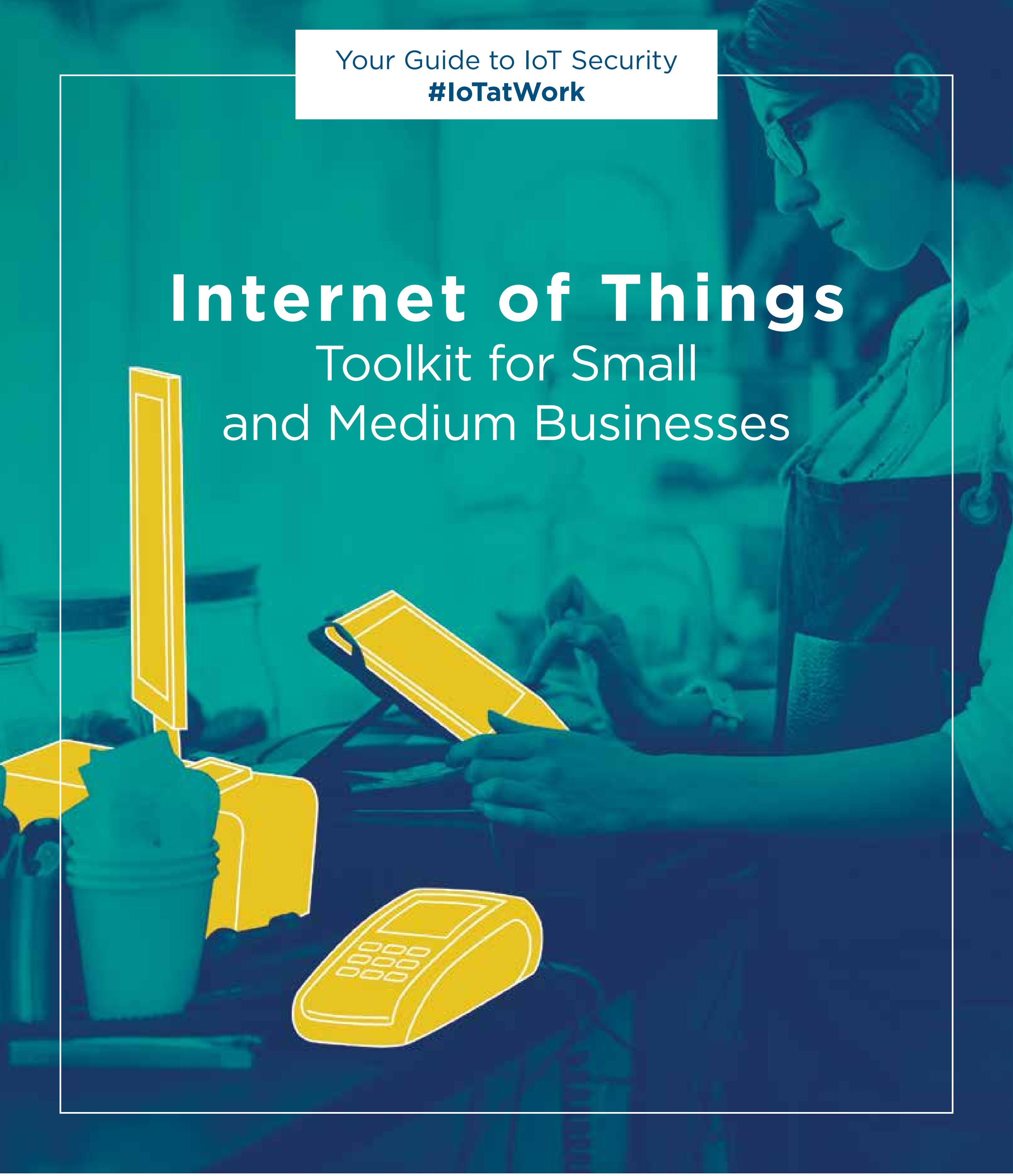
Your Guide to IoT Security
#IoTatWork

Internet of Things
Toolkit for Small and Medium Businesses



GETCYBERSAFE.CA

Canada

Table of Contents

Introduction

The connectivity and automation of the Internet of Things (IoT) can help all business sectors to progress, but it can come with substantial risks. IoT devices connect, communicate, and exchange information via a network, exposing more points of access to the data stored and devices controlled by your network. Cyber security is the key to protecting your small or medium business from possibly devastating cyber incidents.

