The Wearables Revolution Has Arrived

HOW TECHNOLOGY COMPANIES CAN MANAGE THE RISKS OF WEARABLES TO REAP THE REWARDS
How technology companies can manage the risks of wearables to reap the rewards

At one time, people scoffed at the idea of a personal computer in every home. Today, we not only have high-speed Internet available in our homes, but we also connect to the Internet at will with a variety of mobile devices from wherever we happen to be. Tomorrow, we will be wearing Google glasses that allow us to instantly access all the information we need about anything that can be imagined.

In a previous issue of the Travelers Technology Risk Advisor series, I shared our vision for the Bring Your Own Device (BYOD) trend and how enterprises can manage their risks related to it. Today, we find ourselves in the midst of another mega-trend in technology: wearable devices.

Wearable devices represent an exciting and lucrative opportunity in several markets, with many of the world’s most innovative technology companies leading the way. Smart glasses, watches, armbands, and even clothing, hold the potential to transform the way we live our lives. Perhaps some of the biggest quality of life improvements will come in the medical and health care space, where wearable technology holds the promise of detection, prevention, and treatment of chronic disease.

Along with the tremendous upside potential, there are risks involved along the way that must be managed. Device makers and others who understand these risks will be better positioned to protect themselves from liability should devices go awry. This issue of the Travelers Technology Risk Advisor series will expose some of those risks and highlight actions wearable manufacturers should consider as we move forward into The Wearables Revolution.

– Mike Thoma
Chief Underwriting Officer, Travelers Technology

The “risk scenarios” described in this document are intended to facilitate consideration and evaluation of risks and are not necessarily based on actual events. Also, the insurance products sold by Travelers or other carriers may or may not provide coverage for all of the “risk scenarios” described. Circumstances vary, and some risks may not be insurable. Companies should consult an independent agent or broker to evaluate what coverage is right for them.

The “actions to consider for minimizing risk” described in this document are also intended to facilitate consideration and evaluation of how risks can be mitigated. These are not direct guidance or advice on what actions should be taken. Other actions may be appropriate, depending on the circumstances. Companies should consult an independent agent or broker to evaluate what risk management products or services are right for them.
Executive summary

The wearable technology revolution promises to make us more connected and change our lives for the better. Fitness trackers will give us new insights to improve our health, exercise, and diet. Smart watches will keep us organized and better informed. Wearable virtual reality and holographic devices will take us to new worlds with the press of a button. Many of the largest and most innovative technology companies are aggressively pursuing the wearables opportunity, as are many emerging startups.

Along with the many opportunities, wearable technology also creates new risks. Broadly speaking, wearable technology creates risks for three categories of companies:

a) Technology companies directly involved in the development, manufacturing, and distribution of wearable devices.

For example, medical technology firms that handle personal health information collected from wearable cardiac monitoring devices could incur significant liability and expenses if they fail to appropriately safeguard such data. Likewise, firms that make holographic devices could be at risk if their products are blamed for highway accidents due to their customers using their products behind the wheel.

b) Technology companies acting as vendors or suppliers to wearable technology companies.

For example, a software company supplying GPS software incorporated into a wearable security device could be held responsible if a user’s location history data is stolen. An electronics manufacturer supplying a component part for a hinge within a wearable prosthetic leg could be blamed if the device fails, resulting in a severe patient injury.

c) Other companies not traditionally considered technology firms that are now integrating wearable technology into their products.

As textile companies integrate electronic monitors into clothing, they could be exposed to bodily injury risks they had not previously considered. As shoe companies integrate smart sensors into their footwear, they could be exposed to additional liability.

In this issue of our Technology Risk Advisor series, we look at both the upside and the downside of wearable technology. First, we consider wearable technology market size projections, identify key market drivers, and review prominent wearable technology product categories. Then, we identify and explore specific risk classes impacting companies involved with wearables, and we highlight for consideration several specific actions to minimize business risks. Finally, we conclude by highlighting insurance considerations that firms should evaluate with their independent agent or broker, as they pursue the lucrative wearable technology market.
Wearable technology and the Internet of Things (IoT) are poised to redefine mobility in the coming years. SNS Research estimates that wearable device shipments will account for nearly $20 billion in revenue in 2015, and grow at a CAGR of 40 percent over the next six years. Swiss research firm Soreon expects the wearables market to top $40 billion by 2020 in the health care market alone.

Several global market forces are driving the wearables adoption rate, all of which promise to change how we live and how we work. Companies that recognize and understand these drivers position themselves to capitalize on this lucrative and rapidly expanding field.

