feature

The Dilemma for Workplace Usage

Wearable Technology

Craig Krivin, CISA, CISM, ITIL
Is IT audit senior manager at Avnet Inc. and the ISACA Phoenix Chapter research director.

Sanjay Bhide, CISA, ACMA, ACPA, ACS, FCA, MIIIE, PMP
Is the external compliance project manager at Honeywell International Inc.

Sandeep Desai, SSCP
Is IT senior audit leader at Wells Fargo

Ravi Dhaval, CRISC, CCSP, CIPT, CISSP
Is a senior consultant at Deloitte & Touche LLP.

Joe Norris, CGEIT, ITIL, Six Sigma
Is director of IT governance and compliance at Early Warning Systems.

Amanthi D. Pendegraft, CISA, CPA
Is a director, risk consulting with KPMG LLP.

Susan E. Snow, CISA, CISM, CIA
Is a senior information security analyst in data loss prevention and information security.

Dan Wagner, CISA, CRISC, CISSP
Is manager of IT audit at Albertsons Companies.

"Wearables in the Workplace: The Next Big Thing?" "How Should Companies Handle Data From Employees' Wearable Devices?" Headlines such as these seen in *Forbes* and *The Wall Street Journal* proliferate n the daily news and are foremost when thinking about wearable devices.

The ISACA® Phoenix (Arizona, USA) Chapter research committee set out to learn more about the wave of wearable devices and understand the ISACA community's attitudes toward wearables' potential risk and security impacts in the workplace. To that end, the committee conducted two surveys of ISACA membership. This article shares the insights of survey respondents representing many organizational types and geographies.

While preparing the questions and developing the results, the research committee noted that a major electronics manufacturer has developed a device that contains a microphone, an accelerometer, infrared sensors and other data-collection devices. This device can track where workers are, who they talk to, how far away they stand from the colleagues with whom they are talking, how often they make hand gestures, how frequently they nod and how the energy level in their voice changes. Workers can see how meetings and interactions impact these parameters.

Monitoring employees through wearable devices "is about a social contract between employer and employee. It is in nobody's interest to have overworked, stressed and anxious employees who often are not even aware of their own condition. Making things visible is a good thing if there is a culture of trust and accountability."[1]

While there are many perceived benefits of using wearable devices in the workplace, there are also several concerns and risk factors to consider:

- **Less privacy**—Wearables provide new features to customer interactions such as recording interactions, biometric data such as pulse rate or blood pressure, video streams, two-way audio, and location tracking. Employers might be driven by liability considerations to use wearables to track employee health or to interpret and intercept risk such as when staff are entering a dangerous area without adequate protection. Although these tracking mechanisms could be beneficial to employees, there is a perceived lack of privacy.
- **Personal information security and acceptable use**—Certain wearables have the potential to collect detailed and more personal information than do common consumer devices such as smartphones. Ownership and the ethical use of such data are complex and growing legal battlefields.
- **Corporate data security**—Some wearable devices may consume and retain sensitive corporate data such as messages, emails and images. Many wearable devices have entered the enterprise on a bring your own device (BYOD) basis, and employers may not be fully aware of the information risk associated with their use.

The terms "wearable technology," "wearable devices" and "wearables" all refer to electronic technologies or computers that are incorporated into items of clothing and accessories that can comfortably be worn on the body or under an individual's skin. These wearable devices can perform many of the same computing tasks as mobile phones and laptop computers; however, in some cases, wearable technology can outperform these handheld devices entirely. Wearable technology tends to be more sophisticated than handheld technology on the market today because it can provide sensory and scanning features not typically seen in mobile and laptop devices, such as biofeedback and tracking of physiological function.[2]

