TRAVELERS

Harnessing the wearable technology revolution

Technology thought leadership

Contents

Potential vs risks

Wearable technology devices represent an exciting and lucrative opportunity, 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. Perhaps some of the biggest quality of life improvements will come in the medical and healthcare space, where wearable technology holds the possibility of detection, prevention and treatment of chronic disease.

Along with the tremendous upside potential, there are risks involved that must be managed. Those who understand these risks will be better positioned to protect themselves from liability, should devices go awry.

This report will expose some of those risks and highlight the actions that UK wearables manufacturers should consider going forward.

The 'risk scenarios' described in this document are intended to facilitate the consideration and evaluation of risks and are not necessarily based on actual events. Also, the insurance products sold by Travelers or other insurers 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 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 broker to evaluate what risk management products or services are right for them.

Mark Crane
Technology Practice Leader
Travelers
mcrane2@travelers.com
+44 (0)20 3207 6232

Executive summary

The wearable technology revolution promises to make us more connected and change our lives for the better.

Fitness trackers can give us new insights to improve our health, exercise and diet. Smart watches keep us organised and better informed. Wearable virtual reality and holographic devices could take us to new worlds with the press of a button. Many of the largest and most innovative technology companies are aggressively pursuing wearable technology opportunities, as are many emerging start-ups.

Along with opportunities, wearable technology also brings new risks.
Broadly speaking, wearable technology creates risks for three types of company:

a. **Technology companies directly involved in the development, manufacture 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.

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

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

c. **Other companies not traditionally considered to be technology firms that are integrating wearable technology into their products.**

   For example, as textile companies integrate electronic monitors into clothing they could be exposed to bodily injury risks they had not previously considered.

In this report, we look at the upsides and downsides 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 highlight for consideration several specific actions to minimise business risks.

Finally, we highlight insurance considerations that firms should evaluate with their insurance broker as they pursue lucrative wearable opportunities.

"Near Field Communication chips enable customers to make credit card payments directly from wearable technology devices"

Market size and drivers

Wearable technology and the Internet of Things are poised to redefine mobility in the coming years.

Recent research from Mintel estimated that more than three million wearable devices designed to be worn on the wrist were sold in the UK in – up a staggering 118 per cent from 2014. Sixty-three per cent of wrist-worn devices sold were fitness bands significantly outselling smart watches.[i]

Several global market forces are driving this rapid wearable technology adoption rate, all of which have the potential to change how we live and work. Companies that recognise and understand these drivers position themselves to capitalise 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 report 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 the next iteration of this trend. When asked about the design of Apple's smart watch, Chief Design Officer Jonathan Ive said: "It's technology worn on the wrist. I sensed there was an inevitability to it."

Driver 2: Office productivity applications
In the corporate sector, wearable devices deliver innovation leading to productivity gains and cost savings. For example, 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.

Employees won't be the only ones wearing these devices. Companies are now developing mobile devices with Near Field Communication chips that enable customers to make credit card payments directly from wearable devices. Marketed as a combination of function and fashion these wearables are the next step towards contactless payment systems. Disney has invested US$1 billion in the magic wristband, a wearable device for customers to use in its theme parks.

"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."

Market size and drivers
continued

Driver 3: Medical and health applications
It is expected that substantial investment in wearable technology devices will come from the medical and health sector The weight loss and longevity markets have been extremely profitable in recent years a trend that is likely to continue.

In a 2014 US PwC survey, 56 per cent of respondents felt that wearable health devices could extend their life expectancy by 10 years. Forty-six per cent see these devices as a way to help control obesity and 42 per cent expect health wearable technology 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 other hospital staff in the event of an emergency.

Driver 4: Safety and security applications
Employee safety has become a major concern in the workplace. Employees operating forklift trucks or heavy industrial equipment are often required to use both hands to do so. As part of their job they may also need to shift their focus to enter job-specific data into a PC terminal. Wearable technology devices can make these tasks safer by automatically capturing and/or recording data without requiring the employees to break concentration as well as keeping both hands free at all times.

Wearable technology can also keep individuals safer outside the workplace Some device makers are marketing safety devices disguised as jewellery. For example, the Safelet looks like a bracelet but it's actually a smart transmitter that can notify the police or a list of contacts of the user's exact location in the event of an emergency.

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 becoming early adopters of wearable technology.

"As hospital stays become shorter many doctors are sending patients home with wearable health sensors."

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

"Millennials are well suited to becoming early adopters of wearable technology."

Key categories of wearable technology

The following wearable technology device categories are among those with the greatest market potential.