**DRIVER 1: MOORE’S LAW AND THE MINIATURIZATION OF TECHNOLOGY**

Perhaps one of the most powerful drivers is the technology itself. Gordon Moore, founder of Intel and Fairchild Semiconductor, wrote a paper in 1965 noting a doubling in the number of transistors per integrated circuit approximately every two years. This phenomenon, which has continued on a remarkably consistent path, has had a profound impact on digital electronics, allowing smaller devices to assume greater power.

The earliest UNIVAC machines of the 1950s filled rooms the size of department stores. On a regular basis since then, computer companies have released smaller and more powerful models, culminating in today’s high-powered smartphones and tablets. Wearable devices are simply the next iteration of this trend toward miniaturization of computing. When asked about the design of his new smart watch, Apple Chief Design Officer Jonathan Ive said, “It’s technology worn on the wrist. I sensed there was an inevitability to it.”
In the corporate sector, wearable devices promise innovation leading to productivity gains and cost savings. Field technicians wearing smart glasses and head-mounted cameras can send real-time video of off-site problems, eliminating the need for costly consultant travel. Many police departments have purchased wearable cameras for their officers and field investigators to gather crime scene data and interactions with the public.

But employees won’t be the only ones wearing these devices. Companies are now developing mobile devices with Near Field Communication (NFC) chips that enable customers to make credit card payments directly from their devices. Marketed as a combination of function and fashion, these wearables are the next step toward frictionless payment systems – a concept industry experts hope will increase revenues. Disney has invested $1 billion (USD) on the magic wristband, a wearable device that makes it easier for guests to enjoy their theme parks.
As hospital stays become shorter, many doctors are sending patients home with wearable health sensors. These devices can capture real-time vital signs and transmit results to doctors or response personnel in the event of an emergency.

Industry experts predict that substantial investment in wearable devices will come from the health and medical sector. The weight loss and longevity markets have been extremely profitable in recent years, a trend that is likely to continue. In a recent PricewaterhouseCoopers survey, 56 percent of the respondents felt that wearable health devices could extend their life expectancy by 10 years. Forty-six percent see these devices as a way to help control obesity, and 42 percent expect health wearables to improve their athletic ability.

As hospital stays become shorter, many doctors are sending patients home with wearable health sensors. These devices can capture real-time vital signs and transmit results to doctors or response personnel in the event of an emergency. Likewise, big data is big business in the medical sector. IBM finds the medical market so attractive that they have invested $1 billion (USD) in IBM Watson Health, a global analytics cloud, storing health information powered in part by wearable device data feeds.
**DRIVER 4: SAFETY AND SECURITY APPLICATIONS**

Employee safety has become a major concern in the workplace. Many employees are required to use both hands when operating forklifts or heavy industrial equipment. As part of their job, they must also shift their focus to enter job-specific data into a PC terminal. Wearable devices can make them safer by automatically capturing and/or recording data without requiring them to break concentration on the task at hand, keeping both hands free at all times.

Wearable devices can also help keep individuals safer outside the workplace. Even though crime rates are on the rise in many major metropolitan areas, some device makers are marketing smart safety devices disguised as common jewelry. The Safelet smart necklace looks like a fashionable women’s pendant; it’s actually a smart transmitter that can notify law enforcement or a list of pre-configured contacts, and pinpoint the user’s exact location via GPS in the event of an emergency.

**Employee safety has become a major concern in the workplace.**

**DRIVER 5: MILLENNIAL LIFESTYLES**

The Millennial Generation, often defined as those born between the early 1980s and 2000, has scarcely known life without the Internet. Frequently tethered to their smartphones, Millennials are well suited to become early adopters of wearable technology not only in the workplace, but also at home. And because they are far more interested in productivity and convenience than security, they are certain to wear their devices to work, even at the expense of IT directives.

**The Millennial Generation, often defined as those born between the early 1980s and 2000, has scarcely known life without the Internet.**
Key categories of wearable technology – and their impact

Regardless of their physical size or commercial application, wearable devices have **three enabling technologies** that make them “smart.”

<table>
<thead>
<tr>
<th>Sensors</th>
<th>Microprocessors</th>
<th>Transmitters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensors that capture impulses from the user’s body or surroundings, which they translate into actionable data</td>
<td>Microprocessors that extract, transform, and load the data into a transmittable format</td>
<td>Transmitters that wirelessly send the data to a cloud storage for further processing and reporting</td>
</tr>
</tbody>
</table>

Armed with these components, smart wearables are not only capable of powerful computing, but are also comfortable and fashionable to wear. The following wearable device categories are among those with the greatest market potential and relevance to the previously described applications.

**CATEGORY A: SMART GLASSES AND HEADGEAR**

Devices such as Google Glass and the Vuzix M100 present the user with a miniature display similar to a computer monitor. Onboard cameras and tilt sensors allow the device to capture the user’s field of vision and even record the results to the cloud. These devices present a semi-see-through display, allowing the user to view computer output without impeding natural vision. How well they accomplish this varies from user to user.

