# Secure IoT: Labels to Empower Consumers

ISOC Multistakeholder Process – Labelling Group

Editors: Faud Khan and Dr. Hosein Badran

Edition Date: January 18, 2019

Objective:

Safe use of connected devices and associated data streams through the provisioning of clarity on what they do. Labels can “help consumers make smart choices” when it comes to acquiring, using and disposing IoT devices. For this, consumers need to be able to rely on the information provided through a product security label, and the information needs to cover the key aspects buyers are to take into account. Through consumers making smart choices, we believe that the Canadian IoT environment will develop in a safer, more secure way, taking privacy and security into account from the outset. Consumers making smart choices results in manufacturers and business offering better and more secure solutions. Ultimately, this will lead to a higher level of network resilience, both from a societal and from a personal perspective. Consumer education at all levels will need to empower consumers to make the best use of the information provided through the labels.

Key aspects of effective labeling

1. content – providing reliable, relevant and useful information when it is needed;
2. coverage – ensuring that all consumers of all competing products see the information;
3. uniformity – use of a single simple and recognizable design to facilitate comparison.

| Document History | | |
|---|---|---|
| Version | Detail | Editor |
| Initial Public Draft v1.0 | Jan. 18 | Faud Khan & Hosein Badran |
| | | |

## Problem Statement

What labels and/or characteristics of an IoT product/solution does a buyer either consumer or business need to consider when purchasing a product? These characteristics should include aspects of user functionality, security, privacy and safety at a minimum.

# Relevant Research

## Labeling

The sections that follow provide the research and information that was identified over the course of the project. These details were discussed and reviewed for applicability to Canada and as discussion points at the meetings that were held over the project period. We are including them here as a summary review and consideration for labeling requirements.

1.1 The need for a labeling scheme for consumer IoT devices

In Oct. 2018, PETRAS IoT Hub, the Dawes Centre for Future Crime at UCL, and as part of the United Kingdom's "Secure by Design Review" for consumer Internet of Things products, published the report "Rapid evidence assessment on labeling schemes and implications for consumer security" [1].

As mentioned in the report, consumers are not able to distinguish between devices that offer good and inadequate security when making purchasing decisions. Actually, consumers have to investigate the security features and capabilities of the product themselves before purchasing. This would involve evaluating technical information such as what data is collected by the device and how it is shared, security standards compliance, the length of support, and default password configuration.

Awareness campaigns and behavior change interventions can encourage consumer behavior and motivate consumers to routinely assess the security of IoT devices they consider purchasing. However, research has shown that such intervention will not be sufficient to have real impact on consumer decisions when buying an IoT product [1]. A key reason is that manufacturers do not routinely display information about the security features of their products that would need to be evaluated to determine their level of security. Also, the average consumer will not have the knowledge required to evaluate this information, and typically is inclined to avoid cognitively demanding tasks, as per relevant research [2].

Hence, a more achievable intervention that could impact consumer choice would be in the form of a label that consumers can relate to and that would inform their decision making in a meaningful way.

As mentioned, manufacturers do not provide correct or accessible information to inform consumers and retailers about the level of security their devices offer. A labeling scheme would encourage manufacturers to compete on security as a form of market differentiation. It would also promote attention to be directed to the security of devices and for this to be done against clear criteria and guidelines, hence holding manufacturers to account. Finally, a labeling scheme would allow market oversight and consumer protection authorities to assess compliance to IoT security in a more transparent and consistent approach [1].

1.2 Types of labeling formats

The report identifies three different types of labeling formats:

- Descriptive information label: it details security-related information.
- Binary seal of approval label in which a product is certified to a standard.
- Graded scheme label that allows more critical comparisons of security-related compliance.

In order to provide more insight into the relative merits of the different types of labeling, it is useful to refer to critical research performed on well-established labeling schemes, particularly on the food labels and the energy efficiency labels [1].

