# CEAWG Evaluation of Existing Educational Resources

## Canada:

1. Wearable devices and your privacy
   a. Some proposals are unrealistic and a consumer will likely make tradeoffs in favor of convenience/functionality.
   b. Too broad to be applicable.
   c. Steps are easy to follow and content actionable.
2. Privacy and the Internet of Things
   a. Same as first.
3. Get Cyber Safe Blog
   a. Navigation is poor and material is unclear.
4. The Internet of Things
   a. Cites specific incidents.
   b. Graphically presented and easy to follow.
   c. Succinct enough that people may share it with friends and family.
   d. Links to many other resources at the bottom.
   e. Video format allows for distributing via playback in public spaces.

## International:

1. Online Trust Alliance resources for smart home users
   a. IoT Security & Privacy Checklist – Press Release
   b. Smart Home Checklist, Advice for Buyers, Sellers & Renters (Updated March 2017, PDF)
   c. Considerations When Buying & Setting Up A Connected Device (PDF)
   d. Enterprise IoT Security Checklist
2. Stop Think Connect (Department of Homeland Security)
3. OnGuard Online – Set of consumer-friendly resources and videos (Federal Trade Commission)
4. What To Do After A Data Breach (Federal Trade Commission)
5. Tax Payer Guide To Identity Theft (IRS)
6. Protect Your Privacy Online; Educating Washington Residents On Privacy In The Digital Age (State of Washington)
7. Online Tips & Advice (Washington State Attorney General)
8. Consumer Federation of America
9. Consumerman
10. Better Business Bureau – Consumer Resources

11. Identity Theft Risk Calculator (LifeLock)

12. Field Guide To Home Automation (National Association of Realtors)

13. Identity Theft Resources (Identity Guard Resource Center)

14. Top Tips for Consumers: Internet of Things Security and Privacy (Internet Society)

15. StaySafeOnline

## General Feedback

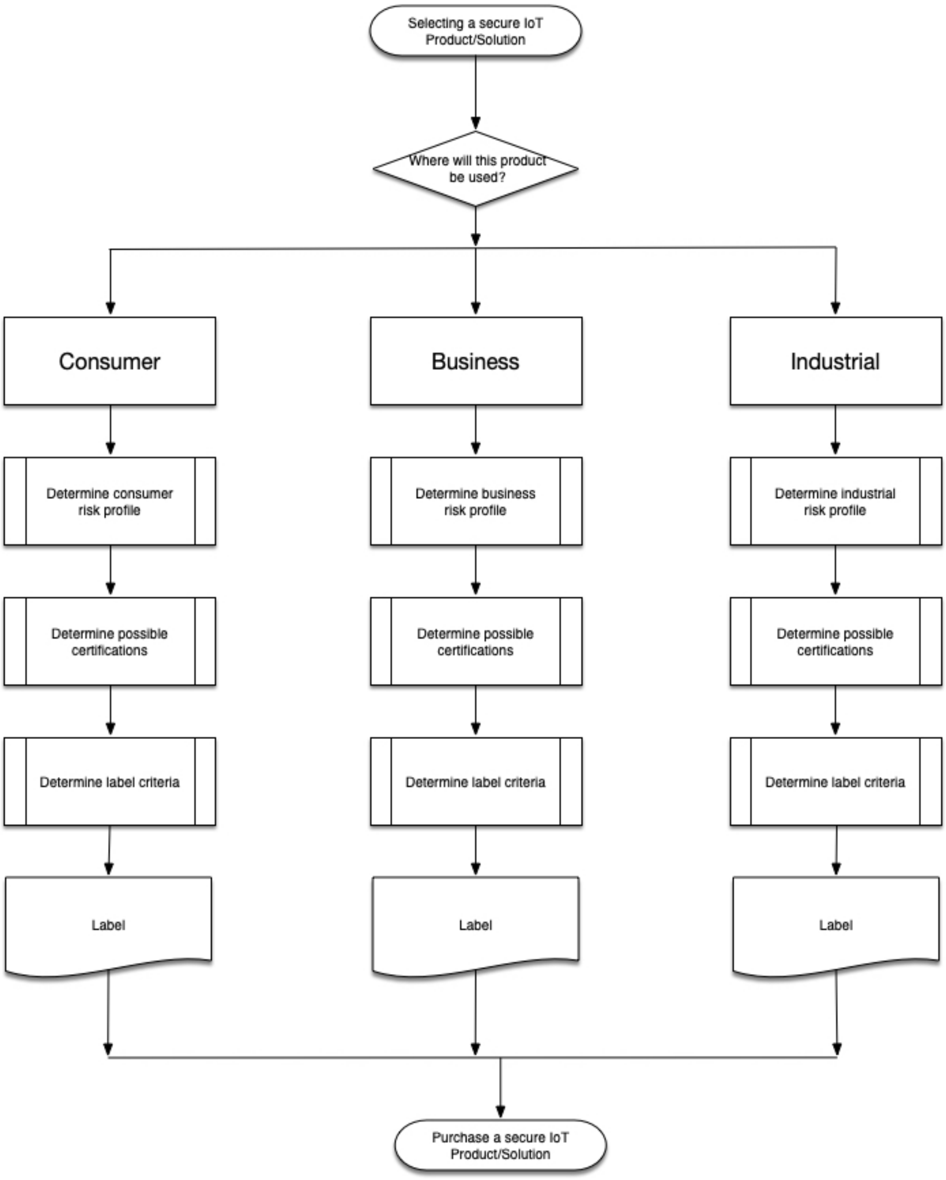
1. Accessibility
    a. Do we know how many people actually seek these resources and read them?
    b. Are there active efforts to promote this information?
2. Framing
    a. Much of the content takes the approach of "these are the steps that a user can take and devices will be magically secure," versus "this is how device security works and the user can start asking what should be done". The former is simple because it requires minimal effort, but the latter is more engaging: rather than carrying out some steps to feel a little more secure, the consumer develops a security mindset that is more likely to go viral, as they are more likely to share this knowledge and have discussions with friends about security.