While many smart glasses promise business benefit, others are aimed squarely at the infotainment market. Oculus VR’s virtual reality headset, Oculus Rift, promises a premium gaming experience with less latency than its predecessors. The company has also partnered with Samsung to produce Gear VR, an Android-specific headset allowing Galaxy Note 4 users to operate their smartphones in virtual reality.
In addition to telling time, most smart watches offer the same standard mobile apps found on their smartphones such as email, instant messaging, calendar, and GPS. But third-party developers are creating a catalog of apps to enhance user utility, both at work and at home. OfficeTime for the Apple Watch allows users to track and tag the time they spend in various meetings and then display a detailed breakdown of their time usage for the week. Another app, Home Remote for iOS and Android smart watches, allows homeowners to lock doors, turn on lights, and even start to cook dinner, all from the touch of an icon.

Making mobile payments has always been difficult for smartphones, which is why so few people use them for that purpose. Smart watches, however, could be the key to making mobile device payments more popular. A smart watch with a payment app can authenticate transactions and transfer funds faster and easier than any smartphone. It does, however, contain a user’s personally-identifiable information, which the watch will access through wireless communication.

In their current and upcoming versions, smart watches can do very little unless paired with a smartphone. Apps must first be installed on the smartphone, then transferred to the watch when the two are synchronized. App developers have hinted that this requirement will go away in future versions of smart watches.

Positioned firmly in the health market, fitness trackers appeal to users’ desire for self-improvement. By tracking and reviewing their fitness activities over time, users can make lifestyle changes to improve their overall health and longevity. Wearable fitness trackers like the Fitbit, Nike FuelBand, and Microsoft Band can detect all user activity throughout the course of their day, not just activity traditionally thought of as exercise.

Most fitness device manufacturers offer progressively more powerful models, each at successively higher price points. The most basic models track steps taken, calories burned, and sleep quality. More advanced versions can track heart rate, blood pressure and display human-readable workout coaching, although some add-on hardware may be required for those features. The highest-end devices combine fitness tracking with smart watch capabilities like email, reminders, call notifications, and social media updates.

Most fitness device manufacturers offer progressively more powerful models, each at successively higher price points.
**CATEGORY D: WEARABLE MEDICAL DEVICES**

Eighty-six percent of health care spending is for patients with one or more chronic conditions, and 71 percent of health care spending is for patients with multiple chronic conditions. Chronic diseases have become such a focal point that the Centers for Disease Control has launched community involvement initiatives to help the general public recognize the onset of chronic disease and take preventative action.

For diabetics, the Medtronic Continuous Glucose Monitoring system measures blood sugar levels through electronic sensors placed slightly under the skin. A wireless transmitter attached to the patient’s belt processes the data and transmits it to cloud data stores for later analysis. It even decreases fingerstick requirements to only two per day. An optional insulin pump delivers insulin as needed, without patient intervention.

Cardiac patients can benefit from wearable heart monitors. The ZIO Wireless Patch detects irregularities in cardiac rhythm, and is far less bulky to wear than the legacy Holter monitor. For more severe cardiac cases, the ZOLL LifeVest Wearable Defibrillator can detect life-threatening abnormal heart rhythms and deliver a treatment shock to restore healthy cardiac rhythm.

Transcutaneous electrical nerve stimulation (TENS) devices help patients who suffer from chronic pain. These devices hook to a patient’s belt and deliver a continuous low-voltage electrical current to the painful area of the body. For some patients, the current blocks pain signals by stimulating certain nerves.

One of the unfortunate symptoms of Alzheimer’s disease is wandering, often at night when caregivers and other family members are asleep. A brilliant 15-year-old invented a wearable device to detect his beloved grandfather’s wanderings. An ultra-thin sensor combined with a coin-sized wireless circuit detects the patient’s movements and alerts a caregiver’s smartphone, prompting intervention to prevent injury.

**CATEGORY E: SMART CLOTHING AND ACCESSORIES**

Just as wearables are the next iteration of mobile devices, smart garments stand to become the next iteration of wearable fitness trackers. As one Gartner research director explained, “Because smart shirts and other smart garments can hold more sensors closer to the skin, they can collect more information and produce better data, like the full wave of the heartbeat rather than just the pulse.”

But smart clothing applications aren’t limited to fitness metrics. Visijax improves cyclists’ safety with a self-lighting jacket to make them more visible in the dark. Exmobaby markets baby-tracking smart pajamas laced with movement sensors and a monitor for parents to keep track of their young children. One company even markets a smart baby diaper to alert parents the moment their child needs changing.

