CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Internet of Things

TECHNOLOGY SPOTLIGHT

"IoT [Internet of Things] is transforming the everyday physical objects that surround us into an ecosystem of information that will enrich our lives. From refrigerators to parking spaces to houses, the IoT is bringing more and more things into the digital fold every day, which will likely make the IoT a multi-trillion dollar industry in the near future."[1]

For a while now the world wide web has enabled communications between people, businesses, and economies. In its infancy, these connections were typically through desktop computers connected to servers and data centres. The network connections were often through tethered outlets that confined devices to fixed locations.

But that is changing. People are no longer chained to one location by cables connected to servers that take up entire floors of office buildings. They can connect through nearly any device that allows you to collect and exchange data. The power of the Internet and advancements in wireless technologies have brought about the age of the Internet of Things.

Description

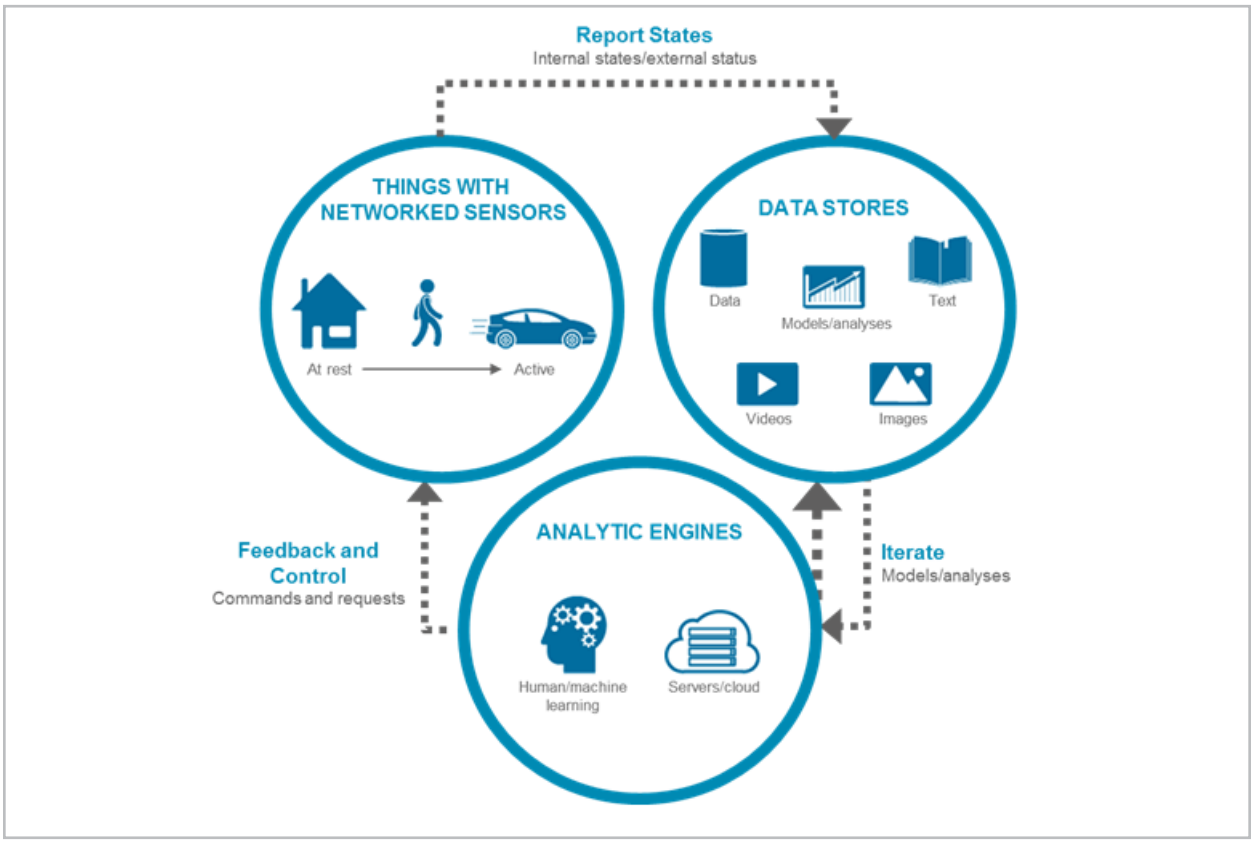
An IoT device is any computing device with the ability to transfer data over a network. TVs, security cameras, appliances, light switches, and motion sensors for the home, or industrial sensors, advanced radio-frequency ID (RFID) tags, beacons, and drones for businesses, are all examples of IoT devices. According to Gartner, the Internet of Things (IoT) is a network of dedicated physical objects (things) containing embedded technology for communicating and sensing or interacting with their own internal states or the external environment. The