1.3 Energy Efficiency Labels

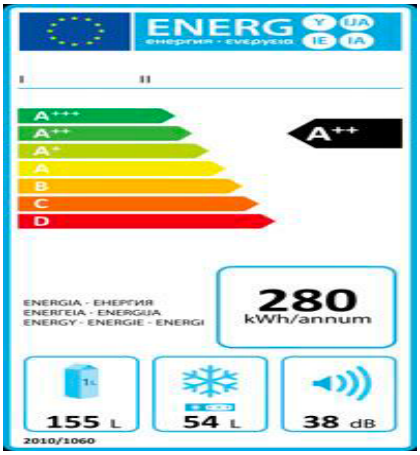



*Figure 1. Energy Efficiency label*

| Refrigerating appliances, as EEI | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| A+++ | A++ | A+ | A | B | C | D | E | F | G |
| <22 | <33 | <42/44 | <55 | <75 | <95 | <110 | <125 | <150 | >150 |

*Figure 2. Label categorization for refrigerators*

The report explains that in 1995, the EU introduced the Directive 92/75/EC that was updated as Directive 2010/30/EU, and it outlines an energy consumption labeling scheme to be displayed on electronic products, as shown in Figure 1 (http://www.charltonandjenrick.co.uk). In 2010, a grading scheme (A+, A++, and A+++) was introduced, following developments in energy efficiency standards. It is mandatory for manufacturers to display energy efficiency labels for certain classes of product, including refrigerators, televisions and dryers (Figure 2).

The EU directive requires manufacturers to provide the labels for free to dealers, and include a performance table in brochures and associated documents.

A challenge for consumers in dealing with the energy efficiency label A+++ to G is that it is quite product dependent. For example, for televisions the label encompasses A+ to F, and for coffee machines they use the scheme from A to G. As for washing machines, in 2010 all machines that were in label category A were prohibited. Then in order to drive market shift, all future washing machines needed to be in the A+ to A+++ range.

As mentioned in the report, these distinctions are generally invisible to the consumer and lead to confusing the consumer among product lines.

Also, the introduction of A+ to A+++ grading has diminished the effectiveness of the label as it became difficult for consumers to identify the difference between A+ to A+++ as the same as A to G. Consumers are generally not willing to make the additional investment to buy an A+ or A++ rated product, and settle for an A product as being good enough.

1.4 Food Labels

As per the PETRAS report [1], food labeling aims at enabling consumers to make healthier food choices and reduce levels of obesity. The European Commission regulates the provision of food labeling, requiring pre-packaged foods to label their nutritional content (EC No. 1169/2011). Labeling on the back of a food package is mandatory, while manufacturers can opt to place labels on the front-of-pack (FOP). FOP labels must display portion values for key risk areas (salt, sugars, saturates, and fat).

There are three types of FOP labels. The first are Guideline Daily Amount (GDA) shown in Figure 3 (https://www.foodlabel.org.uk). Figure 4 shows the GDA scheme with colored traffic light system and is approved by the UK Food Standards Agency (https://www.food.gov.uk). The third FOP type is a health logo, which is basically a “seal of approval” scheme, granted with the food product is proven to meet particular nutritional requirements and/or standards. Figure 5 shows the European Union organic food logo, which came in effect in 2012, and is compulsory on all pre-packaged organic food products produced in the EU and meet specific standards (https://www.foodnavigator.com).

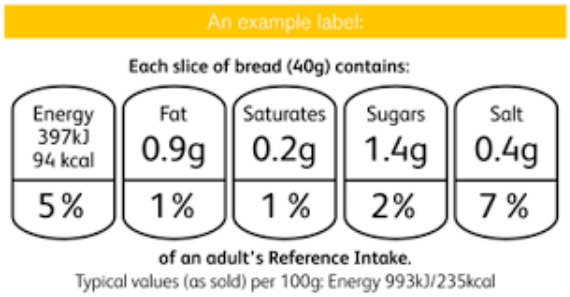



*Figure 3. GDA label*


*Figure 4. GDA label with traffic light system*

*Figure 5. EU organic food logo (Binary food logo)*

Research has shown that the display of FOP labels has increased healthy product choice by 18% [3]. Little consensus exists on the most effective FOP labeling scheme [1].

Research on GDA has shown that consumers find it difficult to identify the nutrient content, while more recent research has indicated that it helps consumers identify healthier products [4]. On the other hand, a number of studies have shown that the traffic light FOP scheme facilitates more healthy food choices, compared to other FOP labeling schemes [3].