Smart armbands, another type of wearable health device, work on the principle of gesture control. They fit over the forearm or bicep, and listen for the slightest adjustments in the user’s muscles. The device’s firmware translates muscle impulses into gestures on a screen. Using Thalmic Labs’ Myo™ armband, doctors can page through medical documents while performing surgery without ever putting down a scalpel. The challenge facing developers will be distinguishing between a user’s true intentions and incidental muscle movement, often referred to as “garbage” input.
The market potential for wearable devices is undeniable. These miniature computers hold the capacity to drive innovation in the corporate sector while reducing costs and improving productivity. Likewise, in the medical field, these devices not only reduce health care costs, but can also improve quality of life.

But as great as the upside potential is for companies involved with wearable technology, the downside liability risk cannot be ignored. Should a device fail at an inopportune time, a business can lose millions of dollars, a consumer’s privacy can be compromised, or a patient can lose their health or even their life. Companies should closely consider three major risk categories posed by wearable devices, so they can decrease their exposure to costly liability claims. These risk categories are cyber, bodily injury, and technology errors and omissions.

Three risk classes wearable technology companies should understand

The market potential for wearable devices is undeniable. These miniature computers hold the capacity to drive innovation in the corporate sector while reducing costs and improving productivity. Likewise, in the medical field, these devices not only reduce health care costs, but can also improve quality of life.

But as great as the upside potential is for companies involved with wearable technology, the downside liability risk cannot be ignored. Should a device fail at an inopportune time, a business can lose millions of dollars, a consumer’s privacy can be compromised, or a patient can lose their health or even their life. Companies should closely consider three major risk categories posed by wearable devices, so they can decrease their exposure to costly liability claims. These risk categories are cyber, bodily injury, and technology errors and omissions.
CLASS 1: CYBER RISK

Cyber risk is often defined as the risk of financial loss, business interruption, or reputational damage due to an organization’s failure to properly secure the data held within its information systems. It can occur as a result of a cyber criminal’s attack, an ineffective IT policy, a failure of IT security software, or even a disgruntled employee.

Cyber risk is a growing concern for enterprises across all sectors, and with good reason. The Identity Theft Resource Center shows an alarming trend in the rate of data breaches. A record-high 783 organizations reported data breaches in 2014, a 27.5 percent increase from the previous year. The economic damage from such data breaches can be catastrophic. The 2014 Ponemon Institute cyber crime study shows the total annualized cost of cyber crime to range from a low of $500,000 to a high of $61 million with a mean annualized cost of $7.6 million.

Nearly all high-profile data breaches lead to proposed class-action lawsuits. Wearable device manufacturers can certainly be among the defendants in such suits if a device is alleged to have played a role in a breach.
Illustrative risk scenarios: Cyber

**CARDIAC HACKING**
A cardiac patient’s wearable heart monitor automatically uploads a block of health data to a cloud data store. The overwhelmed IT department in charge of the cloud database inadvertently fails to apply a security patch correctly, allowing a hacker to gain entry, steal, and sell the sensitive data.

**SIGNAL INTERCEPTION**
An employee brings his own smart glasses to work, which are connected to his smartphone. His phone, in turn, is connected to a company network where sensitive customer data is stored, such as credit card and account numbers. A thief intercepts the Bluetooth feed from the smart glasses display en route to a cloud data store, stealing customer’s login credentials to drain bank accounts.

**PRIVACY INVASION**
An asthma patient wears a device that monitors her vital signs and environmental factors, including air quality, to help her avoid conditions that exacerbate asthma. The device frequently transmits data to her cellphone and doctor. She boards a city bus where she sits next to a cyber enthusiast with a Bluetooth sniffer. He intercepts the signal and sells the data to health data brokers and marketers.

**CORPORATE ESPIONAGE**
An executive enters his building wearing a wireless identity authenticator. Unbeknownst to him, a similarly dressed corporate spy enters a few steps behind him armed with a wireless signal interceptor. After capturing the executive’s unencrypted PIN number from the electronic signature, the spy can now move about the building with all the permissions the executive enjoys, including access to intellectual property, which he then sells to competitors.

**MALWARE INFECTION**
A user with a smart watch connects to her phone to pay bills. However, the user also downloaded a third-party app loaded with malware that detects and records financial activity. Because her user ID and password are passed in plain text from the smart watch, the malware captures it and sends it to an offshore hacker group that silently runs up huge credit card charges.
Actions to consider for minimizing risk: Cyber

Wearable device manufacturers shoulder the burden of proof to demonstrate that the data detected by their wearable device was properly safeguarded. That means that wearable devices should be engineered with data security in mind.

