#IoTatWork for Small and Medium Businesses

Understanding the **Internet of Things**

GETCYBERSAFE.CA

Canada

Agenda

- What is the Internet of Things?
- How does it work?
- What sectors use the IoT?
- IoT Business developments
- Risks to information security
- Risks to privacy
- Risks to safety
- IoT Security checklist

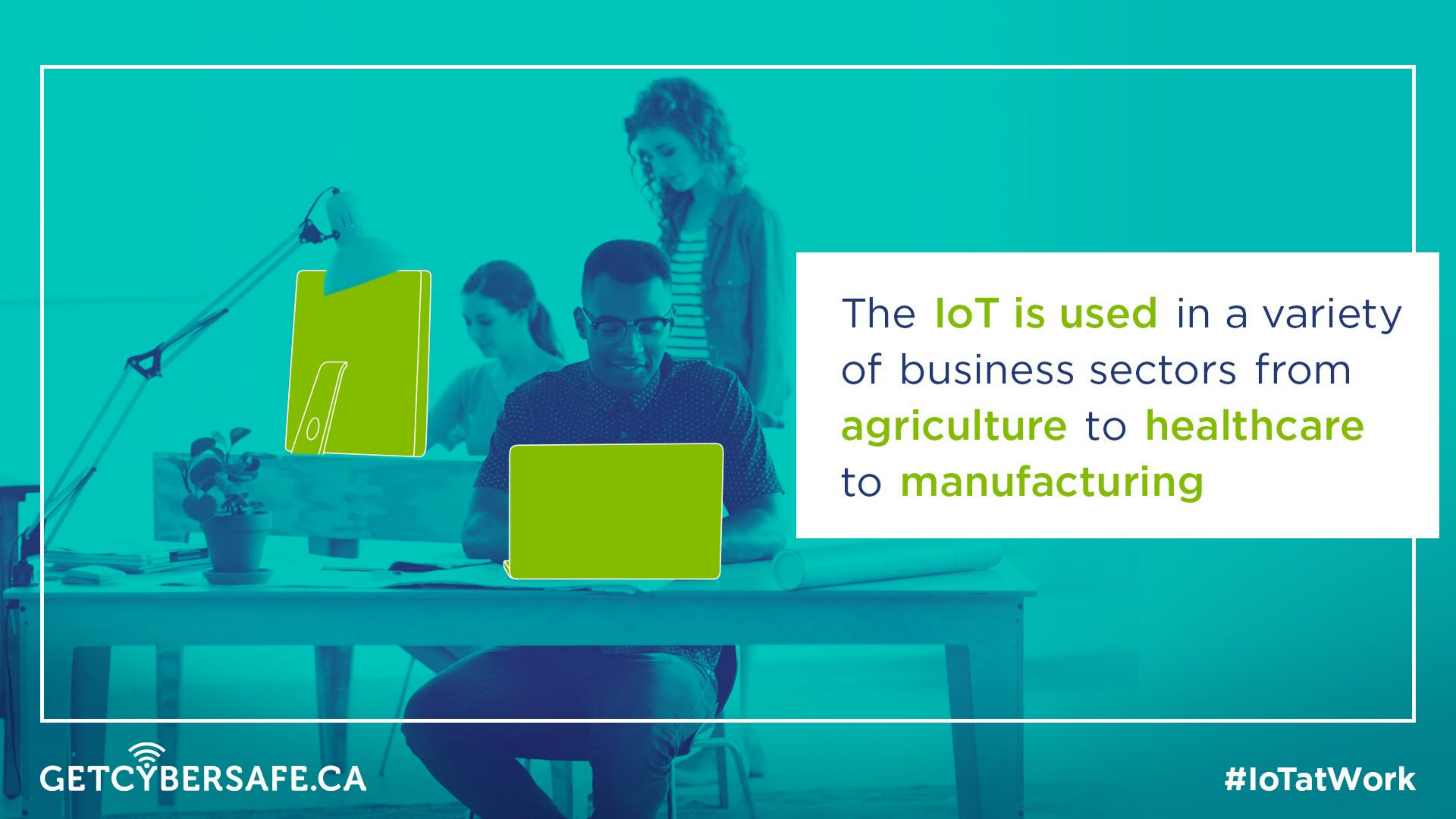
What is the Internet of Things?

