TOP CHALLENGES:

WEARABLES IN THE WORKPLACE

BRAINXCHANGE / WHITEPAPERS

TABLE OF CONTENTS

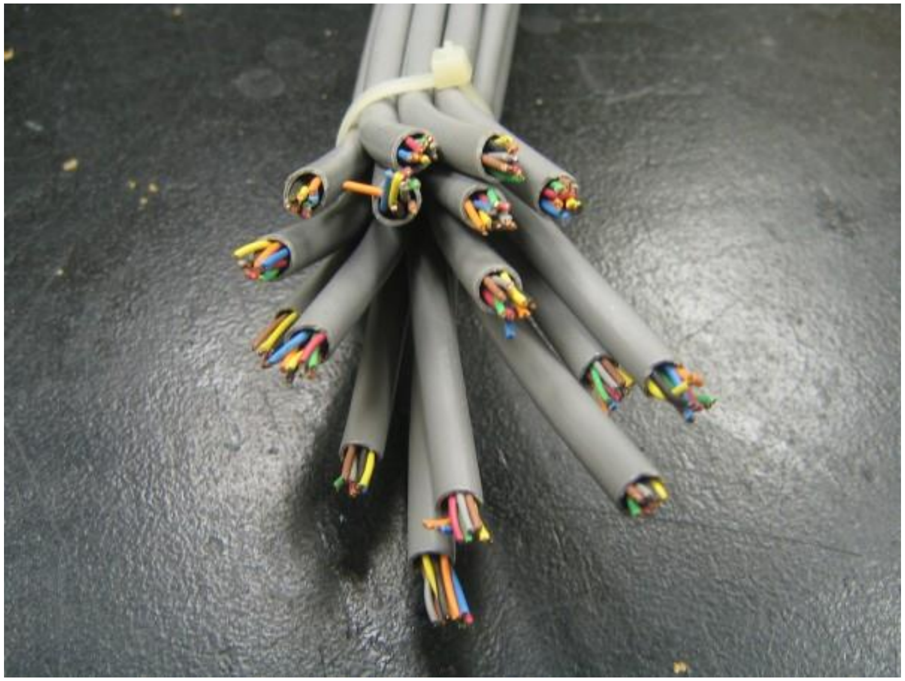
Introduction

Numerous articles site privacy and security as the biggest barriers to the growth of wearables in the enterprise, but the unfortunate truth is that there are a number of challenges – some universal and others more industry- (or office-) specific – holding wearable technology back in the workplace. We have divided these challenges into two categories: ***Technical*** and ***Cultural/Organizational***.

The technical challenges facing enterprise adoption of wearables include such issues as battery life and data security. These are problems for the "tech wizzes" to resolve, and as the technology and related software advances over time, such factors will no longer restrain applications of wearable tech in enterprise. The ultimate resolution of many cultural and organizational challenges, on the other hand, is more "up in the air." Whether factors such as privacy and compliance with regulatory agencies will continue to limit enterprise use of wearables depends in large part upon how the adopting companies – the enterprise end users – handle the change over to this new wave of mobile technology.

This eBook explores some of the major obstacles to realizing the full potential of wearable technology in business and industry, but it does not claim to cover all the obstacles. There are certainly additional challenges we have overlooked, and perhaps a few unforeseen issues that will arise as enterprises continue to test and implement the technology. Despite the challenges, many companies across the industry spectrum are already managing to reap the benefits of wearable technology. And as the technical, cultural, and organizational problems/concerns of wearables are resolved, overcome and put to rest, wearable tech will undoubtedly gain even more traction in the workplace.

Battery & Durability



There are concerns across all industries about whether current wearable device offerings are truly ready for the enterprise, and the general consensus is that they're not. For one, battery life is a major limiting factor.

- Most current models offer hours of occasional use and **up to 45 minutes** of continual use before requiring a recharge.

- Short battery life means most wearables are currently *incapable* of lasting through an entire retail or warehouse work shift, or of sustaining a video conference long enough for an expert at home base to guide a less experienced worker through a complex repair in the field.

Then, there is the matter of the "robustness" or durability of current models, many of which cannot be deemed entirely field-proof and are thus ill-suited for heavy industry.

