WEARABLES FOR SAFETY

Worker Acceptance, Union Buy-In & Data Security Measures

By Toni-Louise Gianatti

The broad adoption of wearables in the workplace is largely dependent on overcoming certain barriers. A study published in *Journal of the Human Factors and Ergonomics Society* notes that these barriers include worker acceptance, and privacy and confidentiality of data (Schall et al., 2018).

When deciding to take on any form of safety technology, it is paramount to be equipped with the right arguments about worker acceptance, have extensive knowledge of what is being collected, decide on what data is most important to collect, and have up-to-date information ready to deal with any union acceptance setbacks.

Three concerns typically arise when deploying technology in the workplace: worker acceptance, union buy-in and data security measures.

Worker Acceptance

According to Schall et al. (2018), approximately 80% of OSH professionals would consider using wearable technology to help track and monitor risk factors at work. Worker acceptance is paramount to whether the technology achieves its goals to keep people safe on the job. The study identifies several worker concerns about acceptance of wearable technology:

- privacy or confidentiality of collected data
- employee compliance, workers concerned with not being able to follow and use technology as per organizational guidelines
- sensor durability in industries such as construction and manufacturing
- safety of the devices in industries such as energy, and oil and gas

Taking these concerns into consideration, implementing any safety technology involves several key elements:

1. Know the product well before approaching the employees and prepare workers mentally. This can be done by presenting past successes of the device or program, particularly in related industries; proving the suitability of the wearable to the organization; showcasing the benefits and what it will mean for the individual; and ensuring the quality and reliability of the technology.
2. Involve workers in the decision process by addressing all concerns and aversions around deployment. This can be done by encouraging open nonjudgmental communication around acceptance and implementation, and stimulating discussion among employees before presenting the technology.
3. Diminish fear by being educated in data security and privacy, and communicate this clearly and openly to workers. When presenting this technology, provide proof that data security measures have been implemented and that provider credibility has been researched. In addition, openly discuss the data collection, how it is being used and whether it will be aggregated or anonymized rather than individualized. Clearly set out exactly what data will be collected and why, and record data only during working hours.
4. Address employee compliance issues by providing workers with clearly outlined instruction sheets, keeping the implementation process simple and quick, and appointing a "champion" or worker who can help anyone with technical issues.

The way technology is presented to employees can significantly affect its adoption and whether safety goals and benefits are achieved.

Union Buy-In

Worker productivity has been measured for quite some time. It dates back to the 1900s when Frederick Taylor and Frank and Lillian Gilbreth studied work being completed to bring about changes and improvements to work processes. Their scientific management theory had an underlying promise of increased productivity and is still used in businesses today with systems such as organizational charts, performance management and production goals. The modern version of their work is sometimes referred to as "digital Taylorism," whereby machines can provide the scientific management of the workers. The changes Taylor and the Gilbreths brought to businesses might suggest that they were not the worker's friend, but it is clear that their methods have greatly impacted the business world today (Schumpeter, 2015).

With advances in safety technology, it is understandable that unions are skeptical about the suggested use of these products. One primary concern is that organizations could use the devices

METAMORWORKS/ISTOCK/GETTY IMAGES PLUS

As Industry 4.0 and related laws are continually evolving, when deciding to deploy any safety technology, it is important for the discussion to include everyone in the organization (e.g., safety and health teams, human resources, legal groups, innovation teams, operational management).

to spy on workers in terms of performance or use geolocation data as proof against employees. Another concern is the issue of data collection security and privacy. It is simply a balance: do the benefits of the technology outweigh the associated risks?

Following are several ways to gain union buy-in:

•Know the product well before approaching the union and communicate openly and clearly about the benefits, proving that the technology is not aimed at providing new methods for digital Taylorism or performance management, but that its purpose is safety and safety management.

•Involve the union in the decision-making process and be receptive to any concerns.

•Be aware of and understand exactly what data is being collected by the technology provider and ensure that only relevant data is collected.

•Work with the technology provider to come up with ways to mitigate the risks as much as possible (e.g., disengage GPS or geolocation if employee location is not absolutely necessary; allow only aggregated or anonymized data to be available to management; allow workers to see all of their own data and have access to it regularly).