As a small or medium business owner and/or leader, you may think your business is not a target for a cyber incident. However, the IoT increases your exposure to cyber incidents, and the complexity of cyber security.

With this guide, you'll learn how the IoT works and where it will have an impact, and the risks related to information security, privacy, and safety. Our five-step cyber security strategy will help you securely implement the IoT into your business, and help you create an IoT security policy to integrate with your existing cyber security policy.

IoT security is a shared responsibility between management, IT, and all employees.

Along with this guide, the **#IoTatWork Toolkit** has other resources to share with your business **GetCyberSafe.ca**.

This guide is a companion to the Get Cyber Safe Guide for Small and Medium Businesses and references sections of that Guide for further information. When you see this symbol 📄, please refer to the indicated section of the Get Cyber Safe Guide for Small and Medium Businesses.

The Internet of Things

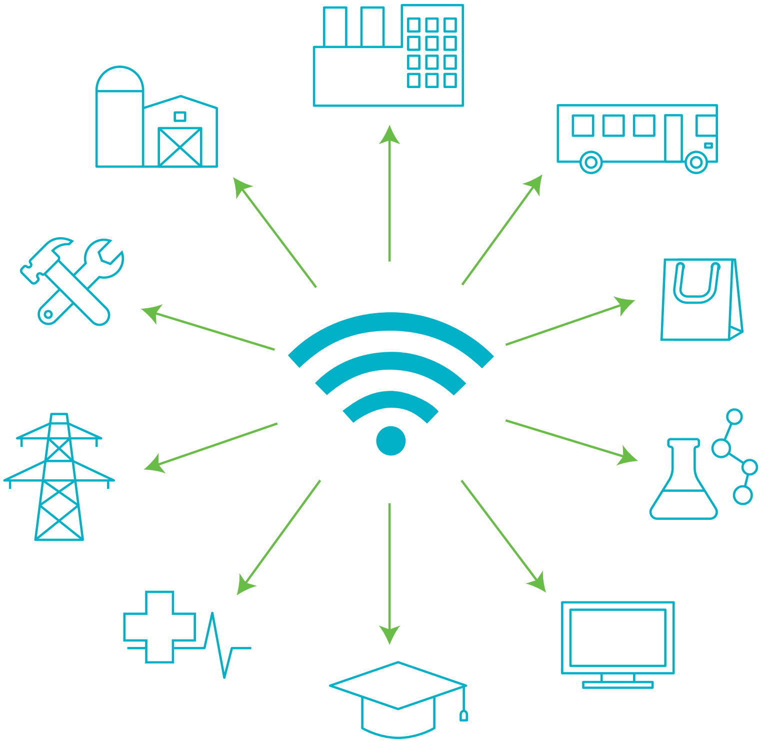
The IoT is made up of 'smart' devices that connect and communicate via a network, such as the Internet. IoT devices collect and exchange information through embedded software, cameras, and sensors that detect light, sound, distance, movement, etc. IoT devices can be remote controlled and monitored, but most operate automatically. Some examples of smart devices include appliances, locks, security cameras, manufacturing equipment, and connected cars.

The Internet of Everything (IoE) is an extension on the IoT, which encompass a more complex system of machine-to-machine communication as well as with people and process. The IoE is comprised of people, data, processes, and things.

The Industrial Internet of Things (IIoT) refers specifically to the integration of IoT technologies, networked sensors, and software into complex physical machinery used in manufacturing, etc. It is also known as the Industrial Internet.

Presence of IoT in Business Sectors

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



Some of the main IoT developments include:

- **Retail**
  - Automated checkout
  - Inventory and warehouse management
- **Manufacturing**
  - Operations efficiencies
  - Asset management and maintenance
- **Consumers**
  - Entertainment
  - Health and fitness
- **Offices and Government**
  - Productivity and energy saving
  - Security and surveillance
- **Transportation**
  - Automation and traffic control
  - Fleet management
- **Healthcare**
  - Monitoring
  - Automated administration of treatment

IoT and the Risks to Information Security

The biggest impediment to businesses implementing IoT is security. IoT risks could have serious consequences on a business's reputation and credibility, could cause a loss of revenue and time, and could lead to legal challenges.

