TRAVELERS

GLOBAL TECHNOLOGY'S RISK ADVISOR SERIES

# The IoT expressway of innovation

With transportation-related applications, the Internet of Things (IoT) presents technology companies with both opportunity and risk.

# Driving innovation to new destinations



Even before the first Model T rolled off Henry Ford's assembly line back in 1927, we have been looking for ways to get people and products to their destinations quickly and efficiently. Transportation technology has reinvented itself many times since then. Today, the Internet of Things (IoT) is bringing innovations to the transportation industry in ways few could have envisioned in the last century.

Powerful micro-sensors in moving vehicles generate gigabytes of operational data over the internet for later analysis by data scientists. Software-controlled self-driving cars are becoming a reality, with Google and other autonomous vehicle developers logging nearly 2 million test miles. Transportation companies are using IoT-captured big data to increase safety and decrease costs. Rail companies send trip data to powerful back-end algorithms to optimize trip efficiency. Most new vehicles come with internet-ready navigation systems to get us to our destinations using the quickest route available while avoiding detected traffic congestion.

Transportation innovations like these represent a prime opportunity for technology companies that are developing IoT transportation technologies including wireless networking, near-field communication (NFC) and real-time positioning systems. The IoT is making transportation safer, less costly and more convenient for everyone.

While the market for transportation technology offers unprecedented opportunity, companies developing and manufacturing transportation IoT should also consider the risks related to this emerging technology. As they transmit large amounts of data, many devices used for transportation applications pose unique cybersecurity risks. Additionally, IoT device reliability poses significant risks, as these new technologies may function in ways that challenge existing safety and security standards.

Technology executives who closely consider these risks will be better positioned to protect their companies and IoT market opportunity.

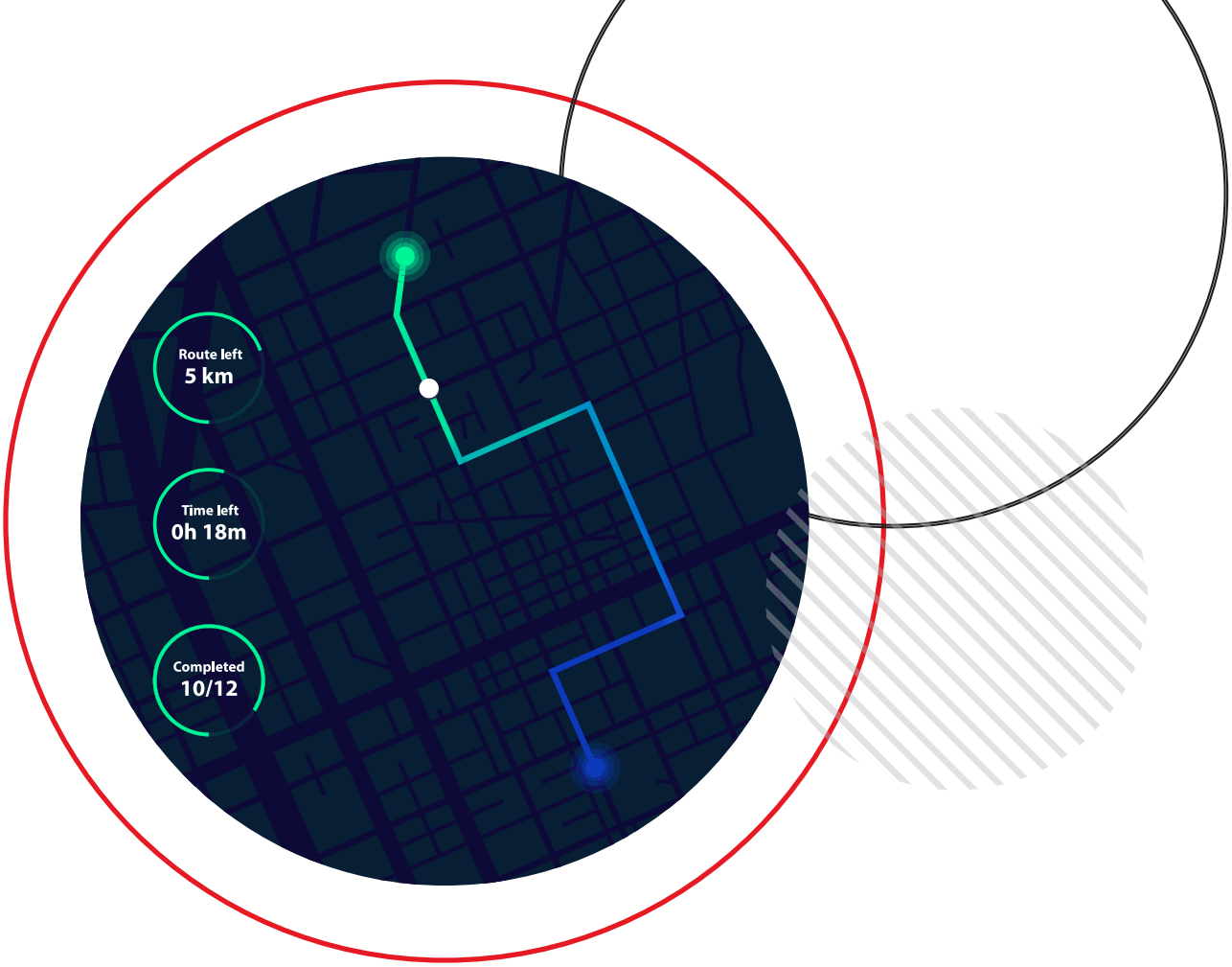
**Mike Thoma**
CHIEF UNDERWRITING OFFICER, TRAVELERS GLOBAL TECHNOLOGY