- Most currently available wearables are **not rugged enough** for a high-risk job site. They're not temperature, or otherwise weather- or chemical-proof. They're just not durable. For example, there is no impact-rated version of Google Glass, making the device not all that suitable for use on, say, an oil rig.

- As demand increases for wearable technology in hazardous industry and as more use cases become apparent, we will surely see more practical, rugged, and tailored form factors.

User Interface & Experience

When it comes to wearable technology in the workplace (as opposed to the consumer realm), experience and engagement matter more than aesthetics and fashion.

Indeed, function trumps form in many job settings, especially in industrial environments: If the wearable device helps a worker to do his job better and/or safer, and as long as it’s not considered to be obtrusive, distracting, unsafe or creepy; then the user experience should be both a positive and willing one.

Issues arise, however, when you consider that current wearable devices do not have standard user interfaces. Imaginably, this would prevent users from comprehending the data emanating from multiple devices, and damage perception of the value of wearable technology in business. ***For wearables to be truly useful to enterprise workers, they need to deliver data that is not just informative but also prescriptive.***

The problem is: It’s not yet clear just what to do with the data harnessed by wearables, and, in addition, many are skeptical of the accuracy of this data. Forget not knowing how to act on the data; if the information is inaccurate, it’s pretty much useless.

IT Infrastructure & Interoperability

As with smartphones and tablets in previous phases of the mobile business revolution, enterprises will have to fit wearable technology (and the loads of accompanying data) into their existing IT infrastructures somehow.

Numerous articles advise that companies should begin strategizing around wearables sooner rather than later. But what does this involve? What do IT teams need to be aware of? **IT departments may have to…**

- **Conceive** original apps for wearable devices whose manufacturers have fairly open and flexible platforms for development. In all likelihood, an IT team will *not* have to design an original wearable gadget à la Walt Disney World.

- **Integrate** wearables with existing enterprise software systems, such as ERP, CRM, work order management, and other legacy corporate systems. In many cases, these systems will need to be adapted or even replaced.

Whether tasked with developing apps for new wearable systems or with creating entirely new products (devices or software), or “simply” instructed to integrate newly adopted wearables into the company system; IT departments will have to adapt and/or overhaul in one form or another to prepare for wearable tech in the workplace.

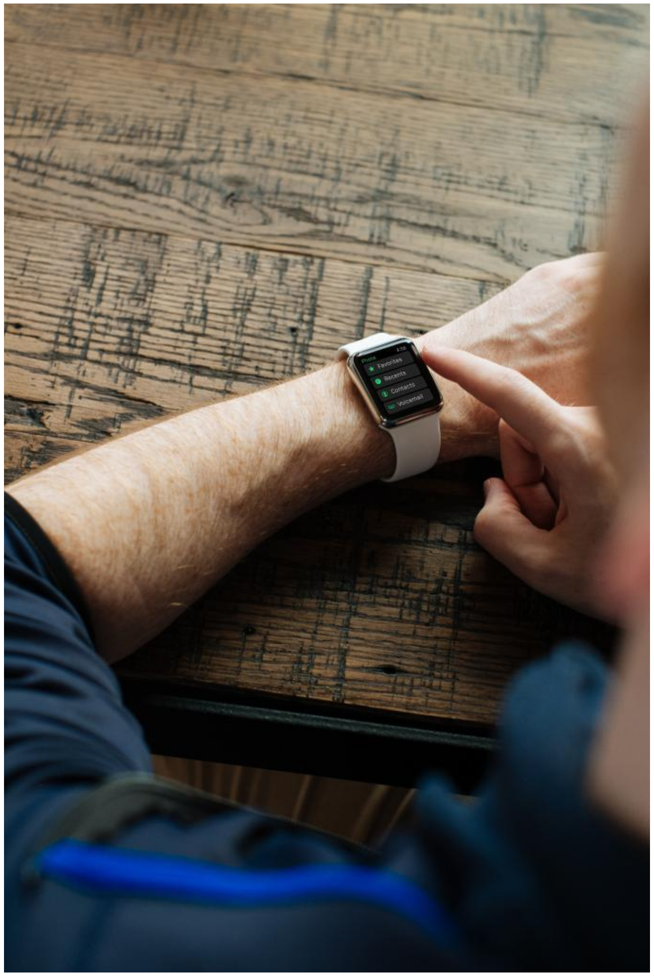
Moreover, in order to make the most of the data emanating from wearables, IT departments will have to be at their most innovative, figuring out how best to manage and interpret the information. IT teams will also have to be at their most cautious, as wearables open up enterprises to a host of new vulnerabilities.