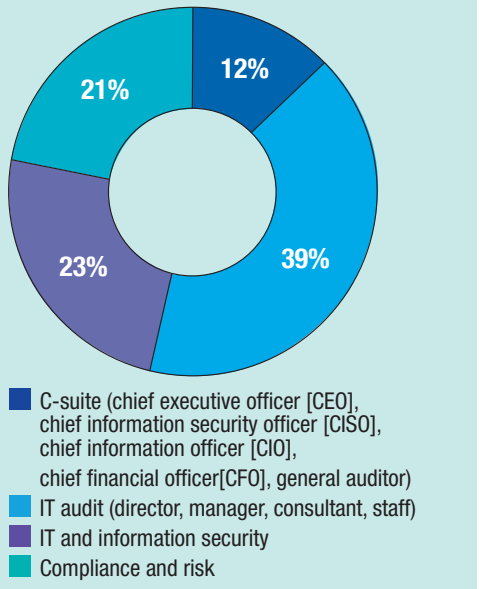
Wearable technology can often be classified into the following categories:

- Smart watches (e.g., Apple Watch)
- Fitness trackers (e.g., Fitbit)
- Sports watches (e.g., TomTom Spark)
- Head-mounted displays (e.g., Oculus Rift)
- Smart clothing (e.g., Sensoria running socks)
- Smart jewelry (e.g., Misfit Swarovski Shine)
- Implantables (a device surgically implanted under the skin)
- Other (multifunction device)

Who Responded to the Survey?

The ISACA Phoenix Chapter research committee's first survey in 2015 was replied to by a group of 135 ISACA and Institute of Internal Auditors (IIA) members in the United States and Canada. This provided the chapter with initial impressions and a good foundation on which to build. The second, more detailed survey was responded to by 325 people representing a diverse, global group of ISACA members. All levels of management and geographies participated, including C-suite members, directors, consultants and staff members across the compliance, risk, IT and information security domains (**figure 1**). Financial and banking respondents made up about 25 percent of the total population, while technology services and consulting, government, and health organizations made up a large percentage of the remaining respondents industries (**figure 2**). Although participants were primarily from North America, approximately 15 percent were from Europe, approximately 9 percent from Asia and approximately 6 percent were from Africa (**figure 3**).

Figure 1—Areas of Respondent Expertise



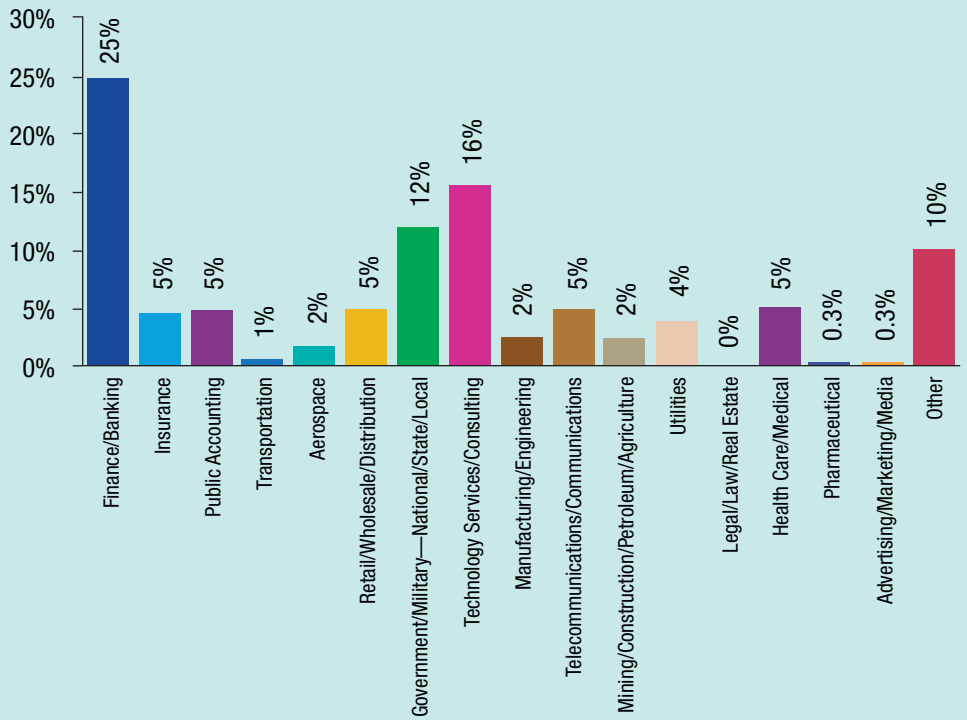
Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

User Reaction to Wearable Devices

Many individuals noted that the issues they identified regarding wearables are top-of-mind concerns. The questions leveraged feedback from compliance, finance, audit and technology authority perspectives. (**figures 4, 5** and **6**.)