However, because some tech firms may focus more on successful product launches, they ship their devices with default settings that promote ease-of-use, which are also the least secure. Companies can often protect themselves by designing some simple, yet effective security features into their devices. They should consider the following steps to help minimize exposure to cyber risk:

• **Custom security level.** Give the user the ability to choose the security level they are comfortable with when they install their device or pair it with their smartphone. Users seldom consider security when wearing their devices, so defaulting to the least secure settings opens a vulnerability for hackers to exploit.

• **Remote erase feature.** Enable wearable users to remotely erase and/or disable their device if it is ever lost or stolen. Apple does this with the most recent version of the iPhone. Wearable device manufacturers should consider offering the same feature.

• **Bluetooth encryption.** Bluetooth offers an encryption API when exchanging data between a device and its target data store, but few companies take advantage of it because it decreases battery life.

• **Encrypt critical data elements.** The most critical pieces of data transferred between wearable devices and data stores are user IDs, passwords, and PIN numbers. Incredibly, most wearable devices transmit these data elements in plain text with no encryption at all.

• **Secure the cloud.** Data is often transmitted from a wearable device to a smartphone and then to a cloud data store. Virtualized clouds can secure data with multiple diverse operating systems, each operating within a different security context. Banks often secure depositor payment details this way; wearables companies should consider similar functionality.
In order for wearable devices to deliver on the quality of life benefits they promise, devices must be used as intended and function properly at all times. Should they ever fail, the device maker could be liable for bodily injury risk: damages from a resulting injury, illness, or even death of a user or patient. Wearable manufacturers should understand and mitigate the risk of a product liability claim.

According to the online consumer legal knowledge base, nolo.com, any of the following three issues can form the basis of a product liability lawsuit.

1. **Defective design**
   
   These devices were engineered with a design so hazardous that a reasonable patient could use the device as instructed, yet still suffer bodily injury. This defect occurs on the drawing board, long before manufacturing begins. If patients can prove the manufacturer knew the danger but took no action, courts may award punitive damages as well.

2. **Defective manufacturing**
   
   These devices were either manufactured improperly or damaged in a way that prevents their proper use. This defect can occur at any point between the factory and the place the patient received the medical device.

3. **Defective marketing**
   
   These devices were designed and manufactured properly, but the patient wasn't properly instructed how to use the device properly or warned about the dangers of using it improperly. Often referred to as the “bad advice” category, these defects occur after the patient has been given the device. Poor documentation, warning labels, or even failure to anticipate improper use of a device is enough to trigger a defective marketing lawsuit.
### Illustrative risk scenarios: Bodily injury

<table>
<thead>
<tr>
<th><strong>ABRASIONS</strong></th>
<th><strong>RISKY BEHAVIOR</strong></th>
<th><strong>ADVERSE REACTION FROM WIRELESS COMMUNICATION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A company develops a smart contact lens with an embedded chip to monitor glucose levels in diabetics’ tears. The device analyzes data through a tiny pinprick hole in the lens. Due to a flaw in the production process, the hole is manufactured improperly, producing sharp edges, causing abrasions to users’ eyes.</td>
<td>Extreme sports enthusiasts gain notoriety by publishing YouTube videos of themselves performing daring activities while wearing “smart helmets” that include cameras. Several users suffer serious back and neck injuries while performing these activities. The device maker is blamed in court for having encouraged the risk.</td>
<td>Smart fitness garments transmit data from sensors to a computing device via short-range radio waves. Prolonged exposure to specialized materials in the sensors leads to an allergic reaction and an allegation of skin and muscle damage by a user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>MISINTERPRETED INPUT</strong></th>
<th><strong>DETECTION FAILURE</strong></th>
<th><strong>SELF-DIAGNOSIS AND OVEREXERTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A smart mechanical knee should become rigid when it detects a patient’s heel strike while walking. The device misinterprets a user’s input on a flight of stairs and goes soft instead, causing a fall and subsequent injury.</td>
<td>A wearable device designed for early disease detection fails to warn a patient about critical health indicators. Without detection from the device, the patient eventually develops a late stage debilitating disease. The patient files a lawsuit against the manufacturer.</td>
<td>A fitness tracker device broadly categorizes activity metrics and exercise recommendations into high, medium, and low intensity levels, leaving many specifics up to the interpretation of individual users. Interpreting activity recommendations from her fitness tracker, a user overexerts herself, leading to a cardiac event. The user sues the device maker.</td>
</tr>
</tbody>
</table>
Actions to consider for minimizing risk: Bodily injury

Companies in the wearable technology market bear a responsibility to ensure that consumers and patients do not suffer injury, illness, or death due to the use of these products. Therefore, it is crucial that companies prepare for all possible outcomes from a user’s experience, particularly those that may result in class action or mass tort lawsuits due to bodily injury risks.