The Device Labeling Working Group also collected some information on the way consumers interact with IoT devices and how specific labels may better inform their decision making. That research is included below.

Users are increasingly attentive to the handling and use of their data across all devices, especially consumer IoT products that have not traditionally been Internet-enabled (appliances, HVAC, lighting, etc.). However, users are faced with a volume of available conflicting information. Therefore, a decision-making model can be provided to help users and businesses identify and assess any labeling used on an IoT device. The model also illustrates that there are different risk aspects of IoT devices in other sectors. The following diagram provides the necessary guidance for each user group to best determine the labels that should be considered.

## Where will the product be used?

Many IoT solutions target three separate sectors: consumer, business, and industrial. These three sectors represent three very distinct risk profiles for the end user. Recognizing that these risks exist and must be used as differentiators will help the vendor and buyer of these solutions to meet label requirements. While this report considers the industrial sector, the focus is on the consumer and business sectors.


Selecting a secure IoT Product/Solution
Where will this product be used?
Consumer
Business
Industrial
Determine consumer risk profile
Determine business risk profile
Determine industrial risk profile
Determine possible certifications
Determine possible certifications
Determine possible certifications
Determine label criteria
Determine label criteria
Determine label criteria
Label
Label
Label
Purchase a secure IoT Product/Solution

## Risk Profiles

In order to make informed buying choices, consumers should be able to consider and evaluate the risks of an IoT solution as opposed to a non-connected alternative. Consumers should be able to develop a 'risk profile' for any device.

The following criteria consider some of the high-level risks that are associated with each level of product category. The only way to fully quantify the risk of an IoT solution would be to conduct a formal security assessment or Threat and Risk Assessment (TRA) against the solution for each sector.

Buyers should, at a minimum, attempt to answer the following questions to determine the risk of exposure. Lack of details from a vendor should be considered as not implemented. Buyers should never assume that security and privacy have been implemented to protect their interests and/or data.

### Security attributes that need to be considered when evaluating a product:

1. **Confidentiality:** Can the vendor provide details of how the design of the solution or product will protect the confidentiality of the data being collected, processed, and stored?
2. **Integrity:** Can the vendor provide details of how the design of the solution or product will protect the integrity of data being collected, processed, and stored? This includes integrity of the device or solution when under attack or potentially compromised.
3. **Availability:** Can the vendor provide details of how the design of the solution or product will protect or ensure that device or solution will be available when and how the consumer wants to access and use it?
4. **Safety:** Can the vendor ensure the product will function as anticipated and not become a hazard due to a device failure that may cause fire, electrocution, burning, melting, emitting of harmful vapor, or emitting harmful radio signals?
5. **Reliability:** Can the vendor provide details of how the device or solution will ensure that it will provide a specific or targeted state of being reliable?

These attributes of the features implemented in a device or solution provide a context or approach for consumers to evaluate and select IoT products, as outlined below.

### Minimum attributes that a vendor should have regardless of product and service:

1. **No default user accounts and passwords:** Upon the setup and configuration of a new device, the device should force the setting of a new password for the device. This password should follow best practices for strong passwords.
2. **The device should be secure out-of-the-box:** New devices should be configured in a state that protects the consumers from having to learn to configure how best to secure the device.
3. **Vendor should clearly outline their privacy practices:** The vendor should provide details of data being collected, processed, and stored for service users. This includes data breach protocols and third parties that are provided this data for free or as a revenue stream for the organization.
4. **Devices and solutions should be formally tested prior to release:** The solution including the device should be tested for the presence of known and potential vulnerabilities.
5. **Vendor should have a vulnerability disclosure process:** The vendor should have a process within the organization that will permit the reception of a potential vulnerability and the ability to perform a vulnerability disclosure in the event a vulnerability is confirmed in their solution.
6. **Encryption technology should be peer reviewed and based on standards:** Vendors should not be developing proprietary encryption technologies but use those that have been peer reviewed and based on standards to ensure interoperability. This may include solutions for protecting data communications but also the boot process and data storage.
7. **Solution should have a secure update method:** The vendor should provide a secure method to provide updates to the device. This may include checks to ensure that the firmware has not been tampered with prior to installation.
8. **Vendor should provide specific dates for product support:** The vendor should be clear and concise about the date or period that a product will be supported with software updates. When possible, users should be notified that a product has reached it end-of-life for software support.

