BUSINESS IOT SECURITY AND PRIVACY GUIDE

Protect your customers and corporate IoT data from compromise.

Release: April 2017

This guide exists a result of the Public Safety Canada Cyber Security Cooperation Program (CSCP). Using our proprietary testing techniques, TwelveDot Labs was engaged to research the risks and impact on Canadian consumers and business who use insecure IoT products and services.

This guide presents the findings and recommendations of this research. We hope that you will find the content helpful and easy to understand and implement. If you find that you do have questions on the content you can reach out us on the following channels.

E-mail	Twitter	LinkedIn
security@twelvedotlabs.com	TwelveDotSecurity	TwelveDot

Internet of Things (IoT) has been around for decades but now with the advances in microelectronic manufacturing, it allows a multitude of sensors and actuators to be accessed and supported via the Internet.

The 3 tenants of information security; Confidentiality, Integrity and Authenticity still apply to IoT, however, depending on how they are applied, they can become an issue of safety. Safety is typically considered in the Industrial sector but with healthcare, agriculture, and other sectors, a failed sensor can now result in harm to humans.

Businesses need to be able to quantify the risks of their IoT systems, service providers, component vendors and in-field support teams. Risk will take many forms and managers will need to be vigilant to quantify and assess risk using a system-of-systems approach to risk management. The ability to qualify this risk will provide the necessary due diligence to determine liability post-compromise.

This guide outlines systems that must be considered and quantified when a risk assessment is being conducted. IoT systems can be complex and will consist of several providers, systems, components, and even staff.

Currently, many devices that are compromised on a IoT network are being used as a pivot point to attack other services on the network or are weaponized to attack 3rd party sites and even foreign governments. Having strong risk management practices that ensure that all risk is identified and mitigated to required minimums is key to your success.

One approach to understanding IoT from a security and risk perspective is the concept of “system-of-systems”. In this context, you need to first evaluate each system independently and then look at each linkage both from a process and logical perspective between each other system until all linkages are identified. Then and only then you can truly threat model and understand the risks of an IoT system.

Using the system of systems an evaluator should considered the following a minimum when evaluating a solution, product or service from an IoT provider:

1. A Risk Management Practice that is part of an Information Security Management Systems (ISMS) or other formal security risk mitigation process within the entire organization. It should start with senior executives and trickle down to lowest members of staff who have access to confidential business information.
2. Software Development Lifecycle (SDLC) of vendor should have security and privacy aspects built into their SDLC. This is easily validated with risk assessments, privacy impact assessments, and product documentation.
3. Threat and Vulnerability Management processes and procedures
4. Human Resources policies and practices

5. Incident Handling Management
6. Asset and Operational Management
7. Supply Chain Management
8. 3rd Party Supplier Management
9. Adherence to updated PIPEDA legislation in Canada

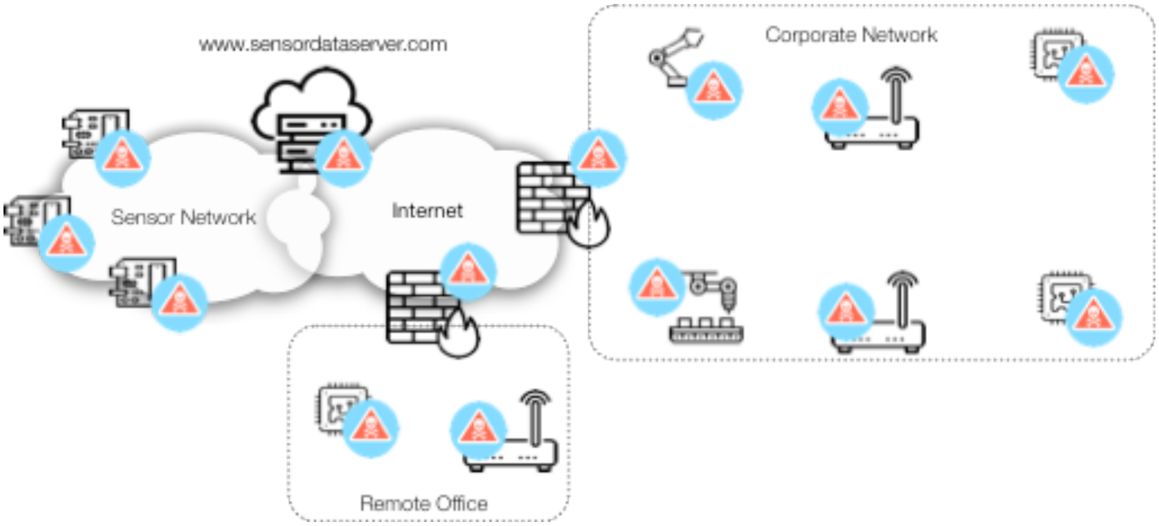

Figure 1: IoT Danger Zones

Figure 1 identifies many of the IoT danger zones of businesses. Businesses need to better quantify their risks across all systems that compromise their corporate networks and IoT networks. As many businesses are now using aspects of smart building to monitor facilities, air quality and climate control, knowing the risks to the sensors and actuators becomes critical.