Interoperability

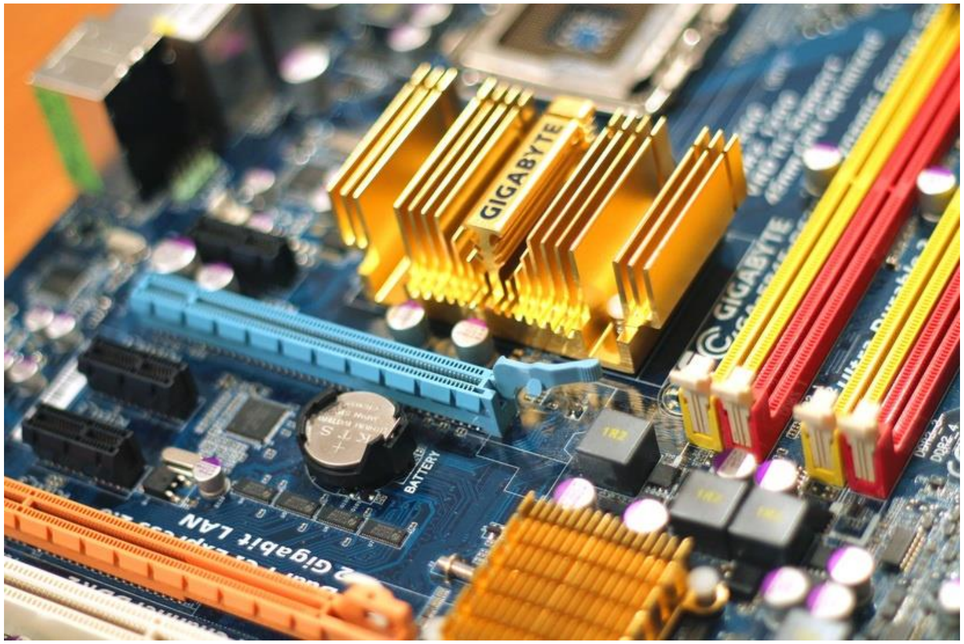
The data provided by wearable tech can be applied very basically, as in a closed experience between the wearable device and a supporting mobile app or other mobile web experience. In this scenario, the wearable technology acts pretty much as a standalone.

In business and industry, however, much more can be gleaned – and gained – by ***integrating wearables into a broader interoperable ecosystem***.

Wearable tech and the accompanying data must be integrated into the enterprise IT architecture so that it can interoperate – i.e. exchange information and functions – with existing software platforms as well as traditional mobile and desktop devices.



Data Analytics



One of the greatest challenges confronting wearable technology in general – and not just in the workplace – is the accuracy and consistency of the data. Sources are divided on just how accurate the data stemming from wearables is. Really, it's the sensor technology embedded in the devices that is in question.

But let's say the accuracy of the data improves. What then? Several analysts cite difficulties in unlocking the deeper value of wearable data as a major issue holding wearable tech back from having a truly significant impact in the enterprise.

At the moment, it is not clear just what to make of the data collected by wearable devices, or how to put it to good, or rather best, use. In other words, *it is difficult to access the data in a meaningful way that might lead to key changes or improvements in an organization*.

Improved communication, increased productivity, and better safety are all great – and currently realistic – benefits of wearables in a variety of business environments, including retail sales floors and construction jobsites; but if enterprises can take the data just one step further, it would potentially generate ***invaluable insight about employee engagement, office structure, process flows, and other factors*** that might indicate key areas for change in the workplace.

Data Security

And so we come to perhaps the mother of all technical challenges, or at least the one to which numerous headlines have attributed notions of serious apprehension and even fear in connection with the adoption of wearable technology.

Whatever the misgivings out there, wearables are inevitably going to come into many businesses in one way or another, whether distributed by management or worn as personal devices by employees in the office. ***Companies will have to expand their corporate security measures, including BYOD policies, to cover wearables***.