Direct and reputational costs from product liability events can cripple wearable technology companies, sometimes endangering their very existence. Companies should consider the following steps to help minimize exposure to bodily injury risk:

- **Conduct extensive testing.** Device makers should not only test their own systems, but also insist that all electronic components that go into their devices undergo the same testing procedures. This is particularly important for components purchased from overseas developers whose local regulations may not be as stringent.

- **Conduct robust hazard analysis.** Methods such as preliminary hazards analysis (PHA), fault tree analysis (FTA), failure mode and effect analysis (FMEA), hazard and operability (HAZOP), and hazard analysis and critical control point (HACCP) can be used to identify and assess potential device hazards at different points in device development and commercialization. These can involve identifying the major components and operating requirements (e.g., raw materials, hardware, device interfaces, operating software, services, and the wearable operating environment) and then identifying potential hazards for each. Hazards can include anything from toxicity and flammability, to unsafe delivery of energy and administration of drugs, to mechanical or electronic hazards. Companies should not ignore hazards that can be introduced during processes such as manufacturing, packaging, labeling, storage, or transport.

Companies should not ignore hazards that can be introduced during processes such as manufacturing, packaging, labeling, storage, or transport.
Companies should assess the likely frequency and severity of all identified potential hazards. Companies should seek to eliminate all high-severity hazards and reduce the potential for medium- and low-severity hazards. Assemble a diverse team that includes personnel outside of the design process to generate potential mitigation solutions.

- **Plan for mitigation.** Companies should assess the likely frequency and severity of all identified potential hazards. Companies should seek to eliminate all high-severity hazards and eliminate or reduce the potential for medium- and low-severity hazards. Assemble a diverse team that includes personnel outside of the design process to generate potential mitigation solutions. Task the solutions team with considering how specific hazards have been mitigated for analogous industries or device categories.

- **Evaluate awareness of and adherence to key standards.** Ensure that all relevant personnel in your company are aware of and adhere to applicable standards. For example, for wearables classified as medical devices, evaluate whether and how your company adheres to ISO 14971 (for the application of risk management to medical devices) and ISO 13485 (for a comprehensive quality management system for the design and manufacture of medical devices).

- **Build in cybersecurity.** A lack of cybersecurity in wearable technology creates the potential for bodily injury. A wearable device designed to deliver medication or electrical stimulation could be breached, resulting in serious consequences for the user. For wearables classified as medical devices, the FDA recommends that where appropriate, companies provide physical locks on devices and their communication ports to minimize tampering. The FDA also recommends implementing device features that protect critical functionality, even when the device’s cybersecurity has been compromised.

- **Develop clear safety and use instructions.** Provide users with clear, unambiguous written instructions on the full range of use for wearable products. Include visual depictions of proper device use. Provide warnings on types of use that should be avoided, with a focus on potential key hazards. Incorporate information on proper device storage and transportation, as well as instructions on what to do if the device malfunctions.

For wearables classified as medical devices, the FDA recommends that where appropriate, companies provide physical locks on devices and their communication ports to minimize tampering.
Despite a wearable device maker’s effort to market a reliable product that people can use to enhance their quality of life, things can go very wrong. In addition to bodily injury, a company can be held liable for an economic loss from the failure of a device to work as intended, due to an error, omission, or negligent act.

Wearable device failures can impact business continuity, reputation, and other factors. Companies who understand the unique nature of this risk category can better protect themselves from liability claims. The following scenarios illustrate how wearable device manufacturers, vendors, and component part suppliers could be held liable for a device’s failure or misuse.
Illustrative risk scenarios: Technology errors and omissions

**NURSING HOME WANDERER**
Nursing home doors should automatically lock when an Alzheimer’s patient wanders. However, a wearable wandering detection device fails to alert the door locking system, allowing the vulnerable patient to wander from the facility, exposing her to dangerous freezing weather conditions. The nursing home purchased the devices and suffered reputational harm following media coverage of the event, leading to an alleged reduction in census and revenue.

**E-COMMERCE SITE SHUTDOWN**
A smart watch user connects to a company network. The smart watch is infected with malware, due to vulnerability in the device software. The malware infects the corporation’s network, executing a DDOS attack, shutting down the company’s e-commerce system for two days.

**HEALTHCARE PROVIDER LOSES PATIENTS**
A smart contact lens used to continuously monitor vital signs transmits patient data to a healthcare provider. A cyber criminal exploits vulnerability in the lens data transmission, triggering system security protocols, resulting in a shutdown of the healthcare provider’s information systems. During the downtime, the healthcare provider is unable to see patients, resulting in lost appointments and new patients.

**VIRTUAL REALITY DEVICE SOFTWARE FAILURE**
A trucking company contracts with a training company that uses wearable virtual reality devices to train long haul truckers for their Commercial Driver’s License (CDL) certification. A glitch in the device software prevents completion of the CDL program, resulting in the trucking company not having an adequate number of drivers. The trucking company fails to complete shipping contracts, losing revenue and customers. Additionally, the training company suffers reputational damage and a loss of business.