IoT devices connect to each other, to your business network and to other devices on that network, back to the IoT supplier, and even to the devices of your customers and employees. Due to such interconnectivity and automation, a cyber incident could affect multiple levels of your business; from the head office, to the supply chain, and even to the customer.

Whether a targeted incident on a certain device, or an indirect incident through viral threats like malware, IoT cyber incidents have downstream effects on your IT security which could weaken your entire IT infrastructure. For example, if your business has a fleet of Intelligent Transportation System (ITS) delivery trucks and the developer/manufacturer of the trucks is affected by malware, your connected trucks could be indirectly affected by the malware incident as well. For more information on malware, refer to Web Security — Malware.

With every connection comes an increase in vulnerability. If you do not control who and what connects to your network you cannot protect the information that traverses it. For more information on information security, refer to Data Security.

IoT and Privacy

For any cyber incident, IoT-related or not, the risk of theft, exposure, or corruption of information is greatly enhanced. Business, employee, and client information could be destroyed, altered, stolen and exposed, or even held for ransom.

IoT devices collect vast amounts of data, which creates concern over the confidentiality, privacy, and integrity of business data. Ensure to use IoT devices that provide transparency on their policies of data collection, such as what information is gathered, how long it is kept, and what it's used for (marketing research, etc.).

With the introduction of IoT into the business, you might consider updating your privacy policies. Consider using a professional cyber security organization to help you conduct a privacy impact assessment, develop IoT standards, and define levels of trust for users vs. machines/devices. For example, a trusted user on an untrusted device, should be untrusted and subject to restrictions. Seeking legal assistance can help you understand and reevaluate legal responsibilities and requirements, IoT device privacy statements, and contractual arrangements.

Your employees' information and privacy could be compromised as well, through personal devices connected to the business network. Employee education and training on the IoT can help protect their privacy. So too can creating an IoT policy, similar to a Bring Your Own Device (BYOD) policy, which addresses network access, permitted devices, passwords, secure sites, etc. For more information on policies, refer to Management Issues — Developing Policies and Standards.

IoT and Safety

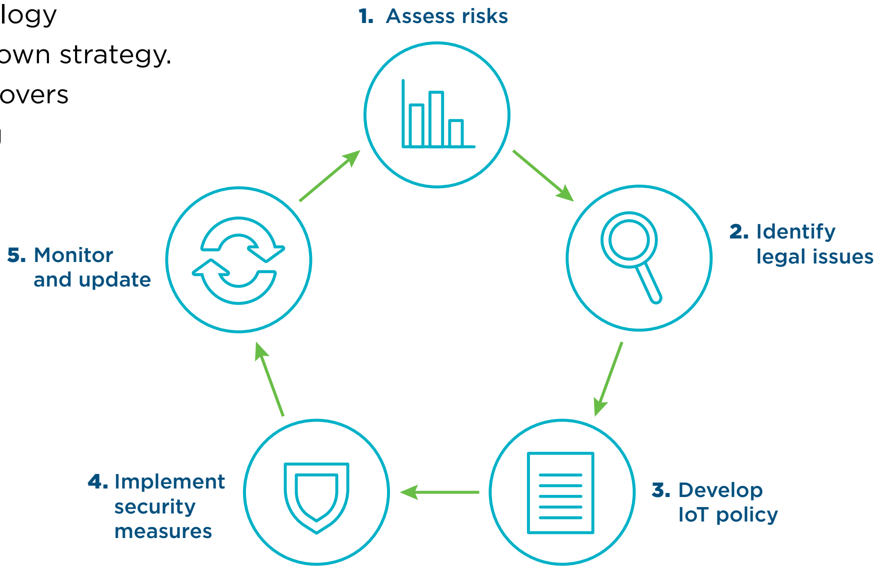
When an IoT device controls physical assets and operations, such a smart vehicle or an insulin pump, the threat of a cyber incident extends beyond a breach in information. The unauthorized control or remote takeover of an IoT device could cause physical damage to data and equipment, or even physical harm. These damages are costly, as you seek to recover your systems, assets, and your reputation. For many devices, their operational roles can be far more important than the information they store. Consider the legal and financial impact of a device failing or being manipulated. For more information on safety, refer to Physical security.