The Internet of Things (IoT) is a network of 'smart' devices that connect and communicate via the Internet.

How does the IoT work?

Smart devices collect and exchange information machine to machine (M2M) and with us.

- Remote control and monitoring
- Operate automatically through software, cameras and sensors



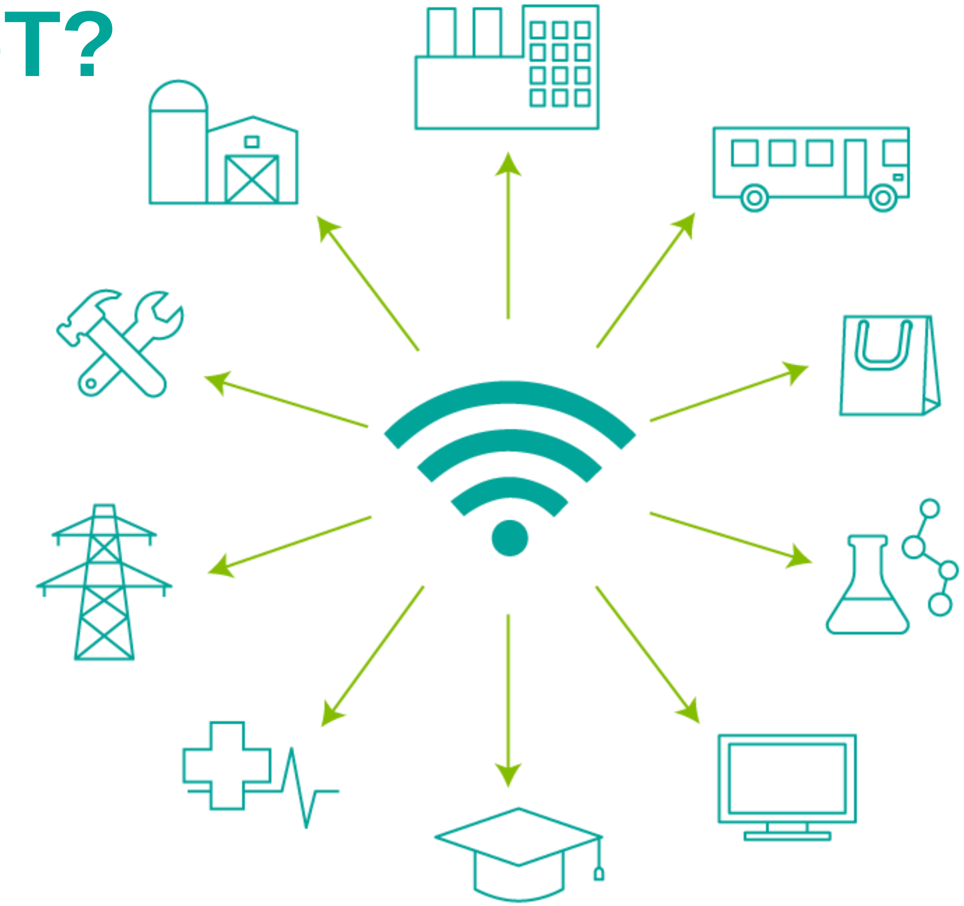
The **IoT is used** in a variety of business sectors from **agriculture** to **healthcare** to **manufacturing**

GETCYBERSAFE.CA

#IoTatWork

What sectors use the IoT?