It is essential to ensure the security of both enterprise and personal data. Enterprise use of wearables will involve the transfer of critical corporate information among various devices and systems, as well as the collection of employees' personal information.

Whenever a device – wearable or not – is connected to a corporate network, there is ample opportunity for data leaks. A **robust security mechanism** is required to protect businesses' data. Preferably, this mechanism would empower a company to wipe off data in cases of unauthorized access or even a lost or stolen device.

Currently, most organizations' BYOD strategies revolve solely around smartphones and tablets, but *wearable technology may pose additional security risks not encountered with traditional mobile devices*. And as wearables become more mainstream in business, the number of endpoints by which hackers could potentially intercept corporate data will increase.

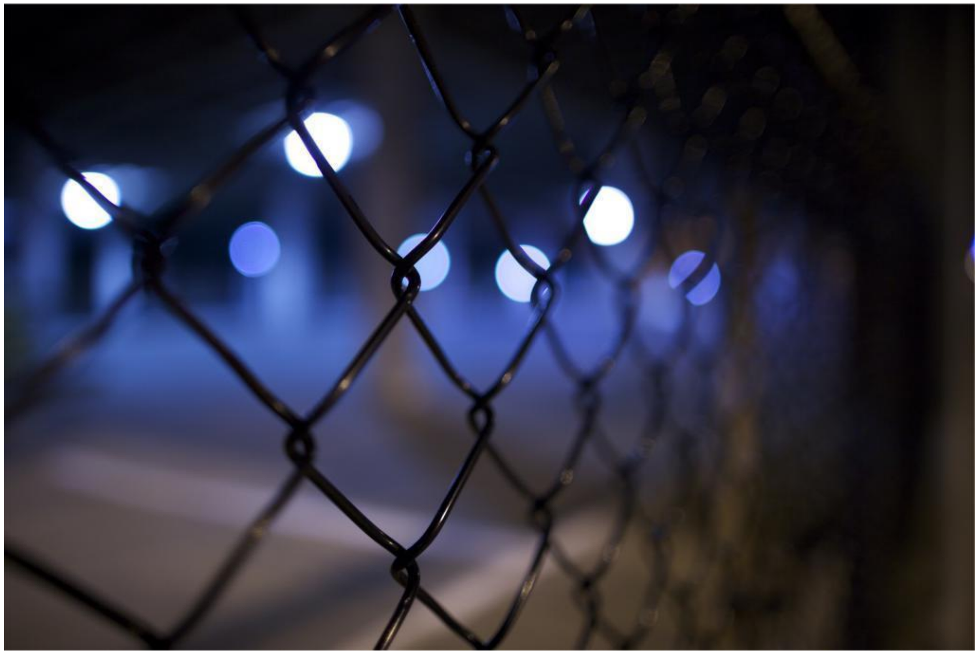
Each wearable device represents a potential node of vulnerability in an enterprise's network that requires management and monitoring. It will be up to IT departments to track when and where wearables are entering the enterprise; and to come up with solid strategies and strong policies for securing these devices and ensuring that unauthorized parties do not have the opportunity to view or intercept sensitive data.

Device tracking among employees will be necessary in this new era of mobile technology. Companies will have to track all assigned wearable assets: If an employee were to resign or lose his assigned wearable device, IT would have to react appropriately, perhaps by administering a full device wipe or even a corporate-wide wipe of all pertinent data.

Tracking the devices also includes *managing data access*. For instance, IT will need to be wary of employees using unauthorized wearable devices as well as apps on authorized devices for unofficial purposes, both of which pose security risks. Authorizing specific assets/parties with access to limited applications and/or groups of data would be a good measure on this front.

Of course, it's not only employees who might misuse data. **The problem of security goes beyond corporate information to extend to personal information**, as well, since wearables collect vast amounts of data about their users' habits and daily activities. How companies use this data and its security is a large part of the challenge – and hesitation – to enterprise adoption of wearable technology.

Privacy & Ethics



Privacy is a major concern when it comes to wearable technology. Specifically, it is the privacy of wearable users' data, or rather the sensitive information that may be revealed by this data, that is "at stake."

