed. In a few cases, an exception is made if the author is a recognized expert and/or from reputable organization in the fields of technology, security, and/or device management.

***Timeliness*.** The issues addressed in this study have only gained currency during the last five years. Thus, the most recently published articles are the most relevant - those published within the previous two to three years, or at most, the previous five years.

***Quality*.** In order to ensure quality, each article or document needs to be clear and concise. Only items in which the writing is clear, and in which the flow and structure of the document are coherent are included. Relevant literature is included if it is without significant

problems related to grammar, spelling, or punctuation unless the author is an expert in the field whose primary language is not standard US English.

***Relevancy*.** Items are only included if the titles, abstracts, and content offer some relevant insight into the subject of best practices for employers concerned with security issues related to the use of wearable devices by their employees, co-workers, or clients.

***Bias*.** In order to be considered for inclusion**,** the author(s) of the document must be deemed credible and sincere (even if imperfect) in their effort to present a non-biased opinion on the subject. The best evidence of this is a willingness to consider various perspectives rather than a single viewpoint to the exclusion of all other perspectives. Articles that are polemic in nature or written for the purposes of selling products or services are not included.

Annotated Bibliography

The following bibliography consists of a collection of 17 references, which are relevant to understanding best practices for employers regarding security issues associated with wearable technologies used by employees. References fall into three general categories: (a) Wearable device security concerns for employers; (b) Technology best practices for employers to address security concerns posed by employee wearable devices, and (c) Policy best practices for employers to address security concerns posed by employee wearable devices. Although many of the documents fall into multiple categories, each is placed under the most relevant heading. Each entry contains three parts: (a) the full bibliographic citation, (b) the abstract, and (c) a summary. The abstract draws from the author(s) actual publication, or from the introductory sections of the document. The summary consists of information gathered from the article without prejudice towards its content or claims.

Wearable Device Security Concerns for Employers

Beltramelli, T. (2015) *Deep-spying: Spying using smartwatch and deep learning*. Master's Thesis, IT University of Copenhagen, Denmark.

Abstract. Wearable technologies are today on the rise, becoming more common and broadly available to mainstream users. In fact, wristband and armband devices such as smartwatches and fitness trackers fill a profitable niche in the electronics market and are becoming ubiquitous. Since they are wearable, these devices provide a new pervasive attack surface that threatens user privacy among others.

In the meantime, advances in machine learning are providing unprecedented possibilities to process complex data efficiently by allowing patterns to emerge from high dimensional unavoidably noisy data. The goal of this work is to raise awareness about the potential risks related to motion sensors built into wearable devices and to demonstrate abuse opportunities leveraged by advanced neural network architectures. The LSTM-based implementation presented in this research can perform touch logging and keylogging on 12-key keypads with above-average accuracy. This demonstrates that deep neural networks are capable of making keystroke inference attacks based on motion sensors easier to achieve by removing the need for non-trivial pre-processing pipelines and carefully engineered feature extraction strategies. The results of this study suggest that the complete technological ecosystem of a user is compromised when a wearable wristband device is worn.

Summary. This 155–page master's thesis offers a very up-to-date and comprehensive investigation of the potential security threats posed by wearable technologies, specifically smartwatches. The author describes a set of formal experiments he conducted using various types of hardware and software. These experiments demonstrate that espionage on the user is not just hypothetical but is feasible with existing technology. The author focuses primarily upon a practice referred to as motion-based keystroke inference. Keystroke inference is the ability of a remote computer to use sophisticated pattern-recognition software to extract information about the specific sequence of key strokes the device wearer enters on a computer key board (or key-pad). The author notes that many wearable devices, especially the latest smartwatches, are almost tailor-made for industrial

espionage making it possible for a hostile outsider to extract information from an employee's wearable any time they make an entry into their computer while at work. A hostile entity can use the same method to extract information from any other computer keyboard into which the worker might type information. The author notes that this technique also works with respect to the digital keypads used with digital locks on rooms, buildings, parking lot gates, for alarm systems, cash registers, and even with vaults and safes. As a result, an employee is inadvertently complicit in making a cyber-attack possible.

Using this approach, hostile outsiders can efficiently and discretely acquire information about what is being entered into the company's computers – to include access to passwords and content, as well discovering the combinations to the company's vaults, safes, security systems, and doors - without the hostile outsider needing to plant a surveillance device inside the company, enter the premises, or recruit a spy from among the employees.

The author devotes most attention elaborating on this threat, and not much on countermeasures relevant to best practices. However, he does briefly discuss various practical recommendations for dealing with the vulnerabilities he describes. One recommendation is simply to prohibit wearable devices with these sensing capacities in close proximity to vulnerable hardware or at least to have their sensing capabilities turned off. This article demonstrates one class of serious and present dangers that wearable computers create for employers.

Banaee, H., Ahmed, M. U., & Loutfi, A. (2013). Data mining for wearable sensors in health monitoring systems: A review of recent trends and challenges. *Sensors, 13*(12), 17472-17500. doi:10.3390/s131217472

Abstract. The past few years have witnessed an increase in the development of wearable sensors for health monitoring systems. This increase is due to several factors including development in sensor technology as well as pressure on politicians and stakeholder to promote projects that address the need for providing new methods for care given increasing challenges with an aging population. An important aspect of this study focuses on how the data is treated and processed. This paper provides a recent review of the latest methods and algorithms used to analyze data from wearable sensors used for physiological monitoring of vital signs in healthcare services. In particular, the paper outlines the common data mining tasks such as anomaly detection, prediction, and decision making in relevance to continuous time series measurements. Moreover, the paper further details the suitability of particular data mining and machine learning methods used to process the physiological data and provides an overview of the properties of the data sets used in experimental validation. This literature review outlines key challenges for data mining methods in health monitoring systems.

Summary. This article provides a good general survey of how wearable medical sensors operate, their purpose, and the value of protecting the information they collect. Privacy and security issues are only briefly touched on. This article suggests that unless employees understand how these technologies work and the security concerns associated with them – something that employees probably will not do unless their employers educate them on these matters – then employees will almost certainly behave in ways that

fail to protect company privacy. This in turn leads to unhappy customers and clients, and leaves the company at risk for customer lawsuits.

The scope of this article is limited to the healthcare industry. However, since physicians are prescribing wearable medical sensors to monitor patients even while they are at work, and thus are collecting, storing, and transmitting personal information about the worker's activities while at work, and these devices may interact with the computers and database at the workplace, the issues the authors raise here are of potential concern to employers. The article is important because it points out another specific way in which wearable computers can create vulnerabilities for employers.

Popat, K.A. & Sharma, P. (2013) Wearable computer applications: A future perspective. *International Journal of Engineering and Innovative Technology (IJEIT) 3* (1).

Abstract. Wearable Computers are a sub-branch of Mobile computing devices, referring to computing devices that we can wear on our body. The first computers occupied a space of approximately two rooms until the invention of Integrated Circuits reduced them to a more portable desktop size. At present, we are using Laptops and Smartphone, which helps us to do our computing tasks anywhere allowing us to carry our office with us. This paper presents wearable computers with their history, present and perspective of their future and their hazards.