**BIOSENSOR FALSE-POSITIVE**
A company’s employee with previous DUI convictions uses a wearable biosensor to enforce the terms of probation. The biosensor gives a false-positive, creating a perceived probation violation. The employee is arrested and put in jail for 48 hours, forcing the employee to miss a key meeting with a large prospective customer to close a seven-figure contract. Due to the employee’s absence, the sale is lost, and the employer sues the device manufacturer.

**APPAREL COMPANY IMPACTED BY CHILD DEATHS**
A company supplies location tracking technology, to be integrated with a line of infant and toddler clothing being launched by a well-regarded and established apparel company. Two highly publicized incidents involve child deaths due to failure of the technology to accurately track child location. The clothing company experiences significant damage to its reputation, sales, and stock price.
**Actions to consider for minimizing risk: Technology errors and omissions**

To minimize exposure to errors and omissions risk, companies should consider the actions described previously for bodily injury risk. This includes robust device hazard analysis, cybersecurity, and clearly documented use instructions.

A company’s contract practices can also impact exposure to this risk category. To help manage exposure, technology companies should evaluate the following customer contract provisions:

- **Limitation of liability.** This provision disclaims liability for certain types of damages – usually incidental, consequential, or special damages. This may be very useful in the event of threatened litigation.

- **Damage caps.** These can be defined in terms of a specific dollar amount or an amount to be determined, based on specific factors defined in the contract.

- **Disclaimer/limitation of warranties.** This provision identifies the warranties provided, disclaims or limits those warranties not provided, and identifies the remedies available in the event the product or work does not comply with the warranties provided.

- **Integration.** This provision identifies the documents that comprise the parties’ contract and will also limit the parties’ reliance on documents and information outside of the contract.

- **Contractual risk transfer and defense/indemnity provisions.** Such provisions can shift risk to other parties.
Device makers face special challenges as they move into the high-risk/high-reward area of wearable technology. Never before have metal sensors been attached to the human body for prolonged time frames, so the liability threat landscape for device manufacturers moving forward is not clear. Safety features, data protection measures, effective contract risk management, and good design decisions can help companies reduce their exposure to some of the risks we see today.

However, given the rapid pace of technological change, companies involved with wearable technology are unlikely to ever fully understand and eliminate their current or emerging exposures. To help manage these exposures, companies should investigate their insurance options for the categories of risk described in this issue of the Technology Risk Advisor series, as indicated in the table on page 22.
### Insurance considerations for wearable technology

<table>
<thead>
<tr>
<th>Risk class</th>
<th>Illustrative risk scenarios</th>
<th>Actions to consider for minimizing risk</th>
<th>Relevant insurance coverage to evaluate with an agent or broker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td>• Cardiac hacking&lt;br&gt;• Signal interception&lt;br&gt;• Privacy invasion&lt;br&gt;• Malware infection&lt;br&gt;• Corporate espionage</td>
<td>• Custom security level&lt;br&gt;• Remote erase feature&lt;br&gt;• Bluetooth encryption&lt;br&gt;• Encrypt critical data elements&lt;br&gt;• Secure the cloud</td>
<td>Information security coverage provides coverage for critical cyber risks. Coverage options vary, but most include network and information security liability, and communications and media liability. Firms can also opt for many first-party expense reimbursement coverages including data restoration, business interruption, computer and funds transfer fraud, crisis management, and security breach notification expenses.</td>
</tr>
<tr>
<td>Bodily injury</td>
<td>• Abrasions&lt;br&gt;• Risky behavior&lt;br&gt;• Adverse reaction from wireless communication&lt;br&gt;• Misinterpreted input&lt;br&gt;• Detection failure&lt;br&gt;• Self-diagnosis and overexertion</td>
<td>• Conduct extensive testing&lt;br&gt;• Conduct robust hazard analysis&lt;br&gt;• Plan for mitigation&lt;br&gt;• Evaluate awareness of and adherence to key standards&lt;br&gt;• Build in cybersecurity&lt;br&gt;• Develop clear safety and use instructions</td>
<td>Product liability coverage provides coverage for loss arising from bodily injury risk. Available options cover consumer fitness tracking devices, as well as doctor-prescribed medical wearables.</td>
</tr>
<tr>
<td>Technology errors and omissions</td>
<td>• Nursing home wanderer&lt;br&gt;• E-commerce site shutdown&lt;br&gt;• Biosensor false-positive&lt;br&gt;• Healthcare provider loses patients&lt;br&gt;• Virtual reality device software failure&lt;br&gt;• Apparel company impacted by child deaths</td>
<td>• Actions mentioned for bodily injury risk&lt;br&gt;• Evaluate customer contract provision options&lt;br&gt;− Limitation of liability&lt;br&gt;− Damage caps&lt;br&gt;− Disclaimer/limitation of warranties&lt;br&gt;− Integration&lt;br&gt;− Contractual risk transfer and defense/indemnity provisions</td>
<td>Errors &amp; Omissions (E&amp;O) liability coverage protects against damages that you must pay because of economic loss resulting from your products or your work and caused by an error, omission, or negligent act.</td>
</tr>
</tbody>
</table>