Category A: Smart glasses and headgear
Devices such as Google Glass present the user with a miniature display, similar to a computer monitor. On-board cameras and tilt sensors allow the device to capture the user's field of vision and even save 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 bring business benefits, others are aimed directly at the 'infotainment' market. For example, Oculus VR's virtual reality headset, Oculus Rift, offers a premium gaming experience. 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.

Regardless of their size or intended purpose, all wearable devices have three technologies in common that make them 'smart':

Sensors that capture impulses from the user's body or surroundings, which they translate into actionable data.

Microprocessors that extract, transform and load the data into a transmittable format.

Transmitters that wirelessly send the data to cloud storage for further processing and reporting.

Category B: Smart watches
In addition to telling the time, most smart watches offer the same standard apps found on smartphones such as email, instant messaging, calendar and GPS apps. However, third-party developers are creating a catalogue of apps enhanced specifically for smart watches to increase their value for both work and home life. OfficeTime for the Apple Watch, for instance, allows users to track the time they spend in meetings and display a detailed breakdown of their time usage for the week. Another device – British Gas's Hive – allows homeowners to control heating, lighting and other electrical devices from anywhere using their phones and tablets.

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 more easily than any smartphone. In their current form, smart watches can do very little unless they are paired with a smartphone. However, app developers have hinted that this requirement will be eliminated in future versions.

Category C: Fitness trackers
Positioned firmly in the health market, fitness trackers appeal to users' desire for self-improvement. Wearable fitness trackers like the Fitbit, Nike FuelBand and Microsoft Band can detect the user's activity throughout the course of a day, rather than just during traditional exercise. By tracking and reviewing their fitness activities over time, users can make lifestyle changes to improve their health and lifestyle.

Most fitness device manufacturers offer a range of progressively powerful models, each at higher price points. The most basic models track steps taken, calories burned and sleep quality. More advanced versions can track heart rate and blood pressure and offer coaching for workouts.

"Near Field Communication chips enable customers to make credit card payments directly from wearable technology devices"

"Positioned firmly in the health market, fitness trackers appeal to users' desire for self-improvement."

Key categories of wearable technology
continued

Category D: Wearable medical devices
For diabetics, the Medtronic Continuous Glucose Monitoring system, which was approved for use on the NHS in early 2016, 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 analysis. It even decreases finger prick test requirements to two per day. An optional insulin pump delivers insulin as needed, without patient intervention.[ii]

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 Holter monitor. For more severe cardiac cases, the ZOLL LifeVest Wearable Defibrillator can detect life-threatening abnormal heart rhythms and deliver a shock to restore a healthy cardiac rhythm.

Transcutaneous electrical nerve stimulation devices help patients who suffer from chronic pain, and they are also used by some women in labour. They hook to a patient's belt and deliver a continuous low-voltage electrical current to the affected area.

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

Category E: Smart clothing and accessories
Just as wearable technology is the next iteration of mobile devices, smart garments stand to become the next iteration of wearable fitness trackers.

Added to that, 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 smart babygros that contain movement sensors, temperature sensors and even elecrtocardiography (ECG) capabilities to help parents monitor their babies.

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 then 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.

"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."

Three risk classes wearable technology companies should understand

The market potential for wearable technology devices is undeniable. But as great as the opportunities are, the liability risks cannot be ignored.

Should a device fail, a business could lose millions of pounds, a consumer's privacy could be compromised, or a patient could lose their health or even their life.

Therefore, technology companies should closely consider three major risk categories posed by wearable technology devices, so that they can decrease their exposure to costly liability claims:

- **Class 1: Cyber**
- **Class 2: Bodily injury**
- **Class 3: Technology professional indemnity**

Class 1: Cyber

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 security software, a disgruntled employee. It can also include increased liability to third-parties via claims for distress.

Illustrative risk scenarios

Cardiac hacking
A cardiac patient's wearable heart monitor automatically uploads a block of health data to the cloud. 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.

Corporate espionage
An executive enters his building wearing a wireless identity authenticator. Unbeknown 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 of the permissions the executive enjoys including access to intellectual property which he then sells to competitors.

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 information and account numbers. A thief intercepts the Bluetooth feed from the smart glasses en route to a cloud data store, stealing customers' 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 her asthma. The device frequently transmits data to her mobile phone and her doctor. She boards a bus where she sits next to a cyber-enthusiast with a Bluetooth sniffer. He intercepts the signal and sells the data.

Malware infection
A user with a smart watch connects to her phone to pay bills. However, the user has previously 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
Wearable technology device manufacturers shoulder the burden of proof to demonstrate that the data detected by their wearable technology device was properly safeguarded. That means that devices should be engineered with data security in mind.