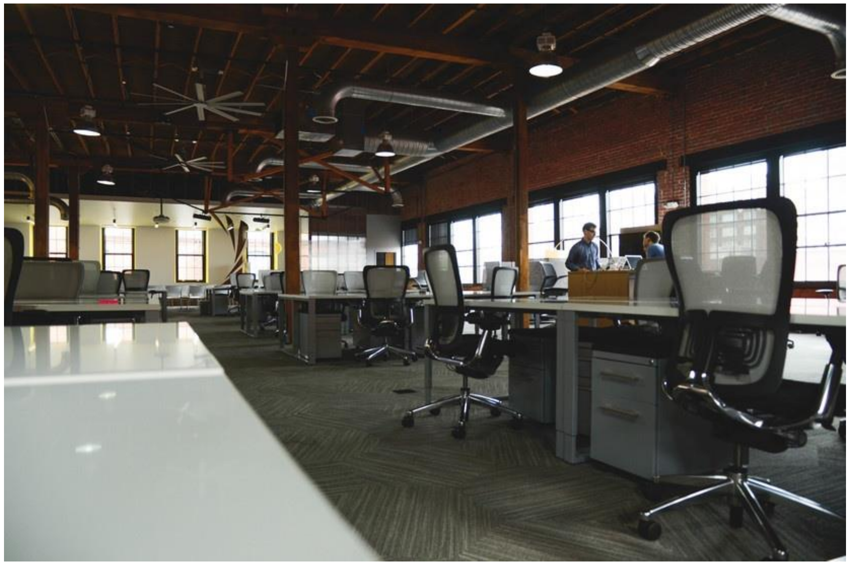
Whereas the security challenge of wearables in the workplace involves potential data leaks, privacy goes beyond a "mere" breach of corporate information or personal data. It involves the data from wearables

- Becoming public when not intended
- Falling into the wrong hands
- Revealing unwanted information
- Or being used somehow *inappropriately, unethically or in otherwise unforeseen and damaging* ways, not only by perhaps unknown third parties but also by employers themselves.

Some sources argue that privacy is not as great a concern in the enterprise space as it is for consumers. After all, employees are more or less used to being monitored in the workplace; and wearable tech is only a new way of monitoring workers. Furthermore, employees are unlikely to resist new technology that helps them to do their jobs better, or so the argument goes. While these are certainly legitimate points, they fail to really address or mollify any privacy concerns.

Wearable technology can capture information related to individuals' habits, behavior and health on top of enterprise information; and all that data could be deemed personal or intellectual property. **Enterprises should not only understand the privacy risks that wearables introduce but they should also make sure employees understand those risks**. Policies will have to be written for the safe and proper usage of workers' wearable data when in corporate boundaries and beyond.

In this new age of mobile technology, businesses will need to be completely open about the data they are collecting via wearable devices, and why. Transparency establishes trust. Even though in these early days it is sometimes not entirely clear just how to use the data collected by wearables towards significant change in the workplace; companies should still be very clear with employees about what kinds of data are being collected and how it is intended that data be put to use.