Health “seal of approval” logos are preferred by consumers due to their simplicity [4] and have been found to reduce the time consumers spend in examining the food packages, as the format is quite intuitive.

In summary, there are clear benefits to a FOP label in aiding consumer choice, with each format offering it own limitations and strengths. Consumers tend to prefer a binary label, however this may lead to rushed purchase decisions and research indicates that traffic light systems help consumers make better judgments and are marginally more effective in driving a healthier product choice.

The success of any of the food label schemes will be limited by the consumer’s attention at the point of sale. Often, consumers are rushed and focus on trading off brand, convenience and taste when making product choices [5].

1.5 Possible IoT Device Security Label

In terms of the possible IoT device security label formats, as explained above, each of the known three labeling schemes has its strengths and weaknesses [1].

The colored graded scheme would attract the attention of consumers and help them compare the security of different devices. For this implementation to be effective the display of the graded label needs to be mandatory for manufacturers.

The Binary or “seal of approval” label is typically preferred by consumers due to its simplicity, but is less effective in guiding attention and informing consumer choice [6]. Care should be given as the use of the binary label may lead consumers into a incorrect sense of security or expect that it requires no actions from them to keep safe and secure.

The descriptive information label provides critical information to consumers and may provide helpful indicators of a device's security readiness. The label needs to communicate the most relevant information only and not burden consumers with unnecessary information. This type of label is more suitable for the voluntary label introduction.

### 1.6 Mandatory and voluntary labels

The Department of Digital, Culture Media and Sport (DCMS) of the UK, released their policy review for Secure by Design for consumer "Internet of Things (IoT)" products, in March 2018 [7]. A key measure in the report is a voluntary code of practice for manufacturers to ship products with features that make them "Secure by Design". The report also proposed exploring the role of a voluntary labeling scheme to communicate important information to consumers that is otherwise invisible to them, or difficult to find, such as how data collected by devices is shared and the support period for the product [7].

A voluntary labeling scheme would be useful as an initial step, but for a sustainable market growth and to ensure manufacturers adherence, as well as to maintain consumer awareness, it will be necessary for the label to be mandatory to be effective. It is feared that manufacturers may be unwilling to display a label that indicates poor security of a product.

### 1.7 QR Codes

A QR code is a type of matrix bar code or two-dimensional code that can store data information and designed to be read by smartphones. QR stands for "Quick Response" indicating that the code contents should be decoded very quickly at high speed. The code consists of black modules arranged in a square pattern on a white background. The information encoded may be text, a URL or other data [8] [9]. The QR code was designed to allow its contents to be decoded at high speed.

QR Codes were created by the Toyota subsidiary Denso Wave in 1994, and were initially used for tracking inventory in the manufacturing of vehicle parts [10].

The popularity of QR codes is growing rapidly all around the world. Nowadays, mobile phones with built-in camera are widely used to recognize the QR Codes.

#### 1.7.1 QR codes usage statistics

The use of code scanning has gone up during the past years, as awareness and adoption of QR Codes grow exponentially. QR code stats done by ScanLife show that 23 million QR codes are scanned during the first quarter of 2015, which is nearly 10 million more than during the first quarter of 2012, and the first quarter of 2012 had posted a 157 percent increase as compared to the first quarter of 2011 [11].

| **Users who scan QR codes in the first quarter of the several years** | |
|---|---|
| Year | Users |

| | |
|---|---|
| 2011-Q1 | 7.5 millions |
| 2012-Q1 | 13.3. millions |
| 2013-Q1 | 18.2 millions |
| 2014-Q1 | 21.8 millions |
| 2015-Q1 | 23.1.millions |

*Table 1. Global QR codes usage by ScanLife [11]*

According to a recent survey by Statistia, in the US alone, an estimated 11 Million households will scan a QR Code in 2020, as shown in Figure 6. This is an increase from an estimated 9.76 Million scans in 2018 [12]. Hence there is a huge potential for US manufacturers and marketers who are considering adding a QR Code to their print media campaigns.