Summary. This article is generally quite optimistic and positive regarding the advantages of wearable devices while acknowledging that wearables create serious security concerns when used within a business context. The authors state that wearables can become openings for security breaches if left unsupervised or unprotected. The

authors point out that the mere portability of wearables - the fact that they travel outside of safe and controlled environments, and go wherever the wearer goes - makes them vulnerable to hacking by any hostile stranger the wearer might encounter (or even walk by) during the day. The article also points out the threat posed to a company's server and protected information by wearable computers that facilitate communication between individuals out in the field and their associates back at the office. According to the authors, the small size and portability of most wearables, combined with the fact they routinely travel outside the secured areas, make them more likely to be stolen or lost and "if left unattended or unsecured, wearable computers provide anyone interested in retrieving information about a person or an organization with an opportunity to do so and use this information to either steal company or personal secrets" (p.5).

The article suggests that, as a result of the capabilities of wearable technologies, employers may need to exert more influence over the behavior of employees in possession of wearable computers than most have doing been in the past. This article points out yet another way that wearables can create a danger for employers.

Kumar, P., & Lee H. (2012). Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors (Basel), *12*(1), pp. 55-91. doi: 10.3390/s120100055.

Abstract. Healthcare applications are a promising field for wireless sensor networks allowing patients to be monitored using wireless medical sensor networks (WMSNs). Current WMSN healthcare research trends focus on patient reliable communication, patient mobility, and energy-efficient routing, as a few examples. However, deploying

new technologies in healthcare applications without considering security makes patient privacy vulnerable. Moreover, the physiological data of an individual are highly sensitive. Therefore, security is a paramount requirement of healthcare applications, especially in the case of patient privacy, if the patient has an embarrassing disease. This paper discusses the security and privacy issues in healthcare application using WMSNs and highlights some popular healthcare projects using wireless medical sensor networks including security concerns. Their aim is to instigate discussion on these critical issues since the success of healthcare application depends directly on patient security and privacy, for ethical as well as legal reasons. In addition, we discuss the issues with existing security mechanisms, and sketch out the important security requirements for such applications. In addition, the paper reviews existing schemes aimed at providing security solutions in wireless healthcare scenarios. Finally, the paper ends up with a summary of open security research issues that needs exploration for future healthcare applications using WMSNs.

Summary. This article deals with a narrow category of devices, and does not specifically use the term wearable technology. However, since the subject under discussion is portable, medical-sensing devices that stay with a patient and collect information, this article is indeed relevant. The article discusses some of the major ways this class of devices can create security concerns, noting that they may be especially vulnerable to actions that compromise the privacy of the person whose medical information it collects, stores, and then transmits wirelessly to a remote device. The article also notes that the specific type of information collected, stored, and processed by

this class of device – medical information about a specific individual – is personal and sensitive in nature, and thus privacy concerns are of a considerably higher priority.

This article limits itself to discussing wearable technologies in the context of only one specific industry (health care), but most of the concerns it raises apply to a much wider range of organizations, including educational institutions, businesses, government organizations, and the military. The authors imply that employers and managers are responsible for establishing and enforcing procedures, and should be ethically (and legally) accountable for failure to do so. Although many wearable medical sensors are only used within the well-controlled environment of a hospital, such prescribed devices are increasingly worn for extended periods on a 24/7 basis outside of the hospital, monitoring the wearer while at home, as they move about town, and while they are at work. Such sensors may monitor GPS, cardiac activity, neurological activity, and physical movements (of the sort Beltramelli(date) expresses concern about). Since such devices collect information while the wearable and the wearer are in the workplace, and might interact with other equipment in that environment, they raise many of the same security concerns, as do other wearables.

This article points out that wearables can collect information of an extremely personal nature creating privacy issues that employers must handle, otherwise the company risks exposure to data breaches.

Page, T. (2015). Privacy issues surrounding wearable technology. *i-Manager's Journal on Information Technology*, *4*(4), 1.

Abstract. Wearable devices give people the ability to track almost every facet of their lives with multiple embedded sensors. The collection of data collected by these sensors is also known as 'personal metrics' - the quantification of everyday activity in order to change, improve or understand human behavior. In order to deliver meaningful insight to the user, these personal metrics are sent to companies for analysis. This collection of data from companies ultimately causes complex concerns for consumer's privacy, most notably among young consumers, who are widely reported as having an increased acceptance for the sharing of their data. The study consisted of literature reviews and online surveys. Overall, it found that education into app privacy regulation and companies' use of data alone has a negligible effect on young adult consumer's behaviors. Furthermore, it concluded that young adult consumers seem to accept their loss of privacy, however some behaviors appear to show a level of concern. Nonetheless, due to limitations in the methodology of the research undertaken, it concludes that further studies would be required in order to ensure the validity of the data.

Summary. The core of this article consists of an online survey of people about their attitudes and concerns regarding privacy issues. This article discusses a wide range of issues related to security and privacy associated with wearables. However, perhaps the most noteworthy point it makes is that for the majority of users merely being aware of potential risks to their privacy and the policies of the company regarding the possible uses of their data does not have much of an effect on their attitudes and therefore does not have a substantive impact on their behaviors. The article suggests that, at least generally speaking, younger adult consumers appear to perceive the benefits and utility of wearable devices and the loss of their privacy associated with their use as an acceptable trade-off.

This suggests that efforts by privacy advocates based on efforts to arouse public outrage about the loss of privacy might prove less effective than some might anticipate or assume. However, the author reports that this casual attitude is not absolute and may shift in certain situations such as when a person feels that an employer or third party is misusing the personal information.

This article again emphasizes the problems caused by the ability of wearables to collect very personal information. The collection and storage of such information creates liabilities for employers, and thus employers must manage such information responsibly. This article also points out the long-term nature of this issue (i.e., that employees might not object when the information is initially being collected, but might subsequently change their mind if they later perceive their information is being used in ways of which they do not approve).

Austen, K. (2015). What could derail the wearables revolution? *Nature, 525*(7567): 22-4.

Abstract. Welcome to the chaotic future of wearable electronics: devices that promise to connect real to digital lives seamlessly. These gadgets are rapidly multiplying, and within five years, there could be half a billion devices strapped onto, or even embedded in human bodies. Today, the most familiar gadgets are fitness trackers and smart watches, which monitor health and provide ready access to online services. Already, there are devices that claim to do more than monitor vitals, such as headbands that alert wearers when they become distracted or wristbands that administer electric shocks to smokers who want help quitting. Electronics companies promise to transform medicine with wearables that can treat symptoms or manage care. Devices are emerging

that alert people with epilepsy to incipient seizures, help prevent anxiety attacks, and enable blind people to navigate.

The potential of wearables crucially depends on the large amounts of data they access and generate which leads to needing to find improved ways to transmit data to and from wearables, and keeping all that information safe. With everything from toasters to cars now connecting wirelessly to the Internet, demands on a finite bandwidth are rapidly straining the system. Nearly half a billion new devices started chattering over mobile broadband last year alone, pushing mobile traffic to 25 times what it was just 5 years ago. Wearables are leading to new security concerns, from the use of highly personal data to track people's activity to maliciously attacking their online presence.

Summary. This recent article summarizes a great deal of earlier material, and raises many serious issues about security related to wearable devices. For instance, it describes the case of one “fitness tracker” that recorded physiological data with such precision that it permitted later analysts to determine whether the individual wearer was engaged in sexual activity or not, at what specific time, and at what specific location. While the consumers were unaware the trackers possessed this capability when they purchased and initially used the devices, once this fact became widely known, this led to numerous outraged complaints to the manufacturer. The fact that such data might be accessible to unauthorized individuals was great cause for concern, and the company quickly took steps to remedy the problem.