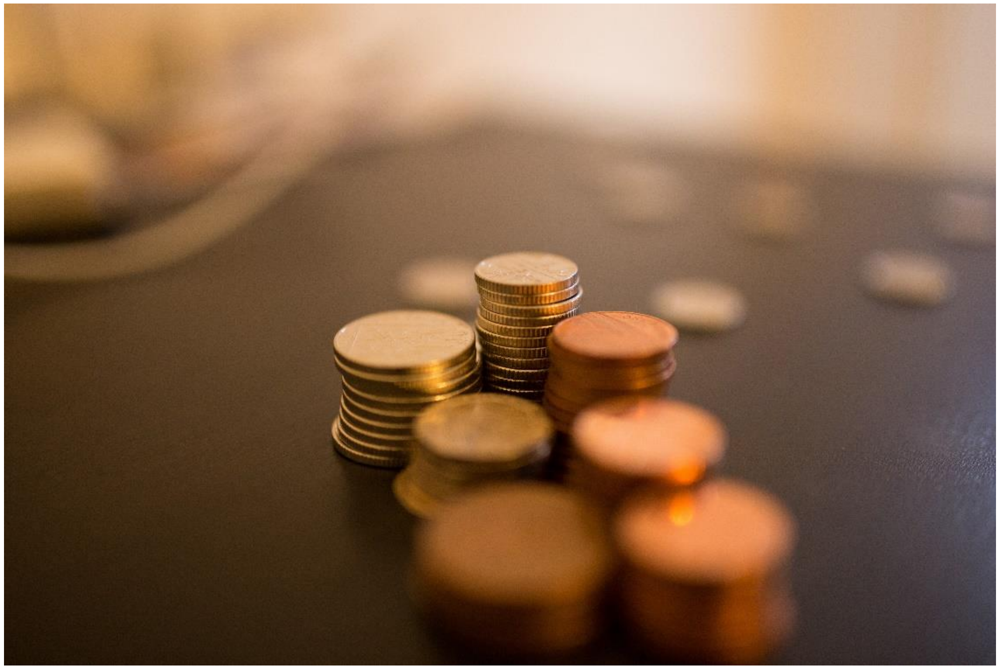


A good governing "philosophy" is the <u>give-to-get ratio</u>: What users get out of the wearable experience – say, increased productivity and other job performance benefits – has to be worth more to them than what they give up, i.e. their data along with a measure of privacy.

Not only do there need to be rules in place to prevent employers from using wearable technology – or rather, the data it creates – to the detriment of employees (for ex. firing or otherwise persecuting an employee based upon his wearable data); but *employees should also be able to opt out of any kind of data interaction in which they feel their privacy may be violated*, and to have their data "returned" or wiped if requested.

At the end of the day, privacy is a boundary that wearable manufacturers and enterprise adopters will have to test and navigate over time. Some currently proposed solutions include ensuring that employers see only anonymous data from workplace wearables, that participation in corporate wearable tech programs be optional, and that there are no punitive implications (applying to both the collected information and the decision to opt out of using the devices). Geofences, which would disable technology in off-limits places such as bathrooms, R&D labs, and private homes, have also been suggested as a viable solution.

Cost & Implementation



Let's face it, wearable technology is expensive. Many of the devices currently on the market are pretty pricey, even by enterprise standards. For instance, the first edition of Google Glass came at the hefty price of $1,500 a pair; and a decent smartwatch runs anywhere from around $200 to $400 for the top-model Apple Watch Sport.

Now perhaps buying a personal Pebble Time won't cause a major dent in your wallet, but just *put yourself in the shoes of a warehouse manager, having to outfit your entire workforce with wearable gadgets costing hundreds of dollars "a pop."* It's just not feasible from a cost perspective unless you have thoroughly tested the use case and can guarantee ROI.

For some companies, cost may be a non-issue. Most retailers, however, no matter their size and industry position, are very capital-constrained and wary of major tech investments targeted towards employees. And while wearable applications are currently being tested in ambulances, police forces, and fire departments across the U.S., finances are nevertheless a major impediment to widespread use of wearables in the public sector.

But the potential total cost is more than the sum of the hardware—there are other cost factors involved in enterprise adoption of wearable tech. In order to realize such productivity benefits of wearables as instantaneous note taking and experience sharing among colleagues, businesses will have to pay for the technology plus the added costs of governance, risk and compliance. In other words, it's not just the hardware: Organizations also need to consider all that goes into implementing new technology, including new or updated software and hiring IT specialists.

Many sources agree, the enterprise wearable technology market is still maturing. *In order for wearables to live up to their potential in business today, the devices need to be somewhat customized for each user case.* We're not at the "plug-and-play" stage yet; so on top of the devices being somewhat unreasonably priced, customizing a wearable tech program for one's business means even higher costs. And to "make matters worse," an organization's failure to understand the solution stack at this early stage can severely slow down the implementation process, and increase costs, as well.

How do you, for instance, justify supplying all your workers with smart glasses as a construction industry leader when the hardware costs at least a grand a piece and there's plenty of opportunity for loss or damage to the devices? And let's not forget all the players you need to bring in – and pay – just to integrate the new technology into your operations and existing IT structure or software platform.