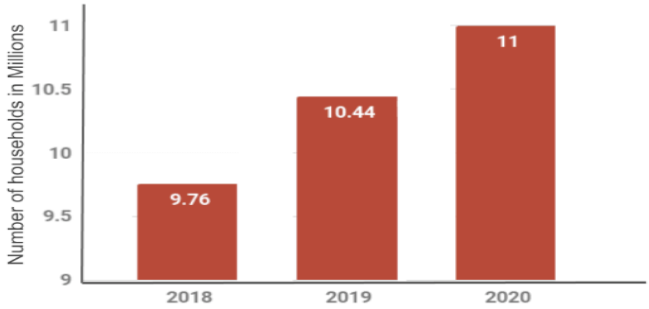



*Figure 6. QR Scans in the US*

According to a 2015 study by ScanLlife, the distribution of global QR code scanning by age is shown in Figure 7 [12].

The age group with the highest percentage of people scanning QR Codes was 34-44 years. Again note that this was in 2015. Since then apps—popular with the younger generation—such as Snapchat, Pinterest, and WeChat—have added QR Code scanning features. This shows that this age distribution in 2018 is likely to shift towards the younger generation [12].

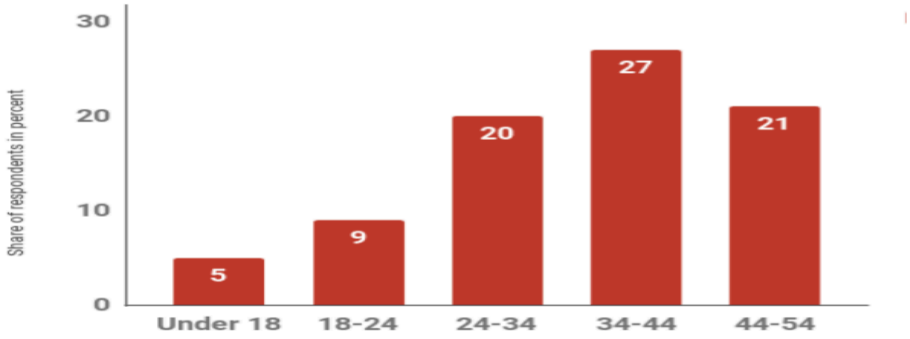



*Figure 7. QR Scans age distribution*

In Canada,

- 27.4 million Canadians are on line representing 80% of the population.
- 93% go online to view and verify product information.

These figures have changed the way Canadian marketers and retailers engage their audience. To strike a chord with the young generation, marketers, retailers, manufactures and even the police have adopted QR Codes in Canada.

### 1.7.2 Relevant Use Cases for QR Codes

The use cases of QR codes vary widely and cover different areas from marketing, product packaging, advertising, special causes, customer surveys, and much more.

Below, three use cases of QR codes are presented, that focus on providing product information particularly in the ICT (information and communications technology) domain [13].

*HP Use Case*

HP sought after a practical and interactive way for customers to receive details on their products right from the package. They wanted potential customers to more easily understand what they were purchasing, and what accessories, like ink packages, were required for each.

HP used ScanLife activated codes extensively on most of their consumer printer line around the world. The codes told customers more about the products and gave them details on accessories which made it easier for shoppers to buy products, especially during the busy holiday season when retail associates were difficult to find.


*Figure 8. QR codes used by HP*

*Staples Use Case*

Staples had a variety of goals for its mobile marketing campaign: To show value for the consumer while also helping the business achieve key sales milestones. However, their ultimate objective was to increase overall conversions through the use of an effective in-store campaign. Staples incorporated QR Codes into its in-store displays.


*Figure 9. Staples mobile marketing campaign using QR codes*

*Keurig Use Case*

Keurig wanted to give customers more dynamic information on all of their products; from K-Cup brewers to K-Cup flavors. Keurig utilized QR Codes as a flexible tool, and needed a centralized code management platform to work across multiple divisions within the organization.

Dynamic codes were generated for Keurig products allowing the experiences to be adapted in real-time. Once scanned, the codes educated consumers on the product of interest. It provided them with product information, a video tutorial of how the product works, and an explanation of why everyone should have a Keurig in their home or office. The campaign helps shoppers decide what Keurig brewing machine was best for them without interacting with sales associates.