This may serve as a good example of the types of issues about which employers may need to be concerned. If a company uses wearable technology in a way that can intrude into personal areas of its employees lives - to a point that employers have

accurate information about how long an employee sleeps, where they go for lunch, how many minutes they spend eating, how long they spend in the restroom, where they go during breaks, and how often they have sex - such invasive technology is bound to eventually lead to objections from employees and could result in lawsuits, refusal to wear such devices, etc.

The article suggests several distinct issues relevant to employers. Firstly, if an employer maintains a database that contains much sensitive, private information about their employees, this may lead to numerous objections and complaints from the employees. It also raises the issue of who owns the information stored within such a database. If that information belongs to the employer, do they have the right to use it, share it, publish it, or sell it? If the employees object, what recourse is available to them to protect their information? A third set of issues center upon the possibility that such a hacker could access the database due to inadequate security measures on the part of the employer. If employees are victims of identity theft or other misuse of their personal information, the employer could be accountable in court.

This is merely a subset of the numerous ways the very personal and sensitive information stored in wearable computers can be different from that in other types of devices, and potentially cause great embarrassment if not kept secure.

The ease with which wearable computers might be hacked, due to the mobility of such devices and other factors, is also discussed. The author suggests that unless designers and manufacturers begin to take the matters of security and privacy of wearable data more seriously than they have in the past, and if consumers come to mistrust such technology as a result, much of the promising potential of wearables might never be

realized. This same concern rises regarding employers who require employees to wear such devices that allow such that collect and store data in the company computers, or even allow employees to use such devices in the workplace. This article is relevant to the matters at hand because it once more suggests employers need to be mindful of the wide range of ways their employee's use of wearables can create problems for employers.

Best Practices for Employers in Technology to Address Security Concerns Posed by Employee Wearable Devices

Malanik, D., & Jasek, R. (2016). Contemporary research on identity theft techniques used on smart devices. *International Journal of Scientific Engineering and Applied Science, 2(3), pp. 447 - 454.*

Abstract. This paper provides a brief introduction concerning trends in modern security threats using online identities. The paper deals with two major modern-day facts: the first fact is the increasing number of active online smart devices; the second fact deals with economic impacts of identity theft, as shown in long-term studies. Many users save online identities in their smart devices. These devices provide improvements and simplify online activities, but hackers could use this very personal information to create fake online identities reconstructed from online profiles. Smart devices become the user's online identity and should therefore be protect. However, smart devices provide only very basic and limited protection functions. If there is no security toolkit installed, it is very difficult to protect a user's online identity and identity theft operations become easier. The attacker only needs access to the victims' smart device. This paper shows techniques for infiltrating a victim's smart device and for stealing private data.

Summary. The authors of this article are both professors in the Department of Applied Informatics, at Tomas Bata University at Zlin, in the Czech Republic. The article addresses the security problems of what it refers to as *smart devices*, which includes a broader range of devices than just wearables, (such as smartphones and various types of small portable tablets). However, the authors make it clear they consider what they call wearable hardware (HW) to be among the most vulnerable and problematic devices. The authors have much to say about the rapidly increasing number of identity thefts during the previous five years, and attribute this increase to the rapid increase in the uses of these smart devices.

However, their explanation for why these particular types of devices are such a security risk is of special interest. The authors say that such devices, which use relatively small and unsophisticated processing chips, can provide little more than the most basic and limited protection systems. It is simply not possible to install the kind of full-scale security software used by more powerful computers. Even if such software could be installed, it would not run properly on such unsophisticated processors. If no such security toolkit is in operation, these devices are far more vulnerable to hacking than are desktop or laptop computers. As a result, these devices are prime targets of hostile persons intending to steal the information stored within them, or to use unauthorized access to such devices as intermediaries and gateways into other more valuable computers and databases. The authors warn readers to be very cautious about using such devices, and, by extension, imply that employers would be wise to avoid permitting employees to bring such devices into the workplace. The main significance of this article

is that it pinpoints what may be the key technological feature of wearable computers that causes them to be a major security hazard for employers.

Chuang, J. (2014). *One-Step Two-Factor Authentication with Wearable Bio-Sensors.*

Abstract. Two-step verification does not imply two-factor authentication. Conversely, two-factor authentication may not require two-step verification. With ubiquitous biosensors, we can strive for one-step two-factor authentication for wearable computing applications. Wearable computing brings new challenges and opportunities for user authentication. On the one hand, wearable devices typically lack a keyboard, and oftentimes [lack] even a touchscreen. This presents a fundamental challenge to implementing password or PIN-based authentication. On the other hand, many wearable devices incorporate a range of physiological and kinesthetic sensors. The signals captured by these sensors could lead to novel authentication techniques that are both more secure and more usable. For example, fingerprint sensors are already incorporated into smartphones such as the Apple iPhone 5S and the Samsung Galaxy S5 specifically for authentication purposes. Accelerometers capture precise body movements useful for gesture-based or gait-based authentication. Motion control sensors offer the promise of authentication based on hand geometry while the hand is in motion. Advances in voice-recognition software allow for voice-based authentication. New consumer-grade biosensors that can capture heart, muscle, and even brainwave signals (ECG, EMG, EEG respectively) are now being integrated into devices to be worn on the wrist, arm, and the head. Going beyond traditional single-factor authentication using biometric

signals (e.g., fingerprints, iris patterns), the new standard for consumer wearables authentication should be one-step two-factor authentication.

Summary. Funded by the National Science Foundation (NSF), the author of this research holds a joint appointment in both the School of Information Sciences and the Department of Electrical Engineering at UC Berkley. He is a recognized expert on wearable computing and biometric sensors. The author makes a very specific recommendation for avoiding many of the security related problems connected to wearable computers. He refers to one of these methods as two-factor authentication. For example, a system using two-factor authentication could demand not only the entry of a conventional password, but also require one (or several) correct biometric signals as well, such as a specific brainwave pattern, a fingerprint, voiceprint, and/or neuromuscular signal. Even if a hacker was able to learn the numeric PIN or password, without providing the additional set of biometric signals or kinesthetic patterns, they could not gain access. Since, by definition, wearable computers are worn on the body of an individual person, they would seem to be ideally positioned to provide such a biometric signal. At least in theory, determined effort and sufficient skill could ultimately defeat such a system. However, in contrast to a simple four-digit numerical PIN, if the password consists of a spoken word, which must also be uttered with the proper timbre, tonality, harmonics, tempo, and volume of the owner's voice, (and perhaps be accompanied by a retinal scan or gestural signal as well), such a security system would prove considerably more difficult to defeat.

The author of this article suggests that by using two-factor authentication, wearable computers could soon become even less vulnerable to hacking from hostile outsiders than

are most other types of computers currently in use in business environments. In terms of best practices for employers, the author says that employers should allow only such wearable devices as use this method of authentication to enter the workplace. Although such devices of this sort are not widely available right now, according to Chuang (2014), the technology implement this procedure cost-effectively has actually been in existence for several years, and there are no obvious technological or economic obstacles that might make such devices unmarketable in the very near-term future. This a valuable article, and while it may not offer the one single perfect solution that will solve all the security challenges of wearables immediately, it does offer some explain the essence of security problems with wearables, and suggests possible avenues to address the challenges of using wearables in the workplace.