While it's easy to excite enterprise users with wearable gadgets and the many potential benefits of wearable technology in enterprise settings; the products themselves need to become more reasonably priced – on top of ensuring data privacy and supporting a longer battery life – before they can really become "business mainstream." **And organizations must think beyond the cost of the hardware, as it may be an equally big challenge – and an even greater cost – to fit wearable tech into the existing enterprise architecture.**

Of course, when the potential cost savings of adopting wearables stand to be in the millions, even billions, of dollars in some industries (field services, for one); all such initial cost considerations as the price of the devices and whatever it takes to get the technology secure and interoperating within the existing IT infrastructure become much less of a barrier.

Proving ROI

How does one measure the ROI of wearable technology in enterprise settings? How does one show statistical results of wearables in the workplace? We've been told of the many potential benefits of wearable tech in business and industry, but where's the proof? *Where are the numbers?*

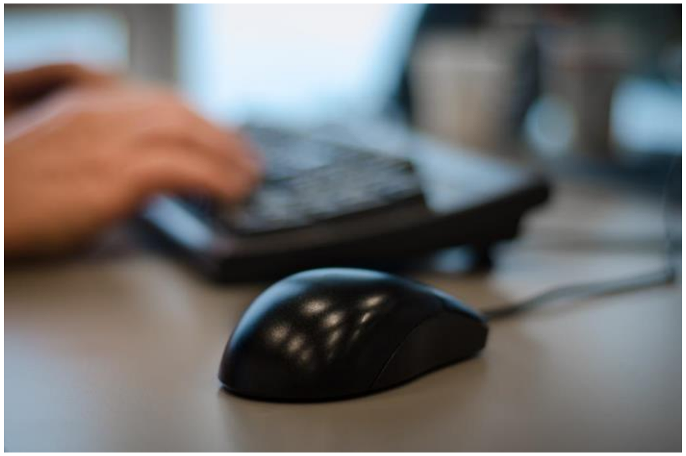
The Human Cloud at Work research project conducted by Dr. Chris Brauer of Goldsmiths, London may be the closest any organization has yet come to providing robust stats for wearables in the workplace. At the very least, it is the most referenced study. But a statement such as "*The use of smart glasses in this manufacturing industry application increased productivity by X% and saved the adopting company Y amount of dollars*" is hard to come by.

So how does one prove the ROI of wearable technology? **An organization might do so by…**

- Demonstrating that wearable tech leads to increased (and quantifiable) efficiencies, documenting a change in operational activities to that effect
- Or it might record an increase in revenue or profit resulting from the introduction of wearable devices to the workforce

In simplest terms, ***wearables have either got to save time or money or both***, the two being inextricably linked in most business and industrial applications. In addition, it has to be shown that wearable technology is a better replacement for existing technology solutions like smartphones, tablets, and other hand-held devices.

Indeed, the new technology has got to be a lot better than the old tech, and evidently so. Wearables have to save even more time and money than traditional mobile solutions, or they just won't cut it in business.



At the end of the day, *quite how ROI is calculated comes down to the objectives of the company that is adopting the technology*, and the metrics put in place at the outset of that company's wearable pilot program or firm-wide implementation of wearable devices.

It seems corporate wellness programs incorporating fitness-tracking wearables are seeing more measurable results at the moment compared to other workplace wearable programs; yet in cases where wearable technology is being tested to enable remote collaboration between field technicians and experts at home base, several organizations are finding that the time it takes to complete tasks has declined, <u>which leads to other measurable outcomes such as cost savings and improved customer satisfaction</u>.

Compliance with Regulatory Agencies & Industry Standards

When it comes to the issue of compliance, perhaps the most obvious circumstance is that of HIPAA compliance of wearable devices in the medical sector. Yet in other industries – especially in the more hazardous industries such as oil & gas, manufacturing, and construction – there are standards that have to be met, certain requirements and expectations for products and equipment utilized at the shipyard, job site, or oilrig. In this eBook, however, we will focus on the challenge of compliance as it pertains to healthcare.

HIPAA

While doctors have been some of the most enthusiastic proponents of wearable technology, ***medical institutions – perhaps more so than any other enterprise organization – face significant privacy obstacles when it comes to implementing wearables***—most obviously, the Health Insurance Portability and Accountability Act (HIPAA).