As Industry 4.0 and related laws are continually evolving, when deciding to deploy any safety technology, it is important for the discussion to include everyone in the organization (e.g., safety and health teams, human resources, legal groups, innovation teams, operational management). Once these discussions have taken place, involve workers in the decision and seek their feedback. This will bring to light all possible setbacks before engaging, from data collection issues to worker acceptance, and help to address any gaps or worker concerns that management may have missed.

Data Security Measures

In 2010, Eric Schmidt, former Google CEO said, "Mankind generates as much information now in 2 days as it did from the dawn of civilization up to the year 2003" (Sielger, 2010).

When using any kind of smart technology, there is always a slight fear about its ability to collect data and the opportunity for vendors to share it for commercial or other purposes. Certain products have a significantly higher risk than others of hacking threats (e.g., identity theft); however, devices used for safety are generally deemed to pose fairly low risk because they usually do not store financial details or passwords that would be required for identity theft (Shahmiri, 2016). This technology may hold movement and biometric data, and, while the user would not like this information revealed, the threat of identity or financial theft is lower. However, hacking is a particular concern with the performance of safety devices. For example, a hacker can disable any of the technology's functions, which could have negative safety consequences.

When engaging any third-party service or purchasing any product in general, it is important to research the company. The same is true for data security. If some areas fall outside of the OSH professional's scope, it is not unreasonable to consult in-house information technology specialists or simply ask for proof or information based on the following:

•Ensure that the product has been designed and manufactured by engineers and not by a traditional consumer-goods producer.

•Question and ask for detailed proof that the engineers are trained in data security and have addressed security concerns with the principle of reasonable security in terms of the technical, physical and administrative requirements.

•Check that encryption measures have been included so that the technology is less vulnerable to hacking.

•Be aware of unsophisticated devices that do not necessarily have the space to add the processing power required by security measures and can sometimes lack robust data security.

•Check that there is the possibility of regular updates and that they are conducted to ensure security against any possible threats.

•Ask for a copy of the vendor's data privacy policy. Check whether the vendor has clear information available that covers its legal obligations, explains exactly what the company deems personal information, how it secures that information, and that the information is written in lay terms.

If using the product in Europe, ensure that the company is compliant with the General Data Protection Regulation (GDPR). This legislation came into force across the EU in May 2018 (GDPR.eu, 2020). It was brought about to protect consumers, and organizations collecting data must do so under strict legal conditions. Data is anything that can be processed to uniquely identify an individual, including name, address, photos, genetic or biometric data.

If the product is from the U.S., there is no federal data privacy law. Ask which state laws the company adheres to and how it defines personal data, as this differs between states. Each state has its own form of data security measures that must be followed.

Conclusion

When adopting any new technology or system into an organization, first gain proof to help with acceptance. Review industry-specific case studies and past successes, and ensure quality, reliability and, most importantly, suitability of the technology. Use clear and open communication with unions and users, and make sure the benefits that the wearable technology provides can easily break through the barriers involved. Executing proper assessment of wearables by involving all stakeholders in the decision-making helps eliminate fear and facilitates positive outcomes. **PSJ**

References

GDPR.eu. (2020). What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr

Schall, M., Sesek, R. & Cavuoto, L. (2018). Barriers to the adoption of wearable sensors in the workplace: A survey of occupational safety and health professionals. *Human Factors, 60*(3), 351-362.

Schumpeter. (2015, Sept. 10). Digital Taylorism. *The Economist*. www.economist.com/business/2015/09/10/digital-taylorism

Shahmiri, S. (2016). Wearing your data on your sleeves: Wearables, the FTC and the privacy implications of this new technology. *Texas Review of Entertainment and Sports Law, 18*(1), 25.

Siegler, M.G. (2010, Aug. 4). Eric Schmidt: Every 2 days we create as much information as we did up to 2003. TechCrunch. https://techcrunch.com/2010/08/04/schmidt-data

Toni-Louise Gianatti is content manager for Soter Analytics, a global safety science company producing artificial-intelligence-supported wearable solutions that reduce the risk of ergonomic injuries. Gianatti has more than 20 years of coaching experience, with a focus on reprogramming body maps to break faulty movement habits and reduce injury risk.