# The IoT is tailor-made for transportation

There is a good reason the IoT appears tailor-made for the transportation sector. In 1999, industry thought leader Kevin Ashton, one of the pioneers of radio frequency identification (RFID) in the transportation industry, coined the term “Internet of Things” (IoT) for a major Proctor & Gamble presentation. During the presentation, he unveiled his notion of enabling P&G’s supply chain for internet connectivity. He may not have realized it at the time, but his idea turned out to be a watershed moment in technology history.

Ashton envisioned a global network of typically offline objects armed with smart sensors connected to cloud data sources. Real-time visibility at each and every point throughout the supply chain would help eliminate waste and increase customer satisfaction. Since then, Ashton and his team of MIT researchers have built this vision into the global force that many Silicon Valley analysts are calling the internet’s third wave. Tens of billions of interconnected devices now give transportation companies new levels of predictability and control. In Ashton’s words, “As you combine information from multiple sources and they are synchronized on the same timeline, you’ll start to see machines making smarter and smarter decisions, anticipating things to a high degree.”

Growth projections of the IoT show great promise. Consulting firm PWC expects business connected-device investment to grow from $215 billion to $832 billion by 2020, contrasted with consumer IoT spending of only $236 billion by 2020. Research firm MarketsandMarkets expects the IoT transportation sector to reach $143.93 billion with a CAGR of 8.95 percent by the year 2020. Clearly, this emerging technology represents a wave of momentum, creating an enormous opportunity for device makers and software developers in the transportation sector.




For example, commercial truck manufacturers now offer optional tracking devices that use wireless machine-to-machine (M2M) communication so carriers can keep track of their rolling stock anywhere on the road. Smart sensors at warehouse loading docks now record arrivals and relay important data points to central dispatchers. Even the packages our goods come in are getting smarter. Intelligent boxes now use smart wireless transmitters that allow shippers and carriers to pinpoint their locations anywhere in the supply line.

Technology companies that produce these exciting new innovations must also be ready for the risks. There can be hidden or unseen ways in which IoT firms can be held liable if devices or software fail to function as intended. That's why it is so important for device makers, software developers and value-added service providers to understand the risks involved and take action to mitigate them.

In this issue of the Travelers Global Technology Risk Advisor, we first consider key factors driving adoption of IoT for transportation applications. We identify and explore specific relevant risk categories. Then, we highlight actions for technology companies to consider for minimizing their risks, and we outline insurance considerations that firms should discuss with their independent agent or broker as they continue to revolutionize the transportation industry with IoT.

# Why now for IoT in transportation?

A few key factors help explain the increasing prevalence of IoT in transportation-related areas. Technology companies that understand these dynamics may be better positioned to both capitalize on the market opportunity and protect themselves from risks.

## A) TECHNOLOGICAL ADVANCEMENTS

Enabling a wider range of device functionality, technological advancements facilitate the adoption of IoT for transportation applications:

- **Ubiquitous internet availability:** Improvements in high-availability internet mean that more IoT devices can transmit data in more physical locations. The pervasiveness of cellular, satellite and Wi-Fi internet connectivity has given transportation IoT devices exactly what they need: extreme mobility.
- **Miniaturization and compounding computer power:** 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.
- **Materials engineering advances:** Progress in developing new advanced materials has facilitated advancements in sensors, actuators, casings and other components used in IoT technology. In many cases, this allows devices to maintain high performance in the wide range of environmental conditions they encounter in many transportation applications.

## B) CONVENIENCE

Opportunities abound for IoT to improve convenience in transportation. In airports, for example, IoT sensors help airlines shift staff where it is needed, helping to reduce passenger wait times. Few things are more frustrating or inconvenient than lost luggage, and smart baggage technology promises to keep passengers informed of their checked bags' location at all times.

In automobiles, Verizon's Hum device, which connects to factory-installed sensors, offers drivers a number of convenience features. Sensors under the hood keep an eye on engine performance. Any issues requiring attention are forwarded to a storage cloud where both the owner and local dealer can see required maintenance and repair issues. The system also lets motorists set speed and boundary alerts, decode engine lights, and summon roadside assistance, via a Bluetooth transmitter that clips to a car's visor.