However, tech firms may ship their devices with default settings that promote ease-of-use, which are also often the least secure. Companies can often protect themselves by designing some simple yet effective security features into their devices.

Tech firms should consider the following steps to help minimise their exposure to cyber risk:

- **Offer custom security levels** – 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 vulnerabilityfor hackers to exploit.
- **Offer a remote erase feature** – enable wearable users to remotely erase and/or disable their device if it is lost or stolen. Apple does this with the iPhone and other wearables manufacturers should consider following suit.
- **Use Bluetooth encryption** – Bluetooth offers an encryption application programming interface when exchanging data between a device and its target data store, but few companies take advantage of it because it decreases battery life. More companies should consider making use of this feature.
- **Encrypt critical data elements** – the most critical pieces of data transferred between wearable devices and data stores are user IDs, passwords and PIN numbers.
- **Secure the cloud** – data is often transmitted from a wearable device to a smartphone and then to a cloud data store. Virtualised clouds can secure data with multiple diverse operating systems, each operating within a different security context. Banks often secure payment details for people making deposits this way, and wearable technology companies should consider similar functionality.

"The most critical pieces of data transferred between wearable devices and data stores are user IDs, passwords and PIN numbers."

Class 2: Bodily injury

In order for wearable technology devices to deliver on the quality of life benefits they bring, 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.

Therefore, wearable manufacturers should understand and mitigate the risk of a product liability claim.

Illustrative risk scenarios
Abrasions
A company develops a smart contact lens with an embedded chip to monitor glucose levels in diabetics' tears.

The device analyses 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 that cause abrasions to users' eyes.

Misinterpreted input
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.

Risky behaviour
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.

Detection failure
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 makes a claim against the manufacturer.

Adverse reaction from wireless communication

Smart fitness garments transmit data from sensors to a computing device via short-range radio waves. Prolonged exposure to specialised materials in the sensors leads to an allergic reaction and an allegation of skin and muscle damage by a user.

Self-diagnosis and overexertion
A fitness tracker device broadly categorises 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.

"Companies should be aware of hazards that can be introduced during processes such as manufacturing, packaging, labelling, storage or transport."

Actions to minimise risk
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. Direct and reputational costs from product liability events can cripple wearable technology companies, sometimes endangering their very existence. Therefore, it is crucial that companies prepare for all possible outcomes from a user's experience.

Companies should consider the following steps to help mitigate 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 match UK requirements.
- **Conduct robust hazard analysis** – methods of hazard analysis including: fault tree analysis, failure mode and effect analysis, hazard and operability, and critical control point 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 and then identifying potential hazards for each. Hazards can include anything from toxicity and flammability to mechanical and electronic hazards. Companies should be aware of hazards that can be introduced during processes such as manufacturing, packaging, labelling, storage or transport.
- **Plan for mitigation** – companies should assess the frequency and severity of all identified hazards. Companies need to eliminate all high-severity hazards and eliminate or reduce the potential for medium- and low-severity hazards. Companies should also assemble a diverse team to include external deign process personnel to generate mitigation solutions. In addition, they should liaise with the solutions team to consider how specific hazards have been mitigated for analogous industries or device categories.
- **Evaluate awareness of and adherence to key standards** – companies should ensure that all relevant personnel are aware of and adhere to applicable standards. For example, for wearables classified as medical devices, companies should evaluate whether and how they adhere to ISO 14971 and ISO 13485.
- **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.
- **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 hazards. Incorporate information on proper device storage and transportation, as well as instructions on what to do if the device malfunctions.

"A lack of cybersecurity in wearable technology creates the potential for bodily injury."

Class 3: Technology professional indemnity

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.

Companies that understand the unique nature of this risk category can better protect themselves from liability claims.

Illustrative risk scenarios

Nursing home patient
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 outside in unfavourable weather conditions. The nursing home suffers reputational harm following media coverage of the event, leading to a reduction in patient numbers and revenue.

Private 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 a vulnerability in the data transmission, triggering system security protocols and resulting in a shutdown of the healthcare provider's information systems. During the shutdown, the healthcare provider is unable to treat patients, resulting in lost revenue.

E-commerce site shutdown
A smart watch user connects to a company network. The smart watch is infected with malware, due to a vulnerability in the device's software. The malware infects the corporation's network, executing a Distributed Denial of Service (DDOS) attack and shutting down the company's e-commerce system.

Virtual reality device software failure
A haulage company employs a training company that uses wearable virtual reality devices to train truck drivers for their commercial driving license qualification. A glitch in the device's software prevents completion of the program, resulting in the trucking company not having an adequate number of qualified drivers. The company fails to fulfil several contracts, losing revenue and customers. Additionally, the training company suffers reputational damage and loss of business.