Dillon, S., Stahl, F., & Gottfried, V. (2015). Towards future IT service personalization: Issues in BYOD and the personal cloud. (Chapter 8 in *Advanced Research on Cloud Computing Design and Applications*, Ed. Shadi Ajamarneh, pp.102-117)

Abstract. Cloud services are ubiquitous today and increasingly used for a variety of purposes, including professional communication, social networking, media streaming, calendar management, file storage, etc. In recent years, cloud services from private applications to corporate usage have evolved. This has led to the question of how private and business services can be dual accessed through a single device, in particular a mobile device that could be included as part of a BYOD (Bring Your Own Device) policy. This chapter considers the issues that arise from a consolidation of private and professional applications when accessed from a single device and introduces the term “personal

cloud" to characterize such situations. It also surveys recent work in the field and finally presents an approach to cloud governance from a business perspective focusing in particular on security tokens, hardware keys and smart containers, thereby providing a glimpse into the future of IT service personalization.

Summary. This is a chapter in a recent book containing a collection of articles related to security issues for multi-user computers and databases. This chapter covers a wide range of subjects and numerous types of security threats related to various types of IT situations, at least some of which are directly relevant to the security issues confronted by employers concerned about wearables. For instance, the authors briefly describe and advocate a particular method for the management of mobile devices allowed access to larger systems, which would include the way wearable computers are used in the workplace. This approach is called *containerization*. The authors define containerization as "strict differentiation between private and professional data applications" (Dillon et al., 2015, p.110).

Although the authors recommend this containerization strategy for a wide variety of situations, the authors present it as being an approach especially useful for situations in which a large centralized computer is potentially accessed by a very great number of different users for a wide diversity of applications and purposes, and in which new, unfamiliar, and potentially hostile devices and hardware frequently request access. As the authors note, this describes the situation of many businesses in which numerous employees and/or customers seek to access the system via their own mobile devices - or wearables.

In practical terms, when using a containerized approach, the employer remains mindful of both the utility of wearables, as well as their vulnerability. For instance, while the IT department of any large company is probably in located within a very secure physical environment, and protected by state of the art security hardware and software systems, the smartwatches of the employees (probably) possess minimal security measures. If the employer is mindful of this contrast, they can do things such as allow announcements calling a specific set of employees to a meeting by sending the message to their smartwatches, but not allow any sensitive details about the agenda or subject of the meeting to be included. They could limit the sent information to the subject of memos and e-mails without allowing the content of those memos or e-mails to show. Information of a delicate, personal, privileged, or proprietary status remains contained only within parts of the system that are assured of being adequately protected, while less private or less sensitive information may be freely sent to smartwatches or other less secure wearable devices.

The authors note that although containerization is possible through many combinations and configurations of hardware, such as storage on separate computers, separate hard drives, storage behind numerous firewalls, etc., it can also achievable via software methods by creating the necessary virtual partitions.

This article is important because it highlights a common data storage practice that is making many employers more vulnerable to the security issues of wearables than they should be, and suggests an approach towards remedying the situation.

Safavi, S., & Shukur, Z. (2014). Conceptual privacy framework for health information on wearable devices. *PloS one*, *9*(12), e114306. doi: 10.1371/journal.pone.0114306

Abstract. Wearable health tech provides allows doctors to remotely monitor their patients' wellness. It also makes it much easier to authorize someone else to take appropriate actions to ensure the person's wellness than ever before. Information Technology may soon change the way we practice medicine by improving the access to essential vital information, thereby improving a doctor’s ability to diagnose which in the long term leads to reduced healthcare costs. The authors analyzed the secrecy demands of wearable devices, including Smartphone, smart watch and their computing techniques that can soon change healthcare provision. However, before this technique is adopted in practice, all devices must be equipped with sufficient privacy capabilities related to healthcare service. In this paper, we formulated a new improved conceptual framework for wearable healthcare systems. This framework consists of ten principles and nine checklists, capable of providing complete privacy protection package to wearable device owners. The basis of this framework is the analysis of existing mobile technology combined with the existing security standards. The approach also incorporates the market share percentage of every app and its respective OS. Furthermore, the authors evaluated this framework against stringent CIA and HIPAA principles for information security, and followed it by testing the capability to revoke rights of subjects to access objects and ability to determine the set of available permissions for a particular subject for all models. Finally, as the last step, the authors looked into the complexity of the required initial setup.

Summary. The authors examine the secrecy requirements of wearable computers used for collection and storage of medical data. Consistent with several of the other articles, this one argues that because the data in these wearables is of a particularly personal and sensitive nature, it requires a substantially higher level of "secrecy" – a higher level than it is generally being given now. The authors seem to believe that the technology *does* exist that could supply the necessary level of security, but that, at least so far, it has not been applied with wearables in the manner or degree to which it needs to be. The article seems to argue the real solution to the security issues connected with wearables lies not so much with a need to improve the technology but rather will result from administrators and employers formulating and enforcing proper rules regarding who is able to access the data collected by and stored within the wearables.

The main value of this article is that it points out that employers do have the ability and the responsibility to make constructive responses to the security challenges that wearable computers present, and offers some specific guidance about what such responses need to be.

Best Practices for Employers in Policies to Address Security Concerns Posed by Employee Wearable Devices

Brooks, J. (2013) *Security issues and resulting security policies for mobile devices*. Master's Thesis. Naval Postgraduate School, Monterey, California.

Abstract. Mobile devices, given their promise of mobility with rich functionality, have broadening use throughout the United States Department of Defense. All the while, these devices can store and access massive quantities of information without there being a comprehensive and specialized security policy dedicated to protecting said information. The importance of having a security policy grows as these devices start providing new capabilities for data capturing and replacing many information systems we currently have deployed. Since the same device can have different applications in different contexts, and each contexts has a potentially different set of security policies, the devices will have to be able to adapt to those contexts. The security policy or policies enforced by the device will have to adapt accordingly. We investigate potential mobile computing security policies to balance this request for context-aware functionality with the information assurance required of these government devices. We investigate the security issues raised in the use of these devices and provide example security policies that address some of these issues.

Summary. Although the author uses the more general term *mobile devices*, which includes portable phones, and hand-held computers, they also include devices such as Google Glasses, miniature tracking devices which can be worn (or swallowed), "computers built into clothing," and other wearable technologies. He points out that

concerns about devices such as Google Glasses and activity trackers are even more serious than those associated with cell phones.

Arguably, the security concerns of wearables in military contexts are even more serious than in medical or business contexts. Rather than loss of individual privacy or financial losses, compromised security in a military context can easily lead to the loss of many lives, the loss of a strategic battle, or to severe danger or damage to an entire nation. The author claims the proliferation of new technologies has proceeded far faster than the ability to address the associated security concerns. He says each new deployment of a technology, or even each new application of an older technology in a new context, creates its own set of security concerns – many of which are new and unanticipated. He suggests that manufacturers analyze their technology for associated vulnerabilities, and specific solutions found which address its unique challenges.

The author covers a vast amount of information, repeating many of the points raised in other articles, such as emphasizing the extremely personal nature of the data collected by and stored in wearables, thus increasing the concerns about privacy. However, he also raises a number of policy-relevant issues not encountered before. For instance, he suggests that many of the devices made in China may have security holes and "backdoors" deliberately designed into them, perhaps intended for some ill-defined future malicious purpose, and thus technology originating from such places, (even if otherwise of excellent quality), should be used with caution, and probably not used at all in sensitive contexts.