# C) ECONOMICS

IoT has the potential to significantly reduce the costs associated with many modes of transportation. The McKinsey Global Institute estimates that IoT systems in vehicles might yield $210-$740 billion in value globally by 2025. Their data includes:

- Reductions in property damage from using IoT vehicle-to-vehicle (V2V) communications using dedicated short-range communications systems that will let cars talk to each other.
- Reductions in auto theft due to IoT tracking.
- Reductions in maintenance costs for aircraft and other vehicles, enabled by remote performance monitoring.

Public entity transportation departments also see an economic rationale for IoT, as the devices facilitate fee collection and dynamic pricing. Some "smart cities" have begun installing data, video and audio sensors to keep their transportation grids running smoothly. High-occupancy toll (HOT) lanes on highways offer commuters a way to get to and from work for an extra fee generated from a wireless fob on their dashboard. Cities calculate and publish route prices to their web-connected highway signs based on sensor-detected traffic volumes. Smart parking meters also feature dynamic pricing based on supply and demand for parking at any given hour. As a result, cities can charge premium parking rates at high demand times.

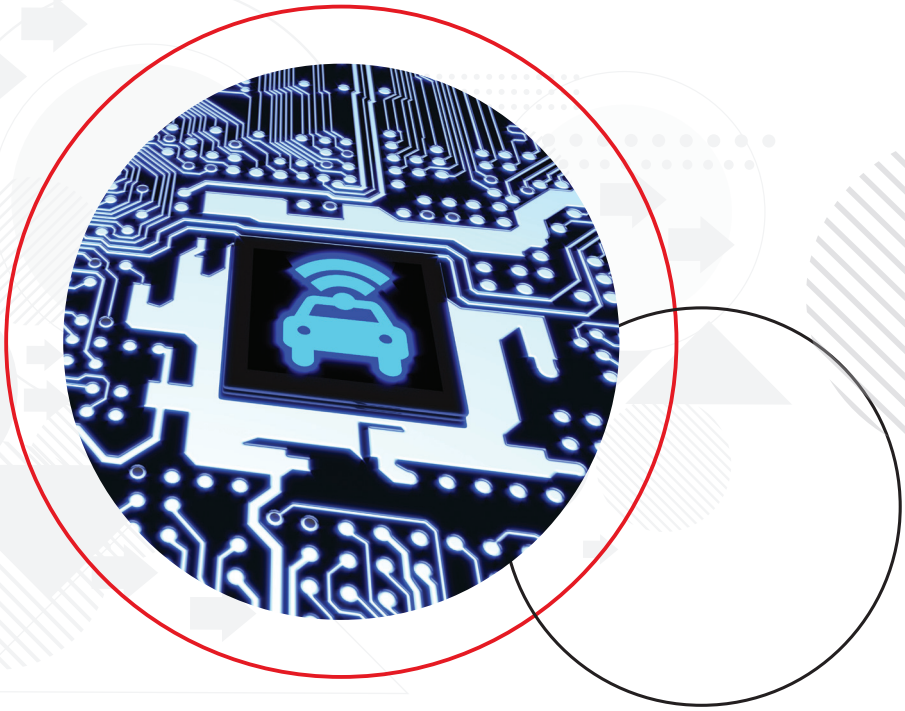
# D) SAFETY

In 2015, 38,400 people were killed, and 4.4 million were injured in auto accidents in the U.S. Manufacturers, regulators and drivers are all looking for IoT tools to reduce these figures. Using IoT to improve fleet safety is one such opportunity.

Telematics firm GeoTab helps trucking companies significantly reduce accidents. A device plugs directly into a truck and sends second-by-second data about the trip to a centralized cloud server. Fleet managers can monitor the health of the vehicle and every action taken by the driver. "Data collection is the first step," says Neil Cawse, GeoTab's CEO. "With telematics, you can know an infinite number of things about the vehicle and what the driver is doing."

IBM also offers IoT devices to track driver behavior from vehicle probe and contextual data. Captured data is sent to a back-end Hadoop® instance, allowing analysts to carve and mine big data very efficiently. Data points such as harsh braking, frequent braking, turn angle and speed range per road type can be monitored, allowing managers to configure individual thresholds for each driver.

Road builders are now building roads and bridges with sensors embedded within the concrete. Wireless signals monitor the structural integrity of the highway under dynamic conditions to alert authorities of safety issues before they turn into catastrophes. These miniature devices can measure temperature, traffic volume, humidity, and ambient weather and traffic conditions. Cities are using this information to improve road conditions and schedule repairs.



# 4 key applications of IoT in transportation

Whether by air, rail, road or sea, technology companies are aggressively developing IoT solutions to improve how the world moves people and transports goods, with the goals of greater efficiency and affordability.