1 www.pwc.com/us/en/increasing-it-effectiveness/assets/future-of-the-internet-of-things.pdf

2 www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

connecting of assets, processes and personnel enables the capture of data and events from which a company can learn behaviour and usage through analytics, react with preventive action, or augment or transform business processes.[2]

Interactions within an IoT System



Source: https://securityledger.com/2014/04/will-ot-big-data-create-darwinian-struggle-for-insurance-carriers/iot-loop/

Importance

With over 20 billion IoT devices expected by 2020,[3] IoT devices will become embedded in our lives and businesses. Appropriate use of IoT devices will support near-real-time data collection and analysis that will lead to better and more timely data-driven decision making. In addition, the IoT will further enable automation and allow businesses to transform processes and increase operational effectiveness (e.g., predictive maintenance). Already there are many real-world applications for the IoT that can benefit businesses and consumers. These benefits are not limited to specific industries even though certain industries like manufacturing, agriculture, retail and healthcare may be poised to benefit more than others.

3 www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/

For CPAs, the immense amount of real-time data that will be available will lead to improvement in the accuracy of planning and forecasting exercises. With "things" gaining the ability to communicate, reporting information such as inventory levels becomes more accurate and efficient. Fraud will be harder to commit and easier to detect by reducing human touchpoints. The IoT will also enable predictive maintenance on machines; CPAs will have a better view of which machines may require maintenance and allocate budgets accordingly. CPAs will need to understand how the IoT can transform the businesses they support and understand how finance systems need to transform along with them.

Business Benefits and Considerations

In a survey conducted by the World Economic Forum, 68% of respondents indicated the IoT as being strategic or transformational to their business. The top three business benefits selected were increased productivity, process automation, and optimization of the value chain.[5]

- **Increase productivity**
  Applying the right IoT devices will enable businesses to anticipate breakdowns of capital equipment so that preventive maintenance can be performed without disruption. This reduces maintenance-related delays and can improve the timeliness of product or service delivery.
- **Automate process**

EXAMPLES OF IOT APPLICATIONS

IoT sensors **in manufacturing and retail environments** can improve asset management by reducing shrinkage and spoilage, ensuring supply chain and store shelves are fully utilized, and improving labour efficiency and customer experience. An IoT-enabled store will be able to monitor stock levels in real time, reduce employee efforts to sort and locate missing items and thereby improve the overall customer experience.

IoT sensors **on the farm** can help monitor light, temperature, humidity and the soil moisture of crop fields to intelligently automate irrigation systems. An IoT-enabled irrigation system can optimize water use and improve crop yields thereby reducing expenses and improving revenue at the same time.

IoT sensors **on commercial aircraft** combined with analytics on maintenance logs and fault messages help airlines avoid costly maintenance delays and cancellations by enabling predictive maintenance. A commercial use case of predictive maintenance is PwC's solution that can predict 15%-30% of maintenance-related delays and cancellations, leading up to 0.3%-0.6% improvement in on-time performance.[4] The application of predictive maintenance can be transferred to other industries as well.