These attributes will guide customers to make better informed decisions when buying an IoT product or solution. The following table outlines potential threats and additional considerations that will help to determine if a product or vendor might pose a cyber risk.

| Profile | Category and Threats | Considerations |
|---|---|---|
| Consumer | Data breach, device compromises, account compromises, and weaponizing of devices. | • Lack of security and privacy requirements and considerations for the solution.<br>• Implementation errors for SSL and other crypto-related technologies due to lack of expertise.<br>• Lack of a formal SDLC that mitigates risks to acceptable levels.<br>• Lack of formal security testing and evaluation including third party assessments and attestations.<br>• Vendor's lack of governance for security and privacy.<br>• Vendor's failure to knowingly report a data breach.<br>• Privacy policy not clear on data aspects collected, processed, and stored by the vendor, including the selling of this data collected to third parties. |
| Business | Data breach of infrastructure, account compromises for users and administrators, weaponizing of infrastructure and devices, source code and firmware compromises. | • Failure to risk assess the IoT solution both at design and implementation stages.<br>• Failure to correctly define the security and privacy requirements for IoT solution.<br>• Lack of governance to oversee the implementation of a solution.<br>• Policies and procedures that do not include incident handling during data breach situations.<br>• Failure to identify either a data breach, device compromise, or user account compromise. |
| Industrial | Secure operation of device in-field and compromises of management infrastructure. | • Lack of SDLC that includes security and safety testing.<br>• Lack of governance to oversee the secure design of a solution.<br>• Threat modeling for both green field and brown field implementations.<br>• Real-time monitoring of management and control infrastructure, including incident handling. |

## Possible Certifications, Marks, and Testing

Currently, there are no formal testing standards specifically for IoT products/solutions. Buyers are left to determine the security of a product typically based on vendor reputation or the recommendation of friends. Consumers typically care about the usability, not the security and privacy aspects of these solutions. However, once a data breach or device compromise has occurred, they are usually left to figure out the situation on their own. Providing the following details will hopefully help consumers purchase a product that meets both security, privacy, and functionality needs.

| Sector | Certification | Considerations |
|---|---|---|
| Consumer | Electrical | • Where was the device manufactured? Some regions require products to undergo electrical certification, which may include the CE mark.<br>• The CE Mark is used in the EU to illustrate products that have been formally evaluated to the EU requirements for electrically powered products. While not security focused, it provides a means to show the vendor has undergone formal assessment by a regulatory framework and does have a minimum level of maturity for organizational processes. |
| | Safety | • If this device were to have a failure such as overheating, not turn off, not turn on, accessible remotely without authority, have connection ports that allow modifications, does not provide load protection or surges, would these have an impact on the buyer?<br>• Look for IEC 15208 to ensure that the product has been assessed for safety. |
| | Quality | • Do you want to purchase a product that has been produced by an organization that has been evaluated for having a quality management process in place?<br>• Look for ISO 9001 or ISO 14001. These symbols indicate formal assessment for process and manufacturing assurance for the vendor. |
| | Security | • Do you want to purchase a product that has undergone security and product testing?<br>• Look for the BSI Kitemark to represent organizations whose product has undergone formal testing and assessment for security and other attributes. It also includes an ISO 9001 audit to ensure the vendor meets certain criteria prior to attaining this accreditation for a product.<br>• UL 2900 also provides a means to determine that a product has undergone a formal product assessment. While the vendor's processes other than development are not considered, it still provides a means to determine that a minimal level of assessment has been completed for a product. The current standard does not have any requirements for privacy. |
| | Security Penetration Testing | • Do you want to purchase a product that has been security stress tested?<br>• Look for indications either on the website or product documentation that penetration tests have been conducted.<br>• Note of caution: Not all penetration tests are equal as there are no formal standards on methodology or tools. As such, it can be a one-and-done approach versus a continuous improvement program within the organization. |

| Sector | Certification | Considerations |
|---|---|---|
| Business | Electrical | • Same as consumer |
| | Safety | • Same as consumer |
| | Security | • Do you need to have a product that will provide a level of assurance for operating environments, such as government, telecommunications, or high-risk operating environments?<br>• Look for Common Criteria ISO 15408 with protection profiles that align to the product base functionality.<br>• UL 2900 Series can also be used to determine if a product has been assessed for specific security design features and flaws. Privacy is not included in this assessment. |