1. Manufacturing
2. Transportation
3. Retail
4. Science and Technology
5. IT and Communications
6. Education
7. Healthcare
8. Energy
9. Construction
10. Agriculture



IoT business developments

Retail

- Automated checkout
- Inventory and warehouse management

IoT business developments

Manufacturing

- Operations efficiencies
- Asset management and maintenance

IoT business developments

Consumers

- Entertainment
- Health and fitness

IoT business developments

Offices and Government

- Productivity and energy saving
- Security and surveillance

IoT business developments

Transportation

- Automation and traffic control
- Fleet management

IoT business developments

Healthcare

- Monitoring
- Automated administration of treatment

The **biggest impediment** to businesses implementing IoT is **security**

GETCYBERSAFE.CA

#IoTatWork

Risks to Information Security

Possible consequences of an information breach:

- Loss of reputation/credibility
- Loss of revenue and time
- Lead to legal challenges

Risks to Information Security

Direct cyber incidents:

- Remote control and monitoring
  - From head office, to supply chain, to customers

Indirect cyber incidents (viral threats, malware):

- Downstream effects on IT security infrastructure
  - A malware attack on the IoT device manufacturer could affect your IoT devices

IoT-related **cyber incidents** increase the **risk of theft**, **exposure**, or **corruption** of **information**

GETCYBERSAFE.CA

#IoTatWork

Risks to Privacy

Business, employee, and client information could be:

- Destroyed
- Altered
- Stolen and exposed
- Held for ransom

Risks to Privacy

Understand IoT device data collection policies:

- What information is gathered?
- How long is data kept?
- What is your data used for (marketing research, etc.)?

Unauthorized control of an IoT **device** could cause **physical damage** or **harm**

GETCYBERSAFE.CA

#IoTatWork

Risks to Safety

IoT device malfunction or manipulation could cause:

- Physical damage to data
- Physical damage to equipment
- Physical harm

Risks to Safety

Possible consequences of IoT device malfunction or manipulation:

- Costly repairs to systems, assets, and equipment
- Legal impact of harm to staff, customers or public
- Loss of reputation

IoT Security Checklist

Before implementation:

- ❑ Research devices before you purchase. Read reviews and get recommendations; research their security capabilities.
- ❑ Have a point of contact with the manufacturers for any issues down the road.
- ❑ Read device materials: operator’s manuals, instructions, support forums.
- ❑ Create a Bring Your Own Device (BYOD) and IoT policies for employees.
- ❑ Assess against your existing IT security policies and standards.

During implementation:

- ❑ Secure your wireless network.
- ❑ Change device default usernames and passwords, and use strong passwords.
- ❑ Keep networks with sensitive information isolated. Consider using separate networks for IoT devices.
- ❑ Ensure the device has system reset capability in order to permanently eliminate sensitive configuration information.
- ❑ Control who can access your network and from where.
- ❑ Encrypt data, commands and communications, both at rest and in transit.
- ❑ Where possible, set operating system, software, and firmware to update automatically. Establish periodic manual updates as required.

IoT Security Checklist

After implementation:

- □ Implement a repeatable process to validate all safeguard and countermeasures in your implementation.
- □ Conduct ‘cyber incident’ tests and audits regularly to ensure the integrity of your network.
- □ Backup data regularly using secure and redundant storage solutions, such as multiple storage units and/or the cloud. Test your recovery process regularly.

IoT Security Checklist

Adhere to your company's Bring Your Own Device/ IoT policy

- ❑ Understand what information is being collected by devices and why, before you download or buy.
- ❑ Use a lock screen password, use strong passwords.
- ❑ Backup data regularly on multiple storage units and the cloud.
- ❑ Connect only to secure Wi-Fi networks.
- ❑ Use safe websites, cloud storage, etc.

Download your **Get Cyber Safe Guide for Small and Medium Businesses** and get more **#IoTatWork** resources at **GetCyberSafe.ca**

Your Guide to IoT Security
#IoTatWork

Internet of Things
Toolkit for Small and Medium Businesses

GETCYBERSAFE.CA

GETCYBERSAFE
Protect while you connect.

Know the Risks.

Protect Yourself.

Protect Your Business.

GETCYBERSAFE GUIDE FOR SMALL AND MEDIUM BUSINESSES

Canada

GETCYBERSAFE.CA

Canada