4 www.pwc.com/us/en/industries/transportation-logistics/airlines-airports/predictive-maintenance.html

5 www.weforum.org/agenda/2015/06/what-are-the-business-benefits-of-the-internet-of-things/

IoT devices can serve as workflow triggers that initiate processes based on pre-set conditions thereby eliminating the need for human intervention. For example, sensors can detect the arrival of inventory at a warehouse and automatically collect and send the relevant information to the inventory tracking system.

- **Optimize value chain**
  IoT devices can improve visibility across the entire value chain (from planning to scheduling inventory) as a unified environment or system. More accurate information and real-time tracking will help management make data-driven decisions to manage inventory better and reduce waste.

In addition to those benefits, IoT can:

- **Improve customer experience**
  Manufacturers of IoT devices can provide firmware updates that improve functionality based on customer feedback or provide proactive support if a breakdown is imminent, thereby improving the customer experience.
- **Create new business models**
  As with any new technology, there is a potential to disrupt existing business models or create new ones. Technology companies such as Google have developed networked security cameras and sensors for the home that can replace traditional home security solutions.

While there are numerous benefits to adopting IoT devices in business, there are still some important risks to manage in order to effectively unlock the value of IoT:

Risk Areas	Risk Mitigation Strategies
IoT devices may increase security threats due to: • **outdated software or firmware** • **lack of encryption to protect transmitted data** • **weak authentication requirements** • **default administrative passwords.**	• Treat IoT devices like other networked devices and implement appropriate encryption and end-point security. • Where possible, contract equipment from known viable and reputable manufacturers or IoT service providers. Ensure the existence of an appropriate update frequency for device software/firmware. • Change default administrative passwords from the manufacturer to a password that complies with organizational IT policies.

Risk Areas	Risk Mitigation Strategies
IoT data stored in the cloud may not be adequately protected when managed by an IoT service provider.	• Business should specify security and protection requirements such as ensuring appropriate controls around storage, transmission, and access as well as breach notification requirements. • Service provider should agree to specific requirements for cloud security in a contractual agreement. • Service provider should provide a third-party assurance report on their cloud security and, if needed, privacy and compliance with contractual obligations. • Consider leveraging edge computing to process the IoT data on a local device to eliminate the amount of sensitive data being transmitted. For example, Apple's FaceID/TouchID data is stored on your device; user verification is done locally without the data being transmitted back to Apple servers for processing.
Network infrastructure may not support bandwidth demands from IoT devices.	• Each IoT device will utilize a portion of available bandwidth on the network. As more devices are added to the IoT network, businesses must ensure adequate bandwidth is available to support communication between these devices and critical applications. Otherwise, network downtime may reduce employee productivity or provide a negative customer experience. • Edge computing moves the processing of data generated by IoT devices from the cloud back to the device, thereby reducing bandwidth demands.
The IoT data breached may include personally identifiable information.	• Generally, stored data should be encrypted with personally identifiable information stripped out in order to minimize the impact of information theft resulting from a data breach. • If personally identifiable information is required to be collected and stored, ensure compliance with local privacy laws such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA) in Canada and the General Data Protection Regulation in Europe. • Prepare a data breach response plan that should include steps to: — contain the breach — evaluate the risks as a result of the breach — notify impacted persons — prevent future incidents

Risk Areas	Risk Mitigation Strategies
Employees may gain unauthorized access of IoT devices through personal mobile devices.	• Create a separate private network for IoT devices that are not shared with the network accessible by employee devices. • Ensure passwords for IoT devices are secure by changing them from manufacturer defaults to forms that meet organizational IT policies.
Employees may gain unauthorized physical access to IoT devices.	• Review IoT devices periodically to ensure outer casing has not been tampered with. • Place IoT devices in locations where access controls are secure and limited to authorized individuals. • Review logs for IoT devices periodically and investigate those where the device has gone offline. Typically, to maliciously tamper an IoT device would require bringing it offline and rebooting it.

This publication is part of the **Technology Spotlight series**.

The entire series covers technology trends that impact CPAs and are available on our website.