He also points out that some seemingly innocent personal information may have unanticipated security implications. For instance, deployed military personnel are generally not allowed to use social media, especially not when on high-risk or sensitive assignments. Therefore, if the level of such an individual's previously active social media use suddenly drops off to nothing, and his fitness tracker simultaneously goes silent, this silence can be a tip-off to hostile forces that a soldier is deployed.

The author uses this example to remind employers that, at least in certain situations, seemingly trivial information can take on strategic significance. For instance, in some business (and social) contexts, where a particular person is, who they are meeting with, when they are meeting with them, and for how long they are meeting with them may be almost as valuable to at least some interested hostile parties as details of the verbal conversation that occurs during the meeting.

The author's main point seems to be that any organization needs to have a centralized and coordinated approach to IT security, and that this effort needs to be an ongoing and continuous project. New technologies will continually be emerging, and hostile entities will continually be searching for (and finding) new and creative ways to defeat even the best security systems. Each new technology and implementation will be unique, each new type of wearable technology will present its own unique challenges, and each will require its own unique responses. This same concept applies to the responses of employers to wearable computers.

The main importance of this document is the emphasis on employer mindfulness regarding security issues raised by wearables (and any other new technologies that may come along), then most of them currently are, and that employers need to give thought to

possible areas of vulnerability they have not considered before – some of which might to unique to their own situation.

Federal Trade Commission. (2015). *Internet of Things: Privacy & security in a connected world*. Federal Trade Commission Staff Report.

Abstract. The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion. Given these developments, the FTC hosted a workshop on November 19, 2013 – titled The *Internet of Things: Privacy and Security in a Connected World*.

This report summarizes the workshop and provides staff's recommendations in this area. Workshop participants discussed benefits and risks associated with the IoT. As to benefits, they provided numerous examples, many of which are already in use. In the health arena, connected medical devices can allow consumers with serious medical conditions to work more effectively with their physicians to manage their disease. IoT will offer numerous other, and potentially revolutionary, benefits to consumers. As to risks, participants noted that the IoT presents a variety of potential exploitable security risks that could harm consumers by: (1) enabling unauthorized access and misuse of personal

information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Participants also noted that privacy risks flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption. In addition, workshop participants debated how the long-standing Fair Information Practice Principles ("FIPPs"), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy.

Summary. This is a report issued by the Federal Trade Commission, primarily regarding a series of workshops and seminars the commission recently conducted (Nov 2013) of the same title, primarily attended by corporate executives, upper management and business leaders. Although much of the content is about specific technologies, the main intent of the presentation is to address policy issues and to offer what the authors of the report refer to as "Best Practices and Recommendations" regarding privacy and security issues related to these new technologies.

This discussion of "Best Practices" is especially relevant to the aim of this present project. This discussion includes recommendations for approaches, some of which resemble the containerization approach mentioned by Dillon et al. (2015). As part of the

efforts to elucidate the dangers with wearables, the authors consider the importance of another prime example of a "best practice," (and the danger of neglecting it), which they refer to as strong authentication:

> In the IoT ecosystem, strong authentication may permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions. In implementing these protections, companies should ensure that they do not impede the usability of the device. (p.31)

Under this strong authentication approach, the parts of the system that are protected by quality, reliable security systems would simply refuse to communicate with those devices with inadequate and/or questionable security systems. Thus, the wearable devices may still be used for numerous other purposes while in the workplace – but have no access at all to the computers which contain all the sensitive, personal, and proprietary information. This article suggests employers who implement these types of policies are far safer than those who do not.

The main value of this report is that it demonstrates several specific policy-related practices with which an employer can respond to wearable technologies and their associated security threats, the most important of which is this practice of strong authentication.

Connolly, M., Niebuhr, J. Mariolis, M. & Bernnat, R. (2014). *Cloud computing: An information security perspective*. Los Angeles: Strategy & PWC.

Abstract. The popularity of cloud computing is growing fast, thanks to its improved flexibility, improved access to data, and lower costs. Yet concerns about the security of the data in cloud environments remain — for good reason, given the inherent loss of control of critical data the technology demands. Only by developing a comprehensive and systematic approach to assessing the risks of moving data into the cloud — one that takes into account the concerns of both business users and IT security managers — can these risks be managed with confidence. Our approach begins with a thorough assessment of the applications of data designated for the cloud. How sensitive is the data, and how serious are the consequences of a potential data breach? Depending on the level of risk, the data must be assigned specific security requirements, and then matched with the cloud architecture being considered — private, public, or hybrid — and its associated security capabilities. Once this process is complete, security managers must work with business users to map out concrete, fact-based solutions regarding which specific cloud environments are appropriate for each data set and application, depending on its level of risk. Ultimately, cloud security needs to be a consideration within the context of each company's overall information security program, including risk management, incident management, continuity planning, and governance. Doing so will require the combined efforts of everyone with a stake in ensuring the security of the data being moved into the cloud.

Summary. This article is about the vulnerabilities of large-scale data storage systems and the practices that increase and decrease such vulnerability. At least some of the key principles discussed by Connolly et al. (2014) are directly relevant to the security issues connected with the use of wearables in the workplace. This article warns of the dangers of any type of situation that relies storing sensitive information onto the cloud - or any other storage system with questionable security protocols. Connolly et al. point out that in any business or organization, much of the information generated and stored is not particularly sensitive, and it is of little consequence if it should be subject to unauthorized or even hostile access. Even so, for every organization, some smaller portion of the data collected and stored is of a very sensitive nature, and unauthorized access to it could lead to very severe consequences. If the employer/administrator fails to appreciate this distinction, and uses the same (suboptimal) level of security for both types of information, they are compromising their security and creating a dangerous vulnerability for themselves and their company. In any such situation, if employees (and the technologies under their control) are given unchallenged access to both sensitive and non-sensitive data, the risk of theft of that highly sensitive information is unacceptably great.

The message of Connolly et al. (2014) is that because of the insecure nature of many types of wearables, when given undifferentiated access to both non-sensitive and highly sensitive data, they are creating precisely this type of situation than Connolly et al. warn is a recipe for disaster. If the employers grant access to the less sensitive parts of their database to employees - and thus to their poorly secured wearables, even a large-scale security breach will be of little or no consequence. However, if such wearables of their employees also are granted access to the more sensitive classes of information, this

creates exactly the type of danger Connolly et al insist should never be allowed to exist, (but which many organizations nevertheless do apparently allow to exist).

As in the quite similar previous discussion of the containerization, the issue here is not actually a question of inferior technology per se that needs to be improved, but a case of sub-optimal policies and practices that lies at the heart of the challenge.

The main relevance of this article is that it demonstrates how specific data storage practices can either maximize or minimize the potential damage that use of wearables in the workplace can create for an employer.

Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation.

Abstract. This paper highlights some of the opportunities presented by the rise of the so-called Internet of Things in general and wearable technology in particular and encourages policymakers to allow these technologies to develop in a relatively unabated fashion. As with other new and highly disruptive digital technologies, however, the Internet of Things and wearable technology will challenge existing social, economic, and legal norms. In particular, these technologies raise a variety of privacy and safety concerns. The better alternative to top-down regulation is to deal with those concerns creatively as they develop, using a combination of educational efforts, technological empowerment tools, social norms, public and watchdog pressure, industry best practices and self-regulation, transparency, and targeted enforcement of existing legal standards (especially torts), as needed. This bottom-up and layered approach to dealing with problems will not preemptively suffocate technological experimentation and innovation. This paper

concludes by outlining those solutions. Finally, policymakers should not forget that societal and individual adaptation plays a role here, just as it has during so many other turbulent technological transformations.