## 1 TRANSPORTATION BY AIR

Airlines leverage IoT components to run smarter, safer, and more intelligently. For example, IoT devices can help them improve day-to-day aircraft operations and maintenance. Manufacturers are equipping new engines with more than 5,000 sensors to capture performance statistics and send them over the web to remote data centers for business intelligence operations. The Boeing 787 Dreamliner is packed with so many built-in sensors and data processing capabilities that it is practically a flying data center. Rolls-Royce is using cloud-based IoT services to analyze plane engine data that cuts fuel costs by $250,000 per plane per year.

In the air, smart sensors capture aircraft telemetry and forward it to centralized cloud storage, where powerful stored procedures extract actionable insights from flight data. GPS systems work with historical flight information to calculate flight paths which optimize fuel consumption and reduce passenger wait times. Some airlines have installed IoT sensors in their seats that can detect a passenger's level of fatigue or dehydration, then notify flight attendants to help make them more comfortable.

On the ground, modern airports are beginning to use IoT devices to speed passengers on the way to their destinations and give them a more pleasant trip. Sensors can detect how many passengers are in line at the gate check-in desk. If the number exceeds a pre-configured threshold, they alert the airline to summon additional staff to the gate to facilitate passenger processing for an on-time departure. Luggage for savvy travelers now comes equipped with built-in Bluetooth capability, GPS technology and location tracking.

## 2 TRANSPORTATION BY RAIL

Like the airline industry, railroads have outfitted their locomotives and rail cars with sensors on critical components such as brakes, wheels and engines. Central railroad control centers can monitor train telemetry indicators like speed, weight and throttle position in real time over wireless broadband. Any detected safety threat is relayed immediately to locomotive engineers and railroad offices, allowing them to take immediate action.

Tracks also have thousands of sensors deployed across their routes, measuring track stress and condition, air and track temperature, and other variables that offer predictive value to maintenance teams. One of IBM's larger rail clients operates a solution that uses Watson's video analysis capabilities to pinpoint track issues. The cloud-based detailed display helps maintenance crews focus on effective repairs, resulting in a safer and more reliable experience for riders.

The Taiwan High Speed Rail Corporation uses a sophisticated railway maintenance system that detects problems throughout the line via connected sensors which capture telemetry of over 320,000 distinct assets, including trains and tracks. The system has proven tremendously successful; 99.15 percent of all trains depart and arrive within six seconds of scheduled times, resulting in increased customer satisfaction and growing ridership.

## 3 TRANSPORTATION BY GROUND

The connected automobile is perhaps the most visible manifestation of the IoT on American highways. Drivers like to be connected on the go, and automakers are responding by transforming vehicles into a mobile-connected data center. Gartner predicts that by 2020, more than 250 million vehicles will be connected globally, with the number of installed connectivity units in vehicles worldwide increasing by 67 percent.

New vehicles are rolling off the assembly line equipped with a myriad of IoT sensors to detect everything from fuel mileage to tire pressure to adjacent collision threats. Modern vehicles send all this data to a manufacturer's cloud which produces periodic vehicle health reports for owners and dealers. With seamless links to smartphones, car companies can detect driver preferences like call volume, app usage and music playlists. All of this data helps companies market to their customers more effectively. Many are also collecting captured data to sell to other product and service providers throughout the automotive ecosystem.

Car manufacturers are already pushing the boundaries of the IoT. In 2013, Tesla started pushing wireless software updates to its Model S cars. Because the features are delivered over the web, most Tesla owners do not notice the upgrades. Toyota is designing a car that allows owners to change the exterior and interior appearance as easily as you change the wallpaper display on your laptop.

Google's Self-Driving Car is expected to be commercially available by 2020, and it will completely abandon the need for steering wheels and pedals. The revolutionary vehicle is operated by sensors, cameras and LIDAR technology that can detect objects and automatically steer around them. The car is equipped with artificial intelligence software that processes information, predicts behavior of objects around it, and responds accordingly to pedestrians, cyclists, other vehicles and obstructions. All data is transmitted wirelessly to engineering headquarters for further research, development and operational improvement.

IoT innovations are helping trucking company fleet managers deliver goods more effectively and efficiently. As commercial trucks travel interstate highways, onboard sensors provide data on logistics, operations, maintenance and safety via cloud-based fleet management systems. According to a 2015 DHL and Cisco Internet of Things Trend Report, the IoT in logistics is expected to generate $1.9 trillion in value, part of an overall $8 trillion in IoT value generated globally over the next decade.

# 4 TRANSPORTATION BY SEA

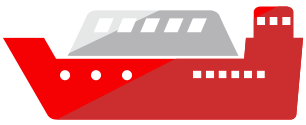
IoT devices are even finding their way onto ships and boats. Maersk Line, the world's largest shipping container firm, has launched a line of 270,000 refrigerated containers, carrying everything from bananas to pharmaceuticals to sashimi-grade tuna. Instead of spending hundreds of millions on physical inspections or paying customer claims for spoiled products, Maersk now uses containers outfitted with a GPS, a modem and a SIM card to enable global tracking via satellite transmitters mounted on Maersk vessels.