Biosensor false positive
A person with a drink-driving conviction uses a wearable biosensor to enforce the terms of their probation. The biosensor gives a false positive, creating a perceived violation of their probation.

Clothing company impacted by child deaths
A company supplies location tracking technology that is integrated in a line of baby and toddler clothing. Two highly publicised incidents involve child deaths due to failure of the technology to accurately track their location. The clothing company experiences significant damage to its reputation.

"A lack of cybersecurity in wearable technology creates the potential for bodily injury."

Three risk classes wearable technology companies should understand continued

Actions to mitigate risk
o minimise exposure to professional indemnity risk, companies should consider the actions described previously for bodily injury risk.

A company's contract practices can also reduce their exposure to this risk category. Therefore, technology companies should consider using the following customer contract provisions:

- **Limitation of liability for damages** – this provision disclaims liability for certain types of damages – usually indirect or consequential damages.
- **Damage caps** – these can be defined in terms of a specific sum or an amount to be determined, based on specific factors defined in the contract.
- **Limitation of liability for warranties** – to the extent permitted by statute this provision identifies the warranties provided, disclaims or limits those warranties not provided, and identifies the remedies available in the event that the product or work does not comply with the warranties provided.
- **Entire Agreement** – this provision identifies the documents that comprise the parties' contract and also limits the parties' reliance on documents and information outside the contract.
- **Contractual risk transfer and defence/ indemnity provisions** – such provisions can shift risk to other parties.

These types of clauses are examples of how tech companies might control their exposure but the law on this area is complex and independent legal advice should be sought to ensure enforceability and compliance with statutory duties.

"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."

The last line of defense

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 timeframes, 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 all help companies to reduce their exposures 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.

Therefore, to help manage these exposures, companies should investigate their insurance options for the categories of risk described in this report.

"Never before have metal sensors been attached to the human body for prolonged timeframes, so the liability threat landscape for device manufacturers moving forward is not clear."

Risk class	Illustrative risk scenarios	Actions to consider for minimising risk	Relevant insurance coverage to evaluate with an agent or broker
Cyber	• Cardiac hacking • Signal interception • Privacy invasion • Malware infection • Corporate espionage	• Custom security level • Remote erase feature • Bluetooth encryption • Encrypt critical data elements • Secure the cloud	**Information security coverage** provides coverage for critical cyber risks. Coverage options vary, but most include network and information security liability, and communication 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.
Bodily injury	• Abrasions • Risky behaviour • Adverse reaction from • wireless communication • Misinterpreted input • Detection failure • Self-diagnosis and overexertion	• Conduct extensive testing • Conduct robust hazard analysis • Plan for mitigation • Evaluate awareness of and adherence to key standards • Build in cybersecurity • Develop clear safety and use instructions	**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.

Technology errors and omissions	• Nursing home patient
	• E-commerce site shutdown
	• Biosensor false-positive
	• Healthcare provider loses patients
	• Virtual reality device software failure
	• Apparel company impacted by child deaths
		• Actions mentioned for bodily injury risk
		• Evaluate customer contract provision options
		  • Limitation of liability
		  • Damage caps
		  • Disclaimer/limitation of warranties
		  • Integration
		  • Contractual risk transfer and defence/ indemnity provisions
			Technology Professional Indemnity coverage protects against damages that you must pay because of economic loss resulting from your products or your work.

How Travelers can help

Travelers understands the unique needs of technology firms.

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

We also stay ahead of technology industry risk. From the Y2K scare to the internet economy, we continue to evolve and provide effective coverage for the latest risks that technology companies face.

As Mark Crane, Technology Practice Leader at Travelers, says:

For more information, contact your insurance broker or visit **travelers.co.uk/technology**

"You come to expect unique exposures when you work with cutting edge tech companies. We've been doing that for 30 years and are adept at understanding the latest risks – and coming up with creative solutions to cover them."

Sources and further reading

Brits step up to wearable technology: sales of fitness bands and smartwatches up 118% in 2015, Mintel, January 2016
http://www.mintel.com/press-centre/technology-press-centre/brits-step-up-to-wearable-technology-salesof-fitness-bands-and-smartwatches-up- 118-in-2015

Monitor implant approved for UK diabetics, Financial Times, February 2016
http://www.ft.com/cms/s/0/af8251b0-d186-11e5-92a1-c5e23ef99c77.html#axzz4GvaM4DWI

2015 Information security breaches survey, government and PwC
https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-reportblue-03.pdf

