# Cybersecurity and the dangers of the Internet of Things

October 31, 2022

## Authors

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Selena Lu

Partner, Lawyer

While the Canadian government has said it intends to pass legislation dealing with cybersecurity (see Bill C-26 to enact the *Critical Cyber Systems Protection Act*), many companies have already taken significant steps to protect their IT infrastructure. However, the Internet of Things is too often overlooked in this process.

This is in spite of the fact that many devices are directly connected to the most important IT infrastructure for businesses. Industrial robots, devices that control production equipment in factories, and devices that help drivers make deliveries are just a few examples of vulnerable equipment. Operating systems and a range of applications are installed on these devices, and the basic operations of many businesses and the security of personal information depend on the security of the devices and their software. For example:

An attack could target the manufacturing equipment control systems on the factory floor and result in an interruption of the company's production and significant recovery costs and production delays.

By targeting production equipment and industrial robots, an attacker could steal the blueprints and manufacturing parameters for various processes, which could jeopardize a company's trade secrets.

Barcode scanners used for package delivery could be infected and transmit information to hackers, including personal information.

The non-profit Open Web Application Security Project (OWASP) has released a list of the top ten security risks for the Internet of Things.[1] Leaders of companies that use this kind of equipment must be aware of these issues and take measures to manage these risks. We would like to comment on some of the risks which require appropriate policies and good company governance to mitigate them.

**Weak or unchangeable passwords:** Some devices are sold with common or weak initial passwords. It is important to ensure that passwords are changed as soon as devices are set up and to keep tight control over them. Only designated IT personnel should know the passwords for configuring these devices. You should also avoid acquiring equipment that does not allow for password management (for example, a device with an unchangeable password).

**Lack of updates:** The Internet of Things often relies on computers with operating systems that are not updated during their lifetime. As a result, some devices are vulnerable because they use operating systems and software with known vulnerabilities. Good governance includes ensuring that such devices are updated and acquiring only devices that make it easy to perform regular updates.

**Poor management of the fleet of connected devices:** Some companies do not have a clear picture of the Internet of Things deployed in their company. It is crucial to have an inventory of these devices with their role in the company, the type of information they contain and the parameters that are essential to their security.

**Lack of physical security:** Wherever possible, access to these devices should be protected. Too often, devices are left unattended in places where they are accessible to the public. Clear guidelines should be provided to employees to ensure safe practices, especially for equipment that is used on the road.

A company’s **board of directors** plays a key role in cybersecurity. In fact, the failure of directors to monitor risks and to ensure that an adequate system of controls is in place can expose them to liability. Here are some elements of good governance that companies should consider practising:

Review the composition of the board of directors and the skills matrix to ensure that the team has the required skills.

Provide training to all board members to develop their cyber vigilance and equip them to fulfill their duties as directors.

Assess cybersecurity risks, including those associated with connected devices, and establish ways to mitigate those risks.

The *Act to modernize legislative provisions respecting the protection of personal information* sets out a number of obligations for the board of directors, including appointing a person in charge of the protection of personal information, having a management plan and maintaining a register of confidentiality incidents. For more information, you can read the following bulletin: Amendments to Privacy Laws: What Businesses Need to Know (lavery.ca)

Lastly, a company must at all times ensure that the supplier credentials, passwords and authorizations that make it possible for IT staff to respond are not in the hands of a single person or supplier. This would put the company in a vulnerable position if the relationship with that person or supplier were to deteriorate.

---

1. See OWASP top 10