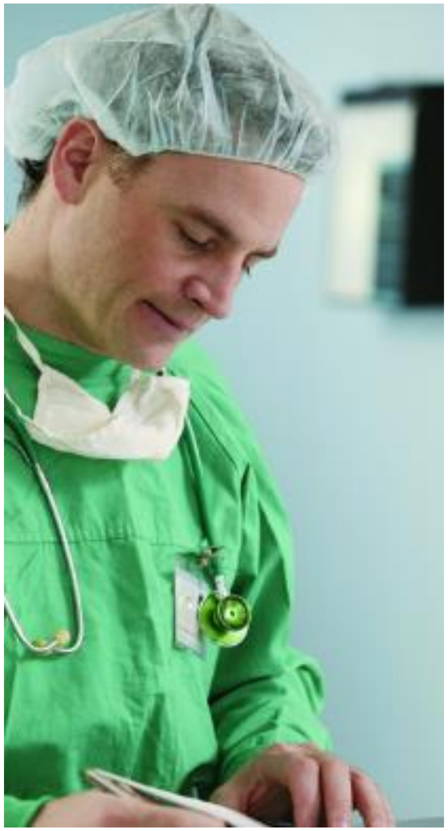
In theory, in order to utilize a wearable device with live-streaming capabilities such as Google Glass in a medical setting in compliance with this act, the device would have to be run over a *healthcare-specific, password-protected, encrypted network.* This is no easy feat, the alternatives being to strip the technology of certain features such as Internet connectivity (which might defeat the purpose of adopting the tech in the first place) or else – and the more unlikely – to substantially alter HIPAA laws to accommodate wearable tech.

So what is HIPAA and why does it matter? Well, one of the main purposes of this act is to ensure the confidentiality of all healthcare information. What developers in the medical/health wearables space should understand are the *privacy requirements* of these laws, and how information or data transmitted by a wearable device or application to an entity such as a doctor or insurance provider is potentially covered by HIPAA.

Certain health information is considered protected under HIPAA, while other data collected by wearables may or may not fall under the act. Metrics such as number of heartbeats, steps taken, or sleep history are technically not considered protected; however, as soon as this information is shared with a doctor, hospital or third-party organization in the course of providing a healthcare service, then it becomes part of a patient's health record and therefore covered by HIPAA.

What we have just described is a scenario in which the data in question stems originally from a consumer's personal wearable device; but there are other scenarios in which HIPAA comes into play, including instances of wearables being used in hospital settings to monitor patients as well as to provide doctors with access to patient records, and especially in cases of **telemedicine, teleconsultation and telementoring**, where visual recording takes place.

At this stage, ***most wearable technology does not acknowledge HIPAA or any other laws – federal or state – covering personal medical data***. Yet the demand to utilize data from wearables in patient healthcare certainly exists, and doctors have found ways “around” HIPAA in order to safely use smart glasses in hospital environments. Inevitably, the legal gap between health-related data collected for consumers’ personal use and that exchanged with HIPAA-covered entities (healthcare professionals and institutions) will be thoroughly tested, navigated, and defined.



THE FDA & the EEOC

The concept of smart contact lenses is rather sci-fi to some, for others a cause for concern. Ingestibles, embeddables, hearables, smart clothing, and the like constitute an area of “close” wearable technology that could be exposed to regulatory factors. You see, as soon as you have devices interacting with the human body in a direct and continuous manner, you are in the realm of technology that will likely require FDA approval.

Indeed, the U.S. government is already considering wearables, at least those used as part of corporate wellness programs. In June, the Equal Employment Opportunity Commission (EEOC) issued a proposed rule amending parts of the Americans with Disabilities Act as it relates to those wellness programs in place at more than half a million U.S. companies. At issue is the data collected by wearables, and whether it qualifies as simple health data (ex. number of steps taken) or medical information (ex. heart rate*), with the latter potentially held to higher levels of privacy.*

When it comes to wearable technology in healthcare, it seems the nature of the collected data is a matter for address. As new and increasingly advanced sensor technology comes about, providing us with more and more personal health metrics, those metrics capable of being measured by wearable devices will have to be categorized somehow, and defined as either *protected* (and under what laws) or *unprotected* and perhaps subject to some kind of consent.