*Figure 10. Selecting Keurig coffee machines utilizing QR codes*

## Standards

As many standards are being developed by many groups, the scope and jurisdiction for these documents tend to confuse consumers. The buyer must consider how he will use this product and the potential risks involved before determining the best documents to consider. This also speaks to the current fragmentation and lack of industry wide collaboration on security and privacy across standards development organizations (SDOs) and trade associations not just in North America but globally.

## Best Practices and Standards

Below are the key referenced standards by the DCMS report "Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security" [14]. They are provided here as reference only as users will need a means to determine risks prior to purchase (Table 2).

| **Organization** | **Standard / Recommendation** |
|---|---|
| European Union Agency for Network and Information Security (ENISA) | Baseline Security Recommendations for IoT |
| GSMA | IoT Security Guidelines for Service Ecosystems |
| IEEE | IoT Security Principles and Best Practices |
| Internet Engineering Task Force (IETF) | Best Current Practices (BCP) for IoT Devices |
| IoT Security Foundation | IoT Security Compliance Framework 1.1 |
| IoT Security Initiative | Security Design Best Practices |
| Online Trust Alliance (OTA) | IoT Security & Privacy Trust Framework v2.5 |

| | |
|---|---|
| U.S. Department of Homeland Security | Strategic Principles for Securing The Internet of Things (IoT) |
| US Senate | S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017 (Bill) |
| Alliance for Internet of Things Innovation (AIOTI) | Report on Workshop on Security and Privacy in the Hyper connected World |
| Broadband Internet Technical Advisory Group (BITAG) | Internet of Things (IoT) Security and Privacy Recommendations |
| CableLabs | A Vision for Secure IoT |
| IoT Security Foundation | Vulnerability Disclosure Best Practice Guidelines, IoT Security Compliance Framework 1.1 |
| Broadband Internet Technical Advisory Group (BITAG)<br>Cloud Safety Alliance | Internet of Things (IoT) Security and Privacy Recommendations<br>Future-proofing the connected world: 13 steps to Developing Secure IoT |
| European Commission and AIOTI | Report on Workshop on Security & Privacy in IoT |
| European Union Agency for Network and Information Security (ENISA) | Baseline Security Recommendations for IoT |
| Cloud Security Alliance (CSA) | Security Guidance for Early Adopters of the Internet of Things (IoT) |
| Industrial Internet Consortium (IIC) | Industrial Internet of Things<br>Volume G4: Security Framework v1.0 |
| IoT Security Initiative | CyberSecurity Principles of IoT |
| Internet Research Task Force (IRTF) Thing-to-Thing Research Group (T2TRG) | State-of-the-Art and Challenges for the Internet of Things Security |
| Microsoft | IoT Security Best Practices |
| Open Connectivity Foundation (OCF) | OIC Security Specification v1.1.1 |
| Open Web Application Security Project (OWASP) | IoT Security Guidance |
| Symantec | Strategic Principles for Securing The Internet of Things (IoT) |
| oneM2M | TR-0008-V2.0.1 Security (Technical Report) |

*Table 2. Key reference standards/recommendations and issuing organizations*

## Certification

Currently, there is no one single standard or recommendation that can provide product/solution assurance to security. However, there some that will provide indications that a product has undergone some evaluation and testing to get a mark. This section provides details to those schemes that should be considered when evaluating a product/solution. Regional efforts currently underway in the UK, EU, Australia, USA and Canada are presented.

### 3.1 Code of Practice for Consumer IoT Security

Recent research, including research by the Internet of Things Security Foundation [15], as well as the UK's Department for Digital, Culture, Media, and Sport (DCMS) report titled "Code of Practice for Consumer IoT Security" [16] published in Oct. 2018, have identified key information and best practices that is critical to be followed and documented by the manufacturer, service provider, retailer, and the consumer.

The principles identified in the Code of Practice for Consumer IoT Security [16] are shown in Figure 6 below.