Risks

The biggest risk to a business is due to a data breach or compromise of the IoT data. As a result of data breach the following aspects need to be considered:

1. Loss of confidence in product vendor and supplier(s)
2. Loss of reputation for vendor
3. Potential lawsuit for negligence or other failure to protect or notify users during a data breach
4. Failure to report a data breach under PIPEDA
5. Rogue IT that stored confidential data on known servers typically on foreign soil
6. The weaponizing of your IoT network to attack either your corporate network or other 3rd party sites

Preparing your organization for IoT Risks

Before purchasing any solution, component or service, you must first determine the data at risk for your IoT solution. Once you understand the data you will be collecting, processing and storing, you will be in a better position to understand the controls that will be required to protect it and the danger of this data being compromised.

1 Implement an ISMS to better understand your data at risk and how best to mitigate the risks specific to your organization. These systems greatly help employees and shareholders better understand the importance of security and privacy to your organization.

2 Implement a security risk management practice that will identify cyber risk for all projects that have a technology component.

3 What critical data will be collected, processed, and stored by your IoT product/solution being considered for deployment? Typically this is determined when a Threat and Risk Assessment (TRA) and Privacy Impact Assessment (PIA) has been conducted.

4 Create the set of policy and procedures that will clearly make employees, partners, and 3rd party providers understand your security requirements for IoT implementations

5 Make sure you understand PIPEDA and how it impacts your organization

Evaluating vendors and 3rd party products and services for risks

Now that you understand how to better protect your organization and data, you must turn your attention to understanding the risk that might exist when building your IoT solution using a vendor or 3rd party organization. Vendors and solutions providers should provide a basic level of assurance to protect against easy exploitation of their products and services in-field. When comparing vendors for security, remember more is better. The more information and assurance a vendor can provide around their security and privacy position, the better for you and your customers who will depend on these solutions for revenue.

1 Does the solution vendor have a secure SDLC? Can they prove it?
2 Has the product/service undergone any formal security testing or evaluation? What reports can they provide to substantiate these claims
3 Has the service provider undergone any formal certification such as ISO, PCI-DSS, FIPS, Common Criteria or other equivalent formal assessment? Self-assessments may provide a view of the security controls but they tend to put the vendor in a positive light where security and privacy are concerned.
4 Ensure all devices and components have the ability to be field upgradable for firmware and can be securely monitored for availability and functional operation.
5 Does the vendor have a vulnerability disclosure program and privacy policy publically posted on web site?
6 Does the vendor have either a security white paper or best practice guide for deploying their technology securely?
7 Check the CVE listing to determine how many known vulnerabilities currently exist for the vendor? This will provide a good preview the current risks of the solution but provides an early view of the code quality of the vendor.
8 Does the vendor have a security mailing list?

What to do to greatly reduce your exposure:

1. Conduct a TRA with the following scope:
    a. Full system analysis
    b. Vendor 3rd party libraries
    c. Vendor CVEs related to product and components
    d. In-field upgradability of solution
    e. Tamper resistance of the solution
    f. User account administration
    g. System and solution monitoring for attack and compromise
    h. Sign up for vendor security mailing list and alerts
2. Determine the residual risk of the system and then determine if you might need cyber insurance to protect against this risk
3. Do you have an incident handling process? If not, get this created and implemented. This includes training all staff who will need to support this effort, including engaging legal and public relations teams.
    a. Create a flow chart that:
        i. Identifies data at risk for IoT solution. What is the worse case scenario if this data was compromised and exposed to the

      public. What would the possible impact be to your company, your customers and potential customers?
   ii. Identifies all systems to be considered
b. For each system
   i. Determine best practice or standard to be used for control implementation
   ii. What controls are required
   iii. How will you detect a failure in this control?
   iv. How will you detect a failure in this system?
   v. How can you mitigate risks, if at all?

4. Document, document, document! Ensure you create documentation that clearly outlines the risk management process and what was done to evaluate and mitigate those risks. This can include supporting information from vendors, service providers and others who will provide the service to your organization.

Further supporting information on security and privacy risks can be found at the following sites:

1. CVE – The Vulnerability list
2. BugTrak – List of known security issues with software. Good starting point to track down unknown or unclassified vulnerabilities
3. Public Safety Canada – The Cyber Security site for PS has several publication that would helpful for Small and Medium Businesses better deal with the cyber security challenges.
4. PIPEDA – New legislation scheduled to be enacted in Fall of 2017 for all business regardless of size or nature of business.

Acronyms

CVE	Common Vulnerabilities and Exposures
GPS	Global Positioning System
ISMS	Information Security Management System
HTTPS	Hypertext Transport Protocol Secure
PIA	Privacy Impact Assessment
PIPEDA	Personal Information Protection and Electronic Documents Act
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSID	Service Set Identifier
TRA	Threat and Risk Assessment
VPN	Virtual Private Network