Communication between ships is becoming more important in determining the most efficient routes and avoiding collisions. Bastø Fosen's Route Exchange software package lets ship captains provide their route intentions and an estimated time of arrival to other seafarers. Shipboard sensors notify cloud-based controls of a ship's position to share with other ships on the same network, a tremendous improvement over radio-based legacy communication methods.

Large shipping ports have sophisticated utilization systems to manage transport and logistics for numerous stakeholders competing for limited space. By collecting and integrating data from multiple vessels among multiple shipping companies, the Port of Hamburg was able to control traffic, improving turnover of goods and reducing idle time throughout its supply chain. Sophisticated information security systems ensure that any vessel is only allowed to see utilization information relevant to them.

# 4 key risk categories every technology company should understand when developing IoT technology

The IoT is gaining tremendous momentum in the transportation industry. Companies of all sizes are finding benefits that produce real business value. But as the technology continues to advance, so do the inherent risks. Every firm throughout the IoT ecosystem should be aware of the ways they could find themselves liable and take actions to mitigate those risks.



## Category 1: Property damage

**Property damage risk refers to the risk of physical damage to, or loss of use of, tangible property caused by a party who is not the property owner. Such property can include real property as well as personal property. If an IoT device malfunctions, a company that uses the device may sustain property damage due to a defect in the device or its failure to function as intended. Any party involved in the product's manufacturing or distribution chain could find themselves named as a defendant in a property damage claim.**

### ILLUSTRATIVE RISK SCENARIOS FOR PROPERTY DAMAGE

**LACK OF LOCOMOTIVE MAINTENANCE**

A railroad company captures locomotive data from IoT sensors and forwards it to a cloud for later analysis. The data is used to keep track of locomotive conditions and alert maintenance crews when a locomotive needs preventive maintenance. The sensor fails to accurately read the locomotive's performance, understating the stress that the machine has endured, so the vehicle goes without timely maintenance. As a result of the failure, the locomotive engine locks up unexpectedly on a curved track causing a derailment and collisions with nearby buildings. The device maker is sued for the physical damage caused by sending inaccurate information.

**SHIPBOARD SANDBAR SENSOR FAILURE**

A safety sensor aboard ship is designed to alert the captain when his vessel is operating in dangerously shallow waters. As the vessel approaches port, a sensor fails to notify the captain of the sandbar ahead due to a logic disagreement between depth measurements and its programmed mapping. The vessel hits the sandbar at a dangerous speed, damaging both the ship and some of the cargo aboard. An investigation shows that the electronic maps the sensor was using were out of date and should have been automatically updated over the internet, but were not. The software company is found liable for failure to deliver promised electronic updates.

**TANK TRUCK LEAK**

A sensor in a tank truck transporting corrosive material sends alerts over the internet to the driver and the trucking company in the event of a leak. The tank experiences a leak that the sensor fails to detect, leading to the loss of liquid cargo while the truck is parked at the trucking company's garage. The sensor's maker is sued for the physical damage that the leak caused to the garage floor.

# **Category 2:** Bodily injury

**In order for the IoT to deliver the convenience, safety and quality of life benefits it promises, devices and communication mechanisms must function properly at all times. A device developer could be held liable for injuries that occur as a result of a device's failure to function as intended. IoT manufacturers and software companies should understand the bodily injury risks that could render them liable in the event of such a malfunction.**

## ILLUSTRATIVE RISK SCENARIOS FOR BODILY INJURY

### SELF-DRIVING CATASTROPHE

An autonomous vehicle manufacturer has produced a self-driving car as a joint venture with an IoT software development firm. The company conducts a live test of its vehicle on public highways prior to release. However, a bug in the hazard recognition software causes the car to cross the median and crash into oncoming traffic on the other side of the highway. The injured drivers and passengers sue the software developer for resulting medical expenses.

### FOGGY AIRCRAFT COLLISION

An airport uses IoT proximity sensors for planes to communicate with each other while they are taxiing on the ground. On an extremely foggy day, one of the sensors fails to detect an adjacent aircraft, so no warning is sent to the pilots or crews. One aircraft collides violently with another, causing all of the baggage compartments on one side of the plane to spring open and spill their contents on passengers on the right side. The falling baggage causes multiple head injuries to affected passengers. The device maker is sued for the sensor's failure to detect other aircraft on the ground.

### CITY BUS NOTIFICATION FAILURE

A city bus is equipped with sensors programmed to automatically detect a collision and notify first responders without interaction on the part of the driver. The bus collides with pedestrians crossing the street, causing injuries. However, the devices fail to automatically call for help. Because the driver knew that the bus was enabled with sensors, he does not call for medical assistance. By the time emergency crews arrive, one of the pedestrians dies from their injuries. Family members sue the device maker for failure to notify first responders.