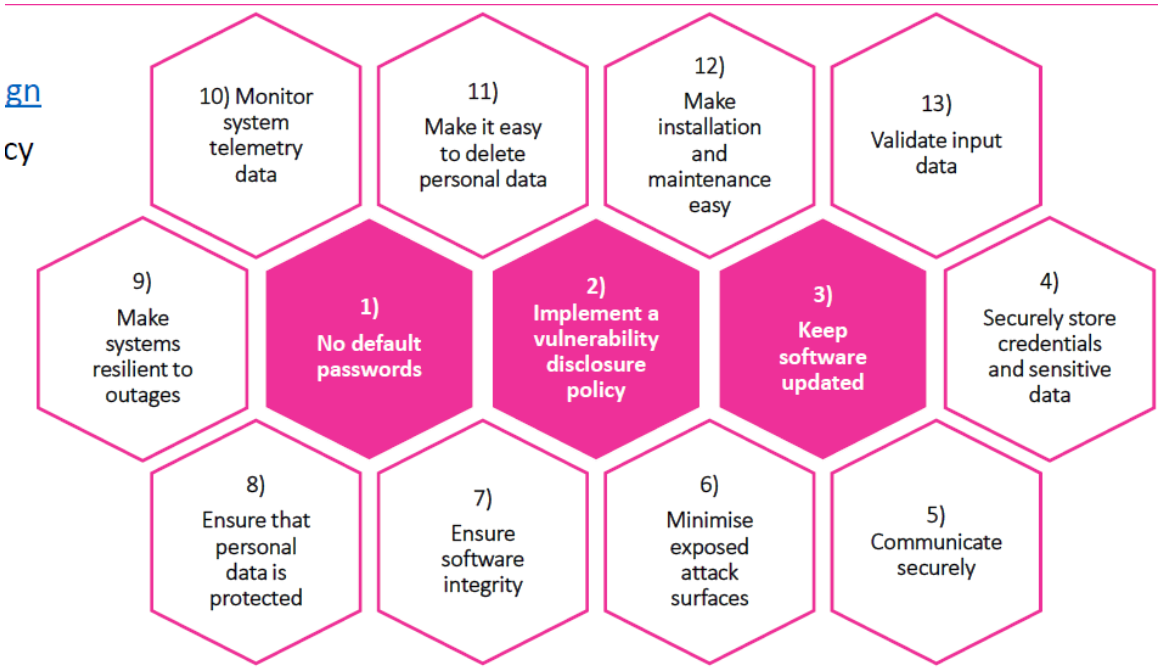



*Figure 11. UK IoT Consumer Code of Practice*

Similar guidelines have been provided by the U.S. Department of Homeland Security in the "Strategic Principles for Securing The Internet of Things" report [17]. The IoT Alliance Australia (IoTAA) published a comprehensive report titled "Internet of Things Security Guidelines" [18]. The IoTAA report identifies "the Trust Framework", which requirements form the basis for evaluating an IoT system for best practices in security and privacy, and form the basis of the IoTAA Security and Privacy Trustmark**.**

### 3.2 BSI Kitemark for IoT devices in the United Kingdom

In March 2018 the United Kingdom Government's Secure by Design review announced a series of measures to make connected devices safer to use [7]. The Kitemark builds on these guidelines by providing ongoing rigorous and independent assessments to make sure the device both functions and communicates as it should, and that it has the appropriate security

controls in place. Manufacturers of internet connected devices will be able to reassure consumers by displaying the Kitemark on their product and in their marketing materials.

There are three different types of *BSI Kitemark for IoT Devices*, which will be awarded following assessment according to the device's intended use: residential, for use in residential applications; commercial, for use in commercial applications; and enhanced, for use in residential or commercial high value and high risk applications [19].

The assessment process involves a series of tests that help ensure the device is fully compliant to the requirements. Before being awarded the Kitemark the manufacturer is assessed against ISO 9001, and the product is required to pass both an assessment of functionality and interoperability, as well as penetration testing scanning for vulnerabilities and security flaws. Once the BSI Kitemark is achieved the product will undergo regular monitoring and assessment including functional and interoperability testing, further penetration testing and an audit to review any necessary remedial action. Importantly, if security levels and product quality are not maintained the BSI Kitemark will be revoked until any flaws