Summary. The author acknowledges the existence of genuine security risks and significant privacy concerns connected with wearables, but questions how dangerous the situation actually is. He acknowledges the risks of embarrassment, shame, and emotional trauma are considerably greater with wearable devices that contain medical and other highly sensitive information than with most other kinds of technology, but argues against any alarmist reactions or unnecessary draconian regulations. Thierer (2015) suggests that despite any short-term problems, a combination of market forces and a "buyer beware" attitude will *eventually* motivate the makers of wearables to correct any significant hazards and security issues. These same general forces will allow employers to come to terms with the security challenges presented by wearable devices, and eventually formulate their own responses and policies tailored to the specific circumstances of their individual work environments.

The main significance of this article is that while it acknowledges wearables in the workplace do create hazards for employers, it urges employers not to panic nor to be quick to seek restrictive new laws or top-down government solutions to resolve the situation. Thierer (2015) says there is no emergency, and that the passage of time will eventually lead to resolution. The author encourages employers to make measured, studied, and appropriate responses to these concerns, and have faith that continued research, discussion, experience, and patience will lead to the evolution of best practices to all the security concerns about wearables in the workplace.

Redmond, S.J, Lovell, N.N., Yang, G.Z., Horsch, A., Lukowicz, P., Murrugarra, L., & Marschollek, M. (2014). What does big data mean for wearable sensor systems? *Yearbook of Medical Informatics, 9*(1), 135-142. doi: 10.15265/IY-2014-0019.

Abstract. The aim of this paper is to discuss recent developments in the field of big data and their impact on the future use of wearable sensor systems in healthcare. The following is discussed: the potential for wearable sensors to generate big data; how complementary technologies, such as a smartphone, will augment the concept of a wearable sensor and alter the nature of the monitoring data created…Importantly, attention is drawn to statistical inference problems for which big datasets provide little assistance, or may hinder the identification of a useful solution. Finally, the paper discusses the risks to privacy and possible negative consequences arising from intensive wearable sensor monitoring. Wearable sensors systems have the potential to generate datasets that are currently beyond our capabilities to easily organize and interpret. However, policy and regulation will be required to ensure that wearable sensor data is not used to invade privacies or prejudice against individuals.

Summary. The article explores the problem of wearable computers that are able to generate data in quantities and forms that may sometimes be beyond the present capacities of existing technology, and IT professionals, to adequately deal with. If such data is beyond current capacities to organize and manage, this implies it may create security challenges and privacy issues of an unforeseen nature as well. The article addresses the fact that data collected by wearables can bring into existence databases that contain "extensive information regarding our lifestyles," which could easily end up being

accessed, (or even owned), by a third party, who might choose to sell it or otherwise transmit it in ways the wearer of the device might not anticipate or approve of. It notes the information collected by and stored within wearables can be of an extremely personal nature, and therefore may make wearers susceptible to various embarrassing and highly intrusive assaults upon their privacy. It discusses possibilities such as that insurance companies may exact higher prices from people they believe are "engaging in unhealthy lifestyles," such as failing to meet minimum recommended exercise quotas. It also discusses concerns about criminals using location information to know when residents have left their homes to break in. The authors seem confident these matters can all be addressed by changes in government "regulations and policies," but they are vague as to what such regulations and policies might look like.

The main contribution of this article is that the authors imply that much of the burden in dealing with the challenges of wearables in the workplace will fall on the employers. Much of these demands will involve the employers making wise and informed decisions about what information they allow these wearable devices to collect, what information should be stored, who has access to it, and what is allowed with that information.

Pearson, S. (2011). Toward accountability in the cloud. *Institute of Electrical and Electronics Engineers Internet Computing, 15*(4), 64-69. doi:10.1109/MIC.2011.98

Abstract. Accountability is likely to become a core concept in the cloud. New mechanisms that help increase trust in the cloud and must be applied in an intelligent way by avoiding a ‘one size fits all’ approach.

Summary. This is a generalized article about IT security concerns. The author’s main point seems to be that each technology and each distinct implementation of that technology may be unique, and call for its own tailored solutions. The article provides no specific solutions for wearables data in the cloud, but the implication is that many of the standard solutions that have worked reasonably well for other technologies in the past might not necessarily address the challenges of wearables. At least by presumption, the author seems to say that manufacturers, vendors, marketers, and employers hoping to profit from wearables might have to take a more proactive stance on the security issues than they have taken thus far. He says that if they fail to do so, the public may eventually conclude that wearables involve unacceptable risks. If this happens, they may turn away from the use of wearables in many contexts, and much of the growth potential of the wearables market may be unrealized. The same principle seems to apply to employee perception of wearables. If such devices come to be widely perceived with suspicion, or as technologies used for excessive surveillance and invasions of privacy by employers, such negative perceptions may act as an obstacle to prevent employers from maximizing the utility (and profit) that could result from the use of wearables in the workplace.

The main contribution of this article is that it points out that employers are ultimately accountable for deployed electronic devices in their workplace, how such devices are to be used, what information they are allowed to collect and store, how such

information is to be used, and for the security of whatever information wearables are allowed to collect and store.

Scheinberg, S. (2015). Emerging technology & employment law.

Abstract. Technologically savvy employment lawyers are essential to modern risk management because employees are often causally involved in security breaches - oftentimes unintentionally. Furthermore, employees can hold their employers accountable and sue if their private information stolen during breaches.

Employees that have their data tracked by wearables and/or their actions monitored by the internet of things provide a great deal of data about themselves and their employer to third parties. Employers have to develop and enforce policies that are strong enough to protect the organization, fluid enough to keep up with evolving technologies and are realistic enough to respect the cognitive and psychological limits of their employees. Employment litigators will increasingly need to address claims predicated on the statistical analysis of massive data pools, including those handed over during discovery. Employment agreements and exit strategies will include a technology-related untangling of employer from employee. To deal with these issues, employment lawyers will not only have to stay abreast of developing technology but will need to be able to have a thorough understanding of how technology works. This requires interacting with folks like CISOs and coders – new ground for many employment lawyers.

Summary. This document consists of a series of short essays compiled by the author, who is an employment attorney concerned with cybersecurity issues. However, the material it presents is also of considerable interest to business leaders, CEOs, IT professionals, government officials, and military personnel concerned with formulating constructive responses to the presence of so many new digital devices in the workplace, including wearable computers and other mobile devices, and the security threats created by them.

One of Scheinberg's (2015) core concepts is that of resilience. He says that it is completely unrealistic to be able to prevent all security breaches on a long-term basis. Instead, he suggests a better approach is to assume such incidents are going to happen, and for employers to arrange their operations in such a way to minimize the damage, recover as rapidly as possible, and be able to continue doing business in as close to a normal fashion as possible even during and after security incidents.

Scheinberg's (2015) discussion has some obvious practical implications. For instance, one could think of using a best practice strategy such as strong authentication, as mentioned previously, as a tactic to minimize the probability of a breach related to the use of wearables. One could likewise also think of a using a best practice strategy such as the containerization approach, as also mentioned previously, as a method of limiting the severity of damage when security breaches do occur (whether the breach is due to wearables or to some other cause).