Wearable devices are used in different contexts, and few policies are standard. Circumstances vary, and all risks may not be insurable. It is important to contact your independent insurance agent or broker to make sure you get the right coverage and services for you and your company.
How Travelers can help

Travelers understands the unique needs of technology firms. We often insure what other carriers won’t, because we’ve been protecting tech companies longer than most. So as device makers work on the next groundbreaking wearable technology, Travelers will be there to help manage their risks with the right insurance products.

Travelers stays ahead of technology industry risk. From the rise of PCs, to the Y2K scare, to the Internet economy, Travelers continues to evolve with effective coverage options to provide technology companies with important insurance coverage for exposures as they continue to innovate. As Chief Underwriting Officer for Travelers Technology, Mike Thoma says, “You come to expect unique exposures when you work with cutting-edge tech companies. And you just figure it out. We’ve been doing that for 30 years.”

Experience and innovation uniquely positioned Travelers to protect technology firms as they take advantage of The Wearables Revolution.

For more information, contact your independent insurance agent who represents Travelers Technology, or visit us on the Web at travelers.com/technology.
Risk expertise for the technology industry

TRAVELERS HAS BEEN INSURING TECHNOLOGY COMPANIES FOR MORE THAN 30 YEARS. HEAR DIRECTLY FROM TRAVELERS TECHNOLOGY INDUSTRY EXPERTS, USING THE LINKS BELOW.

Click on videos to play

MITCH FOSTER II ON TELECOM: http://travl.rs/1cgWzik
KIRSTIN SIMONSON ON INFORMATION TECHNOLOGY: http://travl.rs/1PL9YBL
PATTY NICHOLS ON MEDICAL TECHNOLOGY: http://travl.rs/1FVhMwf

JILL DUFFY ON GLOBAL RISKS: http://travl.rs/1FvhhIL
MIKE THOMA AND RONDA WESCOTT ON INSURING TECHNOLOGY COMPANIES: http://travl.rs/1F8WjZR
RYAN STROUTH AND MIKE DEHETRE ON EMERGING TECHNOLOGY: http://travl.rs/1BnJyKw

KIRSTIN SIMONSON AND CLAIRE KORNEGAY ON CYBER RISKS: http://travl.rs/1J3jASH
MITCH FOSTER II ON ELECTRONICS MANUFACTURING: http://travl.rs/1Fep5cv
EILEEN KAUFFMAN ON CLEAN TECHNOLOGY: http://travl.rs/1LGy5f8
REFERENCES AND SOURCES

“Wearable Technology—Has the Next Enterprise Game-Changer Arrived?”
Frost & Sullivan, 2014, accessed Apr. 2015,

“The Wearable Health Revolution,”
Soreon Research, Oct. 2014, accessed Apr. 2015,

Bloomfield, Ricky, “The Why of Wearables,”
The Mobile Doc, Mar. 2015, accessed Apr. 2015,

Kuang, Cliff, “Disney’s $1 Billion Bet on a Magical Wristband,”
Wired, Mar. 2015, accessed Apr. 2015,
http://www.wired.com/2015/03/disney-magicband/

“Health Wearables, Early Days,”
PricewaterhouseCoopers, 2014, accessed Apr. 2015,

“IBM Watson Group Invests in Pathway Genomics to Help Personalize Consumer Health,”
IBM Corporation, Nov. 2014, accessed Apr. 2015,

Safelet, accessed June 2015,
http://www.safelet.com

Armending, Taylor, “Millennials Becoming Known as Generation Leaky,”
CIO, Feb. 2015, accessed Apr. 2015,

“Multiple Chronic Conditions Chartbook,”

Medtronic, accessed June 2015,
http://www.medtronicdiabetes.com/treatment-and-products/continuous-glucose-monitoring

Ouyang, Ben, “ZIO Wireless Patch May Be Better Option Than Holter Monitors for Cardiac Arrhythmia Diagnosis,”
Jan. 2014, accessed June 2015,

CONTINUED ON NEXT PAGE


Travelers understands the unique needs of technology firms. We often insure what other carriers won’t, because we’ve been protecting tech companies longer than most. So as device makers work on the next groundbreaking wearable technology, Travelers will be there to help manage their risks with the right insurance products.