The market and demand around wearable devices continue to grow and diversify rapidly in use and applicability. In 2015, about 100 million smart wearable devices were in use, with about 35 percent in Asia-Pacific and 40 percent in North America. These numbers are expected to expand to almost 600 million in use globally by 2020, with both Asia-Pacific and North America reaching almost 200 million each.[3]

Figure 2—Industry Categories of Respondents

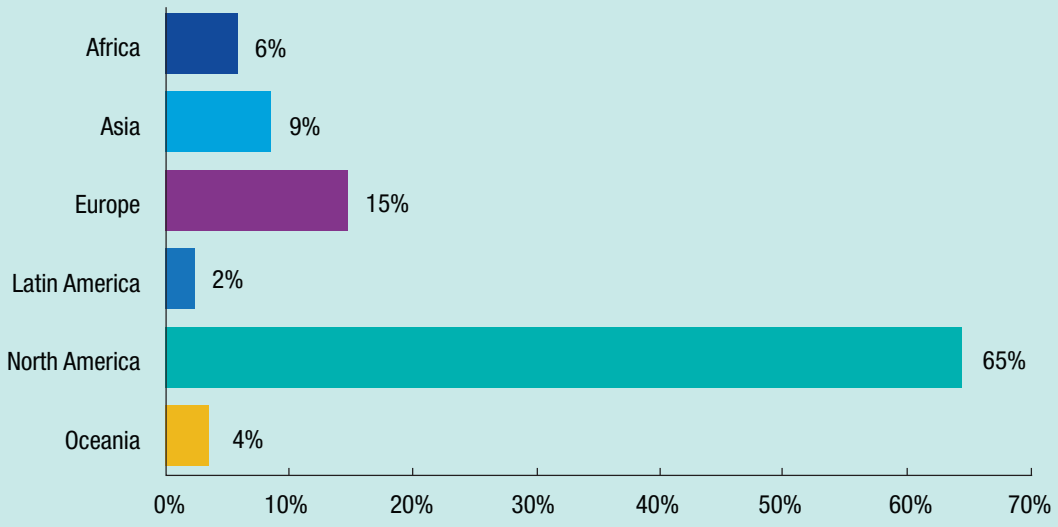


Note: Financial Services accounts for approximately 35%.

- Financial/Banking 25%
- Insurance 5%
- Public Accounting 5%

Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

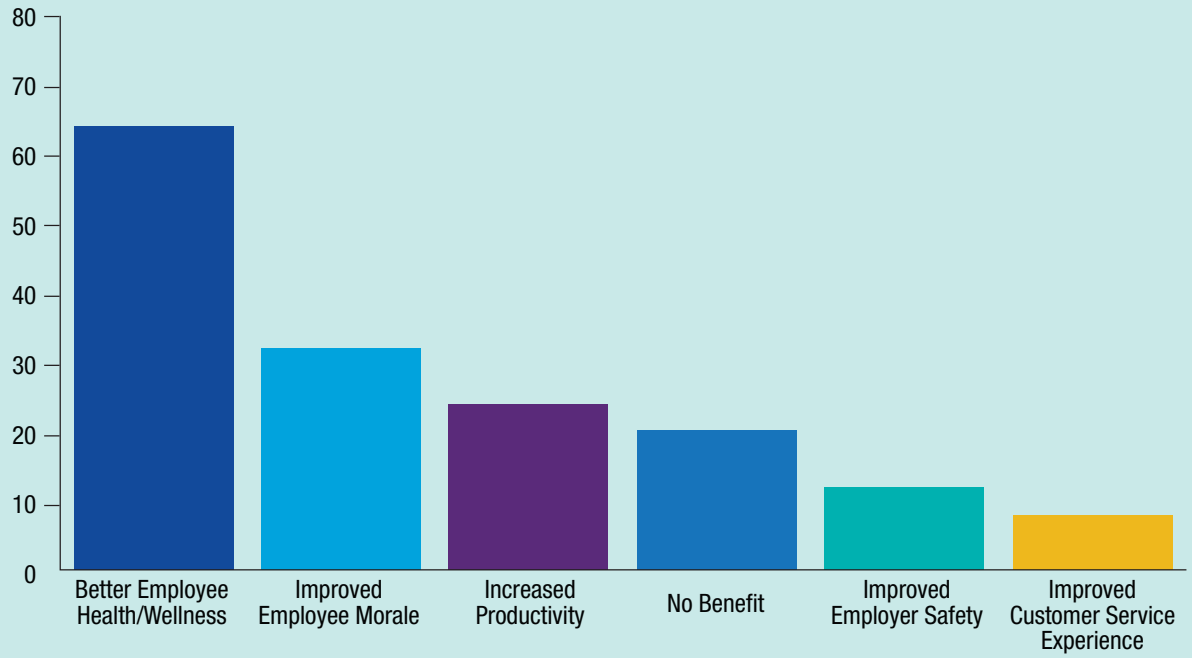
Figure 3—Geographic Region of Respondents



Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

Figure 4—Benefits of Wearables in the Workplace

Which, if any, of the following do you consider a benefit of wearables in the work space? (Select all that apply.)

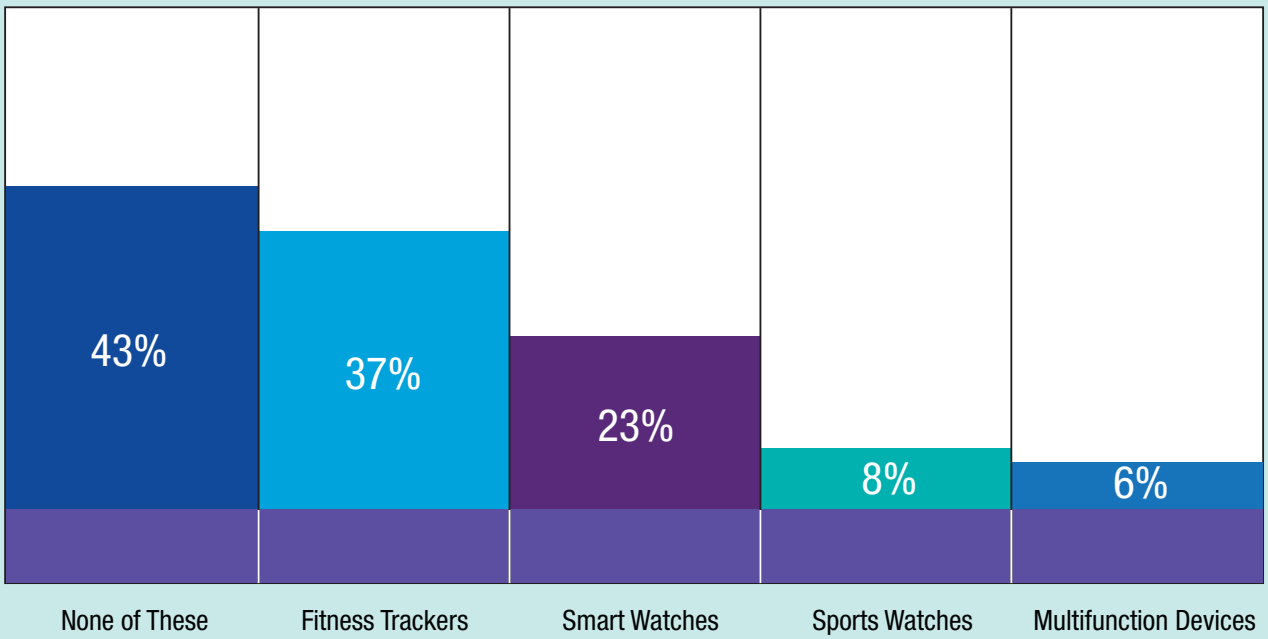


Note: Recipients selected "reduction in inventory loss" and/or "cost reduction" as benefits less than 5 percent of the time.

Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

Figure 5—Ownership of Wearables

Which, if any, of the following types of wearable devices do you currently own? (Select all that apply.)