Scheinberg (2015) also stresses the importance of viewing security matters as a continuing and evolving situation. There has been thievery as long as there has been wealth worth stealing, and no combination of laws, locks, safety precautions, alarm

systems, armed guards, fences, walls, legal philosophies, prisons, policing practices, or law enforcement agencies has been able to end the practice entirely (and probably never will). Even so, businesses continue to thrive. Scheinberg suggests the same general pattern is true of information security breaches. He says there will always be break-ins, information thefts, and cybercrimes, yet the fact of their existence does not have to bring the wheels of commerce to a halt.

He notes that very high percentage of the information involved in serious security breaches is from the keyboards of low ranking employees. (This observation may take on a greater urgency given the point made by in the previously-cited paper by Beltramelli (2015) regarding how easily wearables can be used to steal information from an ordinary computer keyboard). However, the desks and computers of such low-ranking employees tend to be some of least secure parts of any business operation - a fact that Scheinberg (2015) says should concern employers more than it generally does.

In addition to recapitulating many of the issues raised in other articles, Scheinberg (2015) raises a number of other angles of concern to employers. For instance, if a former employee is denied a job elsewhere because someone gains access to restricted information due to inadequate security procedures surrounding his prior employer's personnel files or associated databases, the former employee might take legal action against his former employer. Similarly, if a current employee is a victim of identity theft, harassment, robbery, or some other cyberattack as a result of someone having hacked into the employer's database, and extracting social security numbers, tax information, banking information, or other personal data about the employee that was supposed the be kept safe, the employer might well be held legally - and financially - responsible.

Scheinberg (2015) raises many similar issues that suggest employers are probably not nearly as worried about cybersecurity as they should be. Since wearable computers may be one of the most dangerous sources of compromised cybersecurity in today's world and the world of the near-term future, he says employers would do well to give thought to their policies and practices related to such devices. The less diligently an employer has applied best practices such as containerization and strong authentication, the higher the probability and frequency of security breaches will be. Furthermore, the less convincing the employer is when attempting to demonstrate they have consistently followed such best practices, the more likely they are to be legally liable in cases in which employees claim damages due to security breaches.

Perhaps the main contribution this article makes to the discussion is the concept of resilience. For Scheinberg (2015), the problem is not how to entirely stop or prevent security breaches connected by the use of wearables in the workplace, but for employers to learn how to transact business more or less as usable despite the reality of such security problems.

Conclusion

This section distills the references to conclude that employers need to be increasingly concerned with the significant security challenges presented by wearable computers. The summary falls into the same three categories used in the annotated bibliography: (a) security concerns posed by wearable technologies for employers, (b) technological aspects of such security challenges with respect to employers, and (c) policy issues for employers that concern wearable technologies.

Security Concerns for Employers

The most salient theme in the reviewed literature concerns the personal nature of information gathered by wearable computers. Various authors point out the unprecedented personal nature of the information which at least some wearables collect and store (i.e., 24/7 GPS information, activity logs, physiological data) that automatically raises privacy issues (Austen 2015; Brooks, 2013; Federal Trade Commission, 2015; Page, 2015; Redmond et al., 2014; Safavi & Shukar, 2014; Thierer, 2015). This becomes a concern for employers for a number of reasons. If an employer requires employees to wear devices that collect such private information, this can raise objections among their employees, leading to confrontations with employees, law suits for invasion of privacy, loss of valued employees, and difficulties in recruiting new employees. Other authors (Banaee et al., 2013; Kumar & Lee, 2012; Scheinberg, 2015) note that employers become liable for protecting and properly storing personal data. Litigation, and perhaps prosecution, may result if employers fail to do so. Similar, or worse, problems may arise if the employer subsequently shares this information with, or sells it, to another company without the knowledge or permission of the employees.

Beltramelli (2015) points out that employee use of wearables at work can potentially create severe security hazards for the employer through an entirely different avenue. This is because wearables can collect, record, and transmit data about what the employee enters on their keyboards or keypads, including passwords and access codes. By extension, Banaee et al., (2013), Kumar and Lee, (2012), and the Federal Trade Commission, (2015) raise the possibility that this danger is created not only by wearables issued by an employer to an employee or authorized by the employer, but even by medical trackers prescribed by an employee's physician, about which the employee might not necessarily inform the employer. Multiple authors note as soon as the device is carried outside the relative safety of the workplace onto the street, the sidewalks, into parks, bars, restaurants, sporting events, etc., the devices become considerably more vulnerable to hacking by any hostile person who may come into close proximity (Austen, 2015; Kumar & Lee, 2012; Popat & Sharma, 2013). As long as a wearable computer is on the body, the probability of it being lost or stolen is minimal. However, if it is removed when the employee changes clothes, takes it off to get into the shower, a bathtub, a spa, sauna, swimming pool, during a romantic interlude, while sleeping, etc., the device might be much more vulnerable to being lost, misplaced, or stolen.

Technological Aspects of the Issue

Another important theme concerns the weak security systems, if there are any at all, that protect most wearables. Since they use relatively simple processors, such devices cannot possibly implement the same level of security as a conventional full-sized computer (Malanik & Jasek, 2016). Such simpler processors are therefore more easily hacked. Chuang (2014) also emphasizes that the weak password protection systems of most wearables are very easy to defeat – thus

constituting the Achilles' heel of wearables - and of any larger IT system in which wearables are a component. Chuang proposes that two-factor authentication in response to this vulnerability.

A related theme is the concern about what is referred to as strong authentication – or lack thereof (Federal Trade Commission, 2015). This refers to the fact that an employer's main computers can be set up in a manner that makes access available to wearable devices if and only if a very high standard of user authentication is used. The authors claim this practice needs improved implementation. This highlights another point of great vulnerability created for employers by the use of wearables. Just as an entire chain is only as strong as its weakest link, a system with overall excellent security is compromised if it's connected to even one peripheral device that offers unsecured entry. However, denying access by all but the most trusted and well-authenticated wearables could go a long way towards alleviating many of concerns about wearables with weak security protocols might be used by hostile operators to access an employer's computers and databases.

A similar and related theme concerns the matter of containerization and/or failure to implement it (Dillon et al., 2015). Containerization is a protocol by which allows wearables to access and interact with an employer's computer and databases, but only at a predetermined and superficial level set by the employer. The wearables might receive notifications about meeting times and places, access the titles of emails and memos, office parties and so forth, but *not* about access the full contents of the employer's database.

Rather than debate which of the previous three issues is the single most critical one, one can view these three themes as three separate practices that can potentially combine in a synergistic fashion. Without two-factor authentication (or its equivalent), a hostile operator could gain access to the wearable. Once having accessed the wearable, in the absence of a strong

authentication system, the hostile operator would now have full access to the employers' computers and databases. In the absence of containerization, the hostile operator can then access all of the employer's data, including the most sensitive information. If an employer has put all three, any two, or even one of these measures in place, their system would be relatively secure. However, in the absence of all three, an employer's vulnerability is great.

Policy Issues for Employers

Various experts have raised concerns that, although they involve technology, they actually fall within realm of policies and business practices rather than about technology per se. Connolly et al. (2014) point out the issues raised by failing to make a distinction between highly sensitive information and relatively non-sensitive information. They say that while not all information stored by an employer is sensitive in nature, some specific subset of it invariably will be, and that if this sensitive information is unprotected by a substantially higher level of security than is used with the general information, the employer may be vulnerable to attack.

