Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

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

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

[a] Loyola University New Orleans, 6363 St. Charles Avenue, Box 15, New Orleans, LA 70118, U.S.A.
[b] Terry College of Business, University of Georgia, Athens, GA 30602-6273, U.S.A.
[c] Beedie School of Business, Simon Fraser University, 500 Granville Street, Vancouver, BC V6C 1W6, Canada

KEYWORDS
Wearable technology;
Wearables;
Information security;
Cybersecurity

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

1. The rise of wearables

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

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

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

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

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

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

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

1.1. When we wear computers

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

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

Table 1. Where is the technology worn?

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