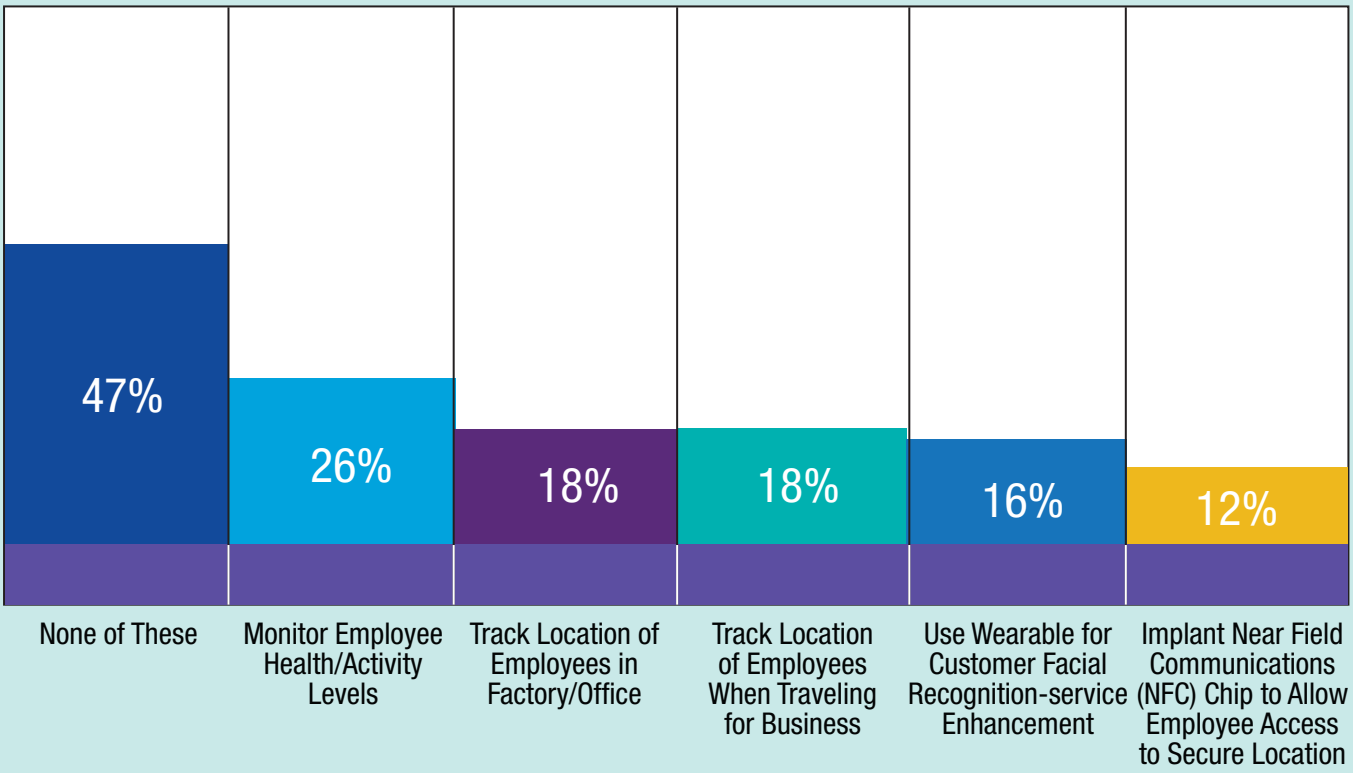


Note: Head-mounted displays, smart clothing, smart jewelry and implantables were owned less than 5 percent of the time.

Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

Figure 6—Support of Wearables in the Workplace

Below is a list of possible scenarios that an employer could undertake using wearable devices. Which, if any, would you support? Select all that apply.



Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

Concurrent with the rapid expansion in this market is a great deal of interest in improving security awareness around these devices.

Wearables are more personal than smartphones and are often in direct physical contact with the body. Compatibility and usability issues may make it difficult for an employer to mandate the use of wearable devices for certain uses.

Just as with smartphones in the past, it is likely that a majority of the world's population will soon use a smart, connected device and possibly more than one device. Hence, it is imperative to promote security awareness and help enterprises build the necessary infrastructure, policies and skill sets required to deal with smart, connected devices accessing the corporate network.