Safavi and Shukar (2014) say that a major part of the problem is not with the technology itself but rather with the insufficient methods currently in practice in many workplaces that increase the vulnerability for the employers. Pearson (2011) draws attention to the importance of accountability, saying that over and above any technological issues, due diligence and responsible behavior is called for from employers. This is required to protect their businesses from potential security hazards, as well as to protect the information of clients, customers - and employees - from wearable technologies. This is more of an ethical issue – a firm resolve of an employer to behave towards employees in a manner that is respectful of their rights, privacy, and concerns. Scheinberg (2015) affirms essentially the same general concept further reminding

employers that security issues surrounding wearable computers should not be a minor issue they can delegate entirely to a subordinate because they need to be at the forefront of key policies and decision-making. Rather, these are continuing concerns that will remain, and will continuously evolve as new technologies, new hacking methods, and new industrial espionage approaches arise (Brooks, 2013).

The first line of defense may be conceptualized as practices that include prohibiting employees to use cash registers, keypads for alarms and locked doors, vaults and safes, or even computer keyboards, at any time when they are hooked up to a wearable which might record such sensitive information (Beltramelli, 2015). This same general category would include policies of avoiding the collection and/or storing of massive amounts of personal information about employees, customers, or clients beyond what is actually necessary for the operation of the business (Austen, 2015; Scheinberg, 2015).

In addition to this set of policies, we could see the three concepts about technological vulnerability as informing the creation of additional best practices. If two-factor authentication becomes mandated in all wearables allowed in the workplace, hackers could not use the wearables as a gateway into the employer's system. Even if a hostile operator somehow passes this line of defense, the practice of strong authentication would prevent them from using the wearable to access the employer's main computers. Likewise, if the employer is using a containerized data system, even if the hostile operator does somehow manage to hack through the strong authentication system, they would still only able to access the most superficial and least sensitive of the employer's information.

One could view the arguments of Connolly et al. (2014) as the basis for an even deeper line of defense. Even if a hostile operator manages to break through the more superficial

defenses and somehow gain access to the employer's main computer database, since all the most sensitive information is placed in special location protected and guarded by formidable security measures, the hostile operator would *still* not be able to do any substantial or permanent damage.

The overall message seems to be that although the security challenges of wearable technology faced by employers are both formidable and multifaceted, they are conquerable. Some aspects of the problem require improvements (or at least alteration) in the technologies, while others require changes in policies and practices that are effectively managed.

References

Austen, K. (2015). What could derail the wearables revolution? *Nature, 525(7567): 22-4*

Beltramelli, T. (2015) *Deep-spying: Spying using smartwatch and deep learning*. Master's Thesis, IT University of Copenhagen, Denmark.

Banaee, H., Ahmed, M. U., & Loutfi, A. (2013). Data mining for wearable sensors in health monitoring systems: a review of recent trends and challenges. *Sensors*, *13*(12), 17472-17500. doi:10.3390/s131217472

Bangia, R. (2010). *Dictionary of Information Technology*, New Dehli, India: Laxmi Publications.

Brooks, J. (2013) *Security issues and resulting security Policies for mobile devices*. Master's Thesis. Naval Postgraduate School, Monterey, California.

Bureau of Justice Statistics. (2015). Summary NCJ248991.

Castellet, A. (2016). A reflection on wearables and innovation in the mobile ecosystem: Two possible scenarios, In J. M. Aguado (Ed.) *Emerging Perspectives on the Mobile Content Evolution*. Hershey, PA: Information Science Reference.

Chuang, J. (2014). *One-Step Two-Factor Authentication with Wearable Bio-Sensors.*

Connolly, M., Niebuhr, J. Mariolis, M. & Bernnat, R. (2014). *Cloud computing: An information security perspective*. Los Angeles, CA: Strategy & PWC.

Dillon, S., Stahl, F., & Gottfried, V. (2015). Towards future IT service personalization: Issues in BYOD and the personal cloud. (Chapter 8 in *Advanced Research on Cloud Computing Design and Applications*, Ed. Shadi Ajamarneh, pp.102-117).

Federal Trade Commission. (2015). *Internet of Things: Privacy & security in a connected world*. Federal Trade Commission Staff Report.

Kumar, P., & Lee H. (2012). Security issues in healthcare applications using wireless medical sensor networks: a survey. Sensors (Basel),*12*(1), pp. 55-91. doi: 10.3390/s120100055.

Luna, A., Rhine, E., Myhra, M., Sullivan., & Kruse, C, (2016). Cyberthreats to health care information systems: A systematic review. *Technol Health Care*, 24(*1*). doi: 10.3233/THC-151102.

Magsam, J. (2014). Hospital data loss touches 4.5 million, including Arkansas. *Journal of the Arkansas Medical Society*, 111(*5*).

Malanik, D., & Jasek, R. (2016). Contemporary research on identity theft techniques used on smart devices. *International Journal of Scientific Engineering and Applied Science, 2(3), 447 - 454.*

Page, T. (2015). Privacy issues surrounding wearable technology. *i-Manager's Journal on Information Technology*, *4*(4), 1.

Pearson, S. (2011). Toward accountability in the cloud. *Institute of Electrical and Electronics Engineers Internet Computing*, *15*(4), 64-69. doi:10.1109/MIC.2011.98.

Popat, K.A. & Sharma, P. (2013) Wearable computer applications: A future perspective. *International Journal of Engineering and Innovative Technology (IJEIT) 3* (1).

Redmond, S.J, Lovell, N.N., Yang, G.Z., Horsch, A., Lukowicz, P., Murrugarra, L., & Marschollek, M. (2014). What does big data mean for wearable sensor systems? *Yearbook of Medical Informatics*, *9*(1), 135-142. doi: 10.15265/IY-2014-0019.

Safavi, S., & Shukur, Z. (2014). Conceptual privacy framework for health information on wearable device. *PloS one*, *9*(12), e114306. doi: 10.1371/journal.pone.0114306.

Schadt E., Linderman, M., Sorenson J, Lee, L., & Nolan G. (2010). Computational solutions to large-scale data management and analysis. *Nat Rev Genet*. 11(9): 647-57. doi: 10.1038/nrg2857.

Scheinberg, S. (2015). Emerging technology & employment law.

Thierer, A. D. (2015). The internet of things and wearable technology: Addressing privacy and security concerns without derailing innovation

Vacca, J. (2013c). *Computer and information security handbook.* 2nd ed. Waltham, MA: Elsevier/Morgan Kaufmann.

APPENDIX

Definitions

This section identifies key terms and concepts commonly used in the information technology and information security fields.

- *Information technology* (IT) is a subsector of information and communications technology (ICT) that involves the use of data processors like computers to store, retrieve, utilize, and transmit data (Bangia, 2010).
- *Information security* is a field of IT that assures the security and quality of the data collected, stored, used, and transmitted within an ICT system (Bangia, 2010). Information security is an important field in IT because it protects data stored within these systems from threats. External threats could come in the form of unauthorized access, perusal, data modification, data theft, and the corruption and destruction of data by an unauthorized entity (Bangia, 2010).
- *Cloud computing* is the practice of using the Internet to store, process, and manage data instead of a local server or a computer-based database (Bangia, 2010).
- *Cloud storage* refers to the storing of data or information in a remote network of servers within the Internet (Bangia, 2010). While the more traditional local servers allow users to access and process data through specific channels, cloud storage allows users to access and process data remotely because the data is stored in a virtual database on the Internet (Bangia, 2010).
- *Wearable technology* refers to a broad range of technological devices that users wear on their person. Among other functions, “wearables” collect data, record motion, take photos, and/or sync with mobile devices (Bangia, 2010).