Wearable Technology—Has the Next Enterprise Game-Changer Arrived?, Frost & Sullivan, 2014
http://ww2.frost.com/news/press-releases/frost-sullivanwearable-technology-has-next-enterprise-game-changer-arrived/

The Wearable Health Revolution, Soreon Research, 2014
http://www.soreonresearch.com/wp-content/uploads/2014/09/Extract-Soreon-Research-Report-The-Wearable-Health-Revolution.pdf

Bloomfield, Ricky, The Why of Wearables, The Mobile Doc, 2015
http://www.rickybloomfield.com/2015/03/the-why-of-wearables.html

Disney's $1 Billion Bet on a Magical Wristband, Cliff Kuang, Wired, 2015
http://www.wired.com/2015/03/disney-magicband/

Health Wearables, Early Days, Pricewaterhouse-Coopers, 2014
http://www.pwc.com/us/en/health-industries/top-health-industryissues/assets/pwc-hri-wearable-devices.pdf

IBM Watson Group Invests in Pathway Genomics to Help Personalise Consumer Health, IBM Corporation, 2014
https://www-03.ibm.com/press/us/en/pressrelease/45376.wss

Safelet
http://www.safelet.com/?cr_exp=s&cr_cid=140818492

Millennials Becoming Known as Generation Leaky, Taylor Armerding, CIO, 2015
http://www.cio.com/article/2885143/security0/millennialsbecoming-known-as-generation-leaky.html

Multiple Chronic Conditions Chartbook, Agency for Healthcare Research and Quality, US Department of Health and Human Services, 2014
http://www.ahrq.gov/sites/default/files/wysiwyg/professionals/prevention-chronic-care/decision/mcc/mccchartbook.pdf

Medtronic
http://www.medtronicdiabetes.com/treatments/continuousglucose-monitoring

ZIO Wireless Patch May Be Better Option Than Holter Monitors for Cardiac Arrhythmia Diagnosis, Ben Ouyang, 2014
http://www.medgadget.com/2014/01/zio-wireless-patch-maybe-better-option-than-holter-monitors-for-cardiac-arrhythmiadiagnosis.html

Zoll, 2015
http://lifevest.zoll.com/patients

Web MD, 2015
http://www.webmd.com/back-pain/guide/tens-for-back-pain

Wearable Tech Invented by 15-Year-Old Tracks Alzheimer's Patients, Michael Guta, 2014
http://www.wearabletechworld.com/topics/wearable-tech/articles/386798-wearable-tech-invented-15-year-old-tracksalzheimers.htm

Sources and further reading
continued

Forget Smart Watches and Glasses. Smart Clothing Will Be the Hottest Trend of 2015, Andy Boxall, Digital Trends, 2014
http://www.digitaltrends.com/wearables/smart-clothing-garmentsat-ces-2015-and-beyond/

2014 Global Report on the Cost of Cyber Crime, Ponemon Institute, 2014
https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5207enw.pdf

Do Wearable Devices Spill Secrets?, Matthew J. Schwartz, Bank Info Security, 2014
http://www.bankinfosecurity.com/do-wearable-devices-spillsecrets-a-7446/op-1

Risk Assessment for Medical Devices, Linda Braddon, Secure BioMed Evaluations
http://www.securebme.com/pdf/braddon_sbme_risk_assessment_presentation.pdf

Basic Principles of Risk Management for Medical Device Design, Ganeshkumar Palanichamy Wipro Technologies
http://www.wipro.com/documents/resource-center/library/Whitepaper_Medical_Devices_Basic_Principles_of_Risk_Management_for_Medical_ Device_Design.pdf

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. Guidance for Industry Food and Drug Administration Staff, FDA Center for Biologics Evaluation and Research, 2014
http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf

i http://www.mintel.com/press-centre/technology-press-centre/brits-step-up-to-wearable-technology-sales-of-fitness-bandsand-smartwatches-up-118-in-2015

ii http://www.ft.com/cms/s/0/af8251b0-d186-11e5-92a1-c5e23ef99c77.html#axzz46Nblc8nU

iii https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-reportblue-03.pdf

About Travelers

Here is a comprehensive list of the covers we provide and the types of business we provide them for.

Products

Business Interruption

Crime

Criminal Protection Response

Cyber (1st & 3rd party)

Directors & Officers

Employers' Liability

Employment Practices Liability

Event Cancellation

Kidnap & Ransom

Personal Accident & Travel

Professional Indemnity

Property

Products Liability

Public Liability

Terrorism

Industries

Advanced manufacturing

Automotive

Educational services

Financial institutions

Healthcare

Hotels

Legal

Marine

Media and entertainment

Professions

Public services

Retail

Transport

Real estate

Technology

Warehousing and distribution

TRAVELERS