For companies with large workforces, the prospect of tracking people's whereabouts and productivity can be beneficial. However, collecting data on employees' health and their physical movements can trigger a host of potential ethical and legal headaches for employers such as human resources (HR) personnel disputes; personal privacy, health or disability claims; and worker performance measurement difficulties.

Some companies already encourage employees to wear fitness trackers as part of optional corporate wellness programs. If employers require device usage as part of a role, an employment contract must detail this information.

Employees can share their step counts or hours of sleep with their employer or health insurance provider, usually allowing the employer to get preferential terms on employee insurance. This is a great employee

benefit, assisting with health and wellness goals and providing a financial incentive as well.

Guidelines for both employee and employer usage of wearables will be critical to help mitigate potential issues in the workplace. Employers will need to consider putting in place policies governing how staff use the technology (**figure 8**).

Important Opportunities and Challenges

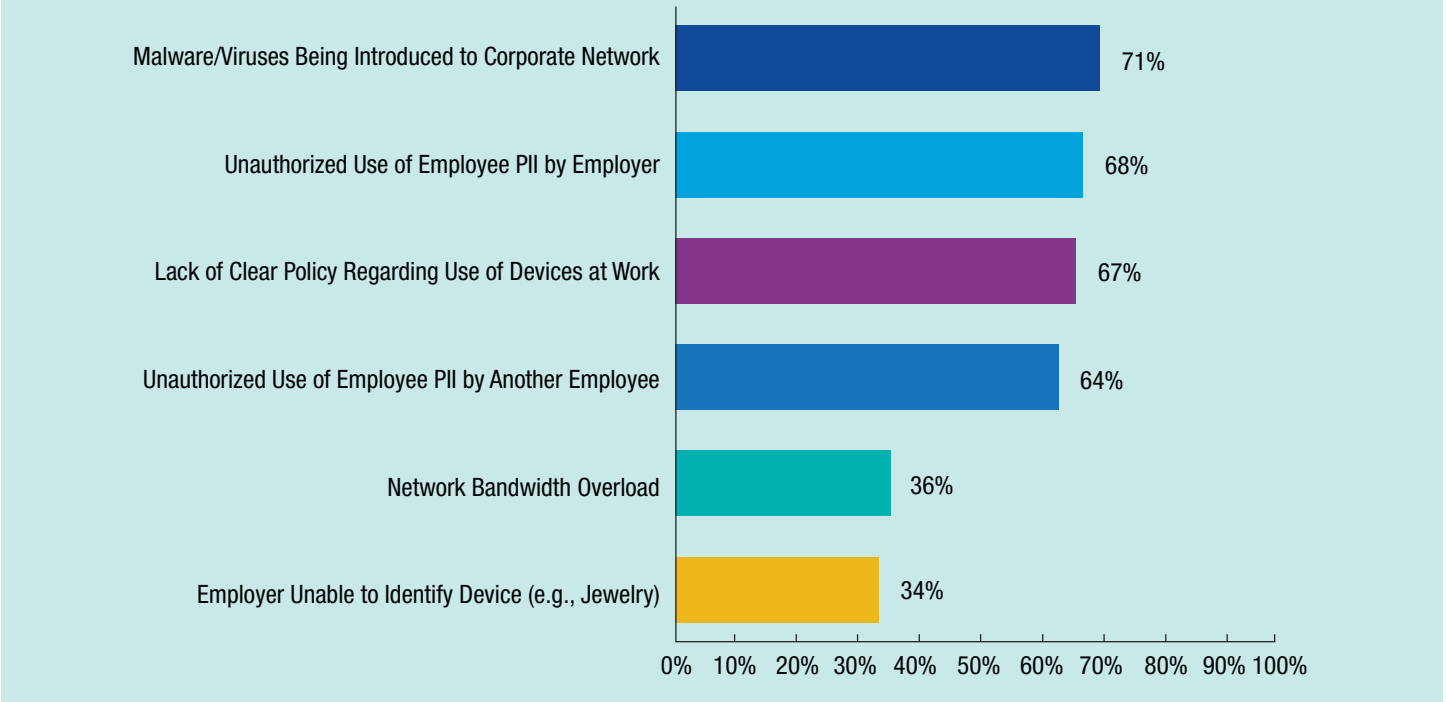
Wearables are enabling a wide range of new digital opportunities and posing new challenges. The research team explored the insights and perspectives of the survey respondents. Almost 56 percent of respondents felt employees should be allowed to connect their personal wearable devices across employers' corporate WiFi, and approximately 25 percent already bring in their wearable devices and connect to the corporate WiFi network. Overwhelmingly, the survey respondents agree that there are no restrictions on wearable use in the workplace today, but they feel there should be.