To protect your equipment, your staff, and your customers, the basic IoT security framework should cover the device, the remote-control element, and the IT infrastructure, and consist of:

- Secure boot and reset capability
- Authentication and integrity
- Encryption
- Firewall
- Updates
- Intrusion detection and reporting
- Remote control and audit

IoT and your Business: a Cyber Security Strategy

Implementing new IoT technology requires a step by step, top-down strategy. Our 5-step security strategy covers the essentials of incorporating IoT into your business. This strategy can also be used for all business IT processes and controls, whether networked or not.To learn more about cyber strategies, refer to Management Issues — Cyber Security Planning.



Step 1: Assess risks

A thorough risk assessment is the first step to updating security policies. With the IoT, cyber crime could come from new and unexpected places. IoT should be part of your overall risk profile.

- Conduct a threat and privacy impact assessment, considering how connected objects will interact with each other.
- Audit apps, devices, networks, databases, and communications protocols. Determine interoperability between those devices that you may already have.
- What's on your network? How valuable is that information? Who's connected? Identify any vulnerabilities and worst-case scenarios.

Step 2: Identify legal issues

The introduction of IoT into your business operations presents possible legal issues and concerns. You should be aware of your company's legal responsibilities in both the physical and virtual worlds.

- Seek legal counsel to understand external obligations such as provincial or federal law.
- Consider the legal consequences of the manipulation or malfunction of the physical controls of an IoT device.

Step 3: Develop IoT policy

To cover all levels of business operations, align your IoT policy with your existing cyber security policies.

- Management and IT should work together to make IoT deployment a cross-business, multi-level responsibility.
- Confirm with your supply chain (partners, suppliers, etc.) they are taking the proper measures to secure their systems as well.
- Consider how the IoT will integrate with your existing business strategy. Make sure the IoT can help you achieve your short and long-term objectives.
- Invest in developing a skilled workforce by educating and training your employees. Download our #IoTatWork employee training presentation **GetCyberSafe.ca**. For more information on policies, refer to Create Stronger Cyber Safety Policies.

Step 4: Implement security measures

Here’s a list of security tips for before, during, and after implementation of IoT devices.

According to a 2017 research study by Public Safety Canada, 57% of small business owners or managers are the person in charge of IT.[1] Consider consulting a cyber security organization/professional for more help.

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. For more information, refer to Run a More Cyber Safe Business.

□ Change device default usernames and passwords, and use strong passwords. Refer to Authentication Best Practices.

□ 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.

[1] Public Safety, Ekos Public Opinion Research

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. For more information, refer to Data Security — Backup and Recovery Options.

Step 5: Monitor and update

Monitor your IoT devices and networks.

- Decide who will oversee IoT, and how often device activity should be monitored.
- Where possible, put automatic auditing tools in place to monitor, measure, detect, and correct IoT security problems. In the absence of automation, implement regular manual procedures.
- How much oversight should management provide, and how often? Consider making updates quarterly.

Updating software, patches, and operating systems is an ongoing process. Therefore, these security steps should be repeated frequently and with each new IoT device. Keep communication between management and IT open. Finally, make sure your employees are adhering to your IoT policy. With more and more connected devices in the workplace come more points of vulnerability and risk.

IoT Developers, Manufacturers, Service Providers

Security should be top of mind for IoT device developers, manufacturers, service providers, and network operators. Security and privacy safeguards should be prioritized in the design, development, and deployment of IoT products.

As a best practice, IoT developers and service providers should include as much information as possible on security in plain language for consumers. Security information and privacy policy statements should be accessible in the following locations:

- Device user manual/instructions
- Company website
- On the app that controls the device
- Support forum
- Help center (online, or call-in)

For more information and user-friendly tips on cyber security for your business, visit the United States Computer Emergency Readiness Team at https://www.us-cert.gov/ncas/tips.

GETCYBERSAFE.CA