# **Category 3:** Financial loss

**A purchaser of IoT technology may sustain economic losses from the failure of the technology to work as intended, due to an error, omission or negligent act in the design of that technology. In such cases, the purchaser may claim lost profits or business disruption. Defense expenses alone in these cases can be catastrophic to a technology business. With each new IoT application, the potential for economic losses increases. Companies that understand the unique nature of this risk category can better protect themselves from liability claims.**

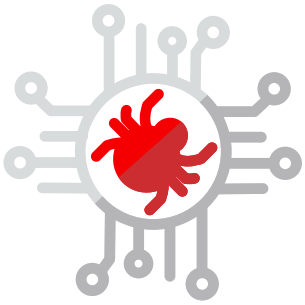
## ILLUSTRATIVE RISK SCENARIOS FOR FINANCIAL LOSS

### GPS PROGRAMMING GLITCH

An automaker stakes its reputation on having higher quality on-board technology than its competitors. A central component of the automaker's feature set is a GPS system from a software firm claiming to deliver the most accurate navigation in the industry. After the automaker sells millions of units, the software firm releases an update with significant bugs that cause vehicles to display incorrect navigation readings. The industry press discovers the problem and publishes articles that portray the automaker as incompetent. The automaker sues the software developer for damaged reputation and millions in lost sales.

**PARKING METER SENSOR FAILURE**

A public entity uses smart parking meters that calculate dynamic parking rates based on supply and demand detected by sensors at strategic locations throughout the city. However, due to a glitch in the software, the sensors understate demand for parking, resulting in lower prices than they should have been charging over a period of six months. The glitch is only discovered when the city hosted a major sports event; nearly all surface street parking spaces were occupied, yet collected revenue was less than a quarter of forecasted income. When the glitch is discovered, the city sues the device manufacturer for lost business due to the bugs in the software.



# **Category 4:** 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. While IT is often the focus of cyber risk, and top management is ultimately held responsible, everyone in the entire company plays a vital role in securing client data and preventing security breaches.**

## ILLUSTRATIVE RISK SCENARIOS FOR CYBER RISK

**UNSECURED LOADING DOCK SENSOR**

A large e-commerce retailer coordinates pickup and delivery at a warehouse for multiple freight carriers. A hacker gains entry from an unsecured IoT device at the loading dock that happens to be connected to the e-commerce payment system. The thief is able to capture thousands of customers' names and credit card numbers, which he sells to foreign hacker groups. The company is sued for failure to secure the device at the loading dock.

**INTERCEPTED CLOUD COMMUNICATION**

A logistics company captures delivery data (customers' names, addresses, bank account and other payment information) and stores it in a cloud for later business intelligence analysis. Cyber thieves intercept unsecured M2M communication between the sensor and the cloud data store which they then sell to competing e-commerce merchants. The device maker is sued for failure to secure M2M communication.

**MARINE BIOMETRIC DATA THEFT**

A marine shipping company uses biometric facial sensors to permit/deny access to authorized areas in a high-volume seaport. The company stores these digital identifiers in a hybrid cloud configuration. A cyber criminal gains access to these files through a vulnerability in the video identification system, then distributes them to other hacker cooperatives for the purpose of gaining unauthorized entry into sensitive port areas. The company discovers the theft and is forced to take the biometric system offline and replace it with an alternative identification method. The shipping company sues the device maker for failure to secure their sensors.

# Actions to consider for minimizing risk from IoT

The IoT offers transportation ecosystems exciting new possibilities for improving throughput and on-time delivery. However, as technology companies develop, manufacture and commercialize IoT devices, they can expose themselves to significant additional risks. Fortunately, there are several actions that companies can consider to minimize their exposure to these risks.

## CONSIDER APPROPRIATE QUALITY AND RISK MANAGEMENT SYSTEMS

Manufacturers producing IoT devices for transportation applications should be aware of and adhere to appropriate quality and risk management systems. This will help to ensure that their products consistently meet requirements and specifications. Manufacturers should develop product requirements to achieve product safety and efficacy.

Direct and reputational costs from product liability events can cripple companies, sometimes endangering their very existence. Regardless of the quality system adopted, device manufacturers should consider the following steps to ensure device safety and security:

### Conduct robust hazard analysis

Methods such as fault tree analysis (FTA), failure mode and effects analysis (FMEA), and hazard and operability analysis (HAZOP) can be used by device makers to assess potential hazards at different points in device development and commercialization. Companies should not ignore issues that can be introduced during processes such as manufacturing, packaging, labeling, storage or transport.

### Conduct routine design reviews

Product manufacturers should not only test their own devices, but also any related software or peripheral hardware they may be using. Software and firmware developers should implement a system of continuous integration to detect bugs as early as possible in the build phase where they are easiest and least costly to fix. Companies should assemble a diverse team that includes personnel outside of the design process to generate potential risk reduction solutions.

### Develop clear safety and use instructions with conspicuous warning labels

Companies should provide users with clear, unambiguous written instructions on the full range of use for devices. This includes providing visual depictions of proper device use, as well as instructions on what to do if a device malfunctions.

### Build in cybersecurity

A lack of cybersecurity in devices creates the potential for unplanned and costly events. A device designed to exchange data with a back-end cloud or perhaps another IoT device could be breached, resulting in serious consequences to customers, employees or property. With the right efforts, companies can protect themselves by incorporating simple, yet effective security features into IoT technology.

# BUILD IN CYBERSECURITY

A lack of cybersecurity in devices creates the potential for unplanned and costly events. A device designed to deliver medication or monitor a facility's conditions could be breached, resulting in serious consequences to patients or property. With the right efforts, companies can protect themselves by incorporating simple, yet effective security features into IoT technology. Consider the following steps to minimize exposure to cyber risk:

### Encourage input from IT security professionals

Cybersecurity professionals should communicate with all business functions responsible for the development and commercialization of IoT technology. To build in security from the start, security engineers should reach across organizational reporting relationships. Every phase of IoT device development should interface with security engineers, including product design, development, testing and customer service. Organizational silos should not prevent security professionals from providing critical input for the finished product.

### Application security patches

A major part of the software application development lifecycle (SDLC) is maintenance. The "always-on" nature of the IoT makes patches and service releases particularly challenging because there is no concept of scheduled downtime; updates need to be applied when all devices are in use. Because security threats evolve over time, application developers must design their apps in ways that can accommodate a real-time "push" service pack installation without compromising performance levels during the installation.

### Physical security

Some IoT devices are very small, making it easier for thieves to steal them unless they are physically secured or otherwise out of a potential thief's reach. If the device has any sort of internal storage mechanism, the data on the device at the time it is stolen will also be at risk. Device makers should anticipate the possibility of a device being stolen and implement warning mechanisms to notify the owners and wipe the local data cache in the event of a device theft.

### Bluetooth encryption

Bluetooth offers an encryption Application Programming Interface (API) when exchanging data between a device and its target data store, but few companies take advantage of it because it decreases battery life. Consider enabling it for more effective security.

### Ensure backward compatibility

Sensor hardware is only half of what is necessary to make the IoT work properly. The other half is the software that receives data from sensors in the field. Embedded devices are very durable, and may outlive the algorithms that power them. IT leaders should take steps to ensure that this does not happen. Make sure that any new algorithms or program changes are backward compatible to the sensors they are designed to accept data from.

### Identity management

In the typical corporate local area network (LAN), two basic building blocks of security are authentication and authorization. Security algorithms allow work to be done by personnel who have input their network passwords by hand. This is not possible with IoT nodes, so input validation must be performed some other way. The National Institute of Standards and Technology (NIST) has recently chosen the compact SHA-3 as the new algorithm for the so-called "embedded" or smart devices that connect to electronic networks but are not full-fledged computers. Other authentication methods to consider include geographic IP filters, strong identities and delay-tolerant networks.

### Secure the cloud

Data is often transmitted from a sensory device to a smartphone and then to a cloud. 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; companies producing IoT technology should consider similar functionality.

### Require strong passwords

Devices should be designed to disallow default passwords and should instead require strong passwords before the device can be deployed.

### Encrypt critical data elements

The most critical pieces of data transferred between IoT devices and data stores are often user IDs, passwords and PIN numbers. Astoundingly, most devices transmit these data elements in plain text with no encryption at all.

### Remote erase feature

Consider building in the option to remotely erase and/or disable a device if it is ever lost or stolen. This feature comes standard on many late-model smartphones.

# EVALUATE COMPANY CONTRACT PRACTICES

From time to time, even well-designed products fail to perform as expected. In those rare cases, a deficiency could have unfortunate side effects that manifest themselves in high-dollar liability claims. Companies can manage their exposure to technology risk by ensuring that they contractually transfer risk where possible. To do this, technology companies should consider the following specific contract provisions:

**Limitation of liability**
This provision disclaims liability for certain types of damages – usually incidental, indirect consequential and special damages. In the event of actual or threatened litigation, these provisions can become very useful in minimizing ultimate exposures.

**Damage caps**
These provisions limit the amount of recoverable damages. The limitations can be defined in terms of a specific dollar amount or an amount to be determined, depending on specific factors set forth 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**
Provisions like these can shift risk to other parties.

# Insurance considerations

It is impossible to predict the many ways in which technology companies could find themselves liable should IoT technology fail to operate as expected. While these risks cannot be eliminated, they can and must be managed. To help decrease exposure, technology companies should investigate insurance options for the categories of risk described in this issue of the Travelers Global Technology Risk Advisor. The following table recounts the key risk categories and illustrative risk scenarios noted earlier, along with information on relevant insurance coverage to protect against potential liability.

| Risk category | Illustrative risk scenario | Relevant insurance coverage to evaluate with an agent or broker |
|---|---|---|
| **Property damage** | • Lack of locomotive maintenance<br>• Shipboard sandbar sensor failure<br>• Tank truck leak | **Products liability coverage** provides coverage for physical damage to a third party's property arising out of a product manufactured, sold, handled, distributed or disposed of by you. |
| **Bodily injury** | • Self-driving catastrophe<br>• Foggy aircraft collision<br>• City bus notification failure | **Products liability coverage** provides coverage for physical harm to a person arising out of a product manufactured, sold, handled, distributed or disposed of by you. |
| **Financial loss** | • GPS programming glitch<br>• Parking meter sensor failure | **Technology Errors and Omissions (E&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. |
| **Cyber risk** | • Unsecured loading dock sensor<br>• Intercepted cloud communication<br>• Marine biometric data theft | **Cyber liability and cyber-related first-party coverages** provide protection for critical cyber risks. Liability coverage options vary, but most include coverage for loss caused by the failure to prevent a security breach. First-party expense coverages can include forensics, data restoration, business interruption, social engineering fraud, system failure, extortion, computer fraud and funds transfer fraud, and public relations and breach notification expenses. |

Each company's security requirements are unique, so few insurance policies are standardized.. Likewise, not all risks may be insurable. It is important to contact your independent insurance agent or broker to discuss your company's unique insurance requirements.

# How Travelers can help

Travelers understands the unique needs of technology firms. We often insure what other carriers will not, because we've been protecting tech companies longer than most. So, as you work on the next groundbreaking IoT technology, Travelers will be there to help manage the 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 options to provide technology companies with important insurance coverage for exposures as they continue to innovate. Mike Thoma, Chief Underwriting Officer for Travelers Global Technology, says, "You come to expect unique exposures when you work with cutting-edge tech companies. And you figure it out. We've been doing that for 30 years."

Experience and innovation have uniquely positioned Travelers to protect technology firms as they bring the IoT from idea to reality.

For more information, contact your independent insurance agent or broker who represents Travelers, or visit us on the web at **travelers.com/technology**.

# References


Ashton, K., Ante, E., "The Internet of Things is Becoming a Nervous System," The Intelligence of Things, accessed Dec. 2016, https://flex.com/intelligence/iot/internet-things-becoming-nervous-system

"The Industrial Internet of Things: Why it demands not only new technology—but also a new operational blueprint for your business," Price Waterhouse Coopers, 2016, accessed Dec. 2016, https://www.pwc.com/gx/en/technology/pdf/industrial-internet-of-things.pdf

"IoT Market in Intelligent Transportation Systems by Components (Semiconductor, Wireless, and Others), Products, Software & Services, Verticals (Road, Rail, Air, and Maritime), Solutions, Applications, and Geography – Analysis & Forecast to 2014 – 2020," MarketsandMarkets, April 2015, accessed Dec. 2016, http://www.marketsandmarkets.com/Market-Reports/iot-in-transportation-market-48213177.html

"How Smart Packages Are Changing the Shipping Industry," Water.IO, 2016, accessed Dec. 2016, http://www.water-io.com/shipping-smart-packages

"Hum," Verizon, 2016, accessed Dec. 2016, https://www.verizonwireless.com/connected-devices/hum-by-verizon/

Dickson, Ben, "How IoT and machine learning can make our roads safer," Tech Crunch, July 2016, accessed Dec. 2016, https://techcrunch.com/2016/07/13/how-iot-and-machine-learning-can-make-our-roads-safer/

"Driver Behavior," IBM Blue Mix Catalog, 2016, accessed Dec. 2016, https://console.ng.bluemix.net/catalog/services/driver-behavior/

Rapolu, Bhoopathi, "Internet Of Aircraft Things: An Industry Set To Be Transformed," Aviation Week, Jan. 2016, accessed Dec. 2016, http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed

Harpham, Bruce, "How the Internet of Things improves air travel," CIO Magazine, May 2015, accessed Dec. 2016, http://www.cio.com/article/3074125/internet-of-things/how-the-internet-of-things-improves-air-travel.html

Jenner, Gillian, "Analysis: How airlines are tapping into the Internet of Things," General Electric, 2016, accessed Dec. 2016, https://www.ge.com/digital/press-releases/how-airlines-are-tapping-internet-things

Bellias, Matt, "Connected trains: how IoT is driving the future of rail," IBM Internet of Things blog, Nov. 2016, accessed Dec. 2016, https://www.ibm.com/blogs/internet-of-things/connected-trains-rail-travel/

Ninan, S., Gangula, B., von Alten, M., Sniderman, B., "Who owns the road? The IoT-connected car of today—and tomorrow, The Internet of Things in automotive," Deloitte, Aug. 2015, accessed Dec. 2016, https://www2.deloitte.com/insights/us/en/focus/internet-of-things/iot-in-automotive-industry.html

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 technology companies evolve, Travelers will be there to help manage their risks with the right insurance products.

TRAVELERS

**travelers.com**