"Overwhelmingly, the survey respondents agree that there are no restrictions on wearable use in the workplace today, but they feel there should be."

It appears by their answers that survey respondents would like to take a more conservative stance on wearables usage, given the current immaturity of controls over wearables. This is indicative of the early stage of wearable technology and the lack of business strategy to address the associated risk.

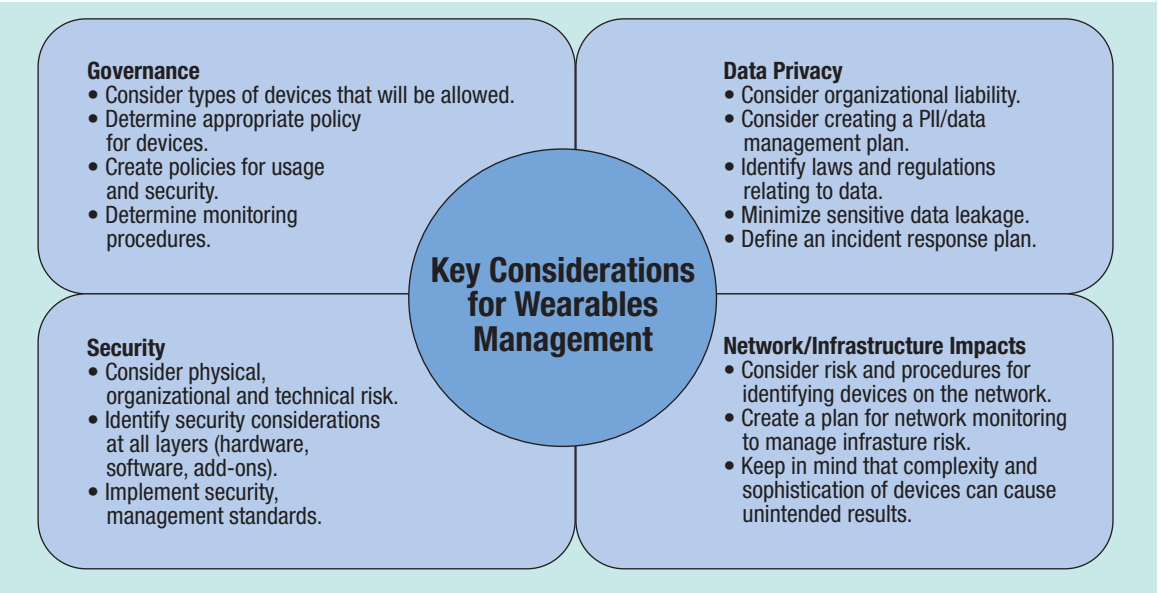
Some of the top concerns by survey respondents include (**figure 7**):

Figure 7—Concerns About Wearables in the Workplace



Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

Figure 8—Key Considerations for Management of Wearables



Source: ISACA Phoenix Chapter Research Committee. Reprinted with permission.

- 71 percent felt there is a danger of malware/viruses being introduced to the corporate network.
- 68 percent indicated there is a risk of unauthorized use of employee personally identifiable information (PII).
- 67 percent felt that clear guidance and policy are lacking.

These results illuminate that the emerging technology and market behind wearables. Combine this with the rapid speed of new product introduction and it becomes important for corporate policy managers to respond quickly. This rapid growth is similar to the previous emergence of BYOD policies for mobile computing devices that many organizations now have.

Compliance and Wearables

This group of responses clearly indicates that the survey community is not comfortable with the collective readiness to handle wearable devices in the workplace:

- More than 80 percent responded negatively (33 percent) or indicated feeling unsure (49 percent) about whether employers are keeping up to date on wearable compliance regulations.
- More than 76 percent feel similarly about controls to adequately protect PII.
- Approximately 64 percent believe that they or their employers have the responsibility to let people around them know about their own wearables or wearables being worn nearby.

Key Insights

Most people would agree that wearables are attractive, even "cool," but the concerns about them are alarming. Respondents noted several benefits to the use of wearables in the workplace: health and wellness, morale, and productivity. However, the responses to this survey highlight concerns about the immaturity of technology controls and potential privacy risk:

- **Rules and guidelines needed**—Nearly 60 percent of respondents supported restrictions on the types of wearables in the workplace and supported initiatives to disallow wearables in the workplace.
- **PII protection required**—More than 75 percent felt that employers lack controls to protect PII from wearables.

- **Employer responsibility**—Sixty percent reported that their employer is responsible for protecting PII on the network.
- **Regulatory adherence**—More than 80 percent were not convinced that employers are keeping up to date with applicable regulations.
- **Missing usage restrictions**—Almost two-thirds indicated that employers do not have restrictions on the kinds of wearables employees can use at work.

The disruptive business growth of wearable technology presents a whole new set of challenges and questions for individuals and organizations. Technology transformation is occurring at an exponential rate, understandably making proactive management difficult. A challenge for technology management is to help reap the benefits of technology while substantially managing its risk.

In light of these findings, the following are some key questions that organizations should ask themselves:

1. Should employees be allowed to use wearable devices while at work?
2. How will wearables impact the workforce?
3. What is the risk, including security risk, that should be considered?
4. Would wearable devices be appropriate within the context of the industry or location?
5. Which department(s) within the organization would be responsible for implementing and managing policies relating to wearable devices?
6. What laws and regulations need to be followed?
7. Will the organization have access to or need to manage PII that is gathered via these devices?
8. How will device onboarding, management and decommissioning be managed?
9. What are the financial implications and costs associated with allowing wearable devices?

The research reported in this article resulted in the key considerations illustrated in **figure 8**, a good starting point in governance development.

While there are many items that could be considered when allowing the use of wearable devices, the four key areas are governance, security, data privacy and network/infrastructure impacts, as shown in **figure 8**.

“The disruptive business growth of wearable technology presents a whole new set of challenges and questions for individuals and organizations.”

Management must first determine what types of devices will be allowed and what the policies are relating to these devices. Are the devices going to be provided to employees or would employees be bringing these devices into the workplace? Are the devices going to be used for work purposes, for personal usage, or both? The answers to these questions could have an impact on the security, data management and device life cycle management components.

There are several security considerations when allowing wearable devices in the workplace. Given the wide variability and connectivity there is no “one-size-fits-all” security strategy that can be applied. Each organization should carefully weigh the risk vs. the benefits of allowing these devices. Risk relating to physical, organizational and technical aspects should be considered and evaluated. Further, the technology behind these devices and the interconnectivity between devices often cause additional risk that needs to be considered.

Management should look at all layers, including hardware, software and add-on accessories, as part of the security assessment. Creating a comprehensive security standard that is based on an established framework can greatly reduce risk and allow management to take a proactive approach to securing devices.

Depending on how these devices are going to be used in the workplace, management may need to consider the risk and procedures relating to the entire life cycle, which includes the onboarding, usage and deactivation of devices. Handling lost or stolen devices and providing reimbursement are additional topics that may need to be considered.

The ISACA Phoenix Chapter research committee concludes that although the rate of wearables proliferation is astounding, ISACA's global community has an important opportunity. Because usage is still limited to the personal spectrum, there is a window of opportunity to institutionalize a governance model before the risk becomes a new normal.

Endnotes

1 Haggin, P.; "How Should Companies Handle Data From Employees' Wearable Devices?," *The Wall Street Journal*, 22 May 2016

2 Tehrani, K.; A. Michael; "Wearable Technology and Wearable Devices: Everything You Need to Know," *Wearable Devices Magazine*, March 2014, *www.wearabledevices.com/what-is-a-wearable-device/*

3 Cisco Systems, Inc., *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update*, 2015–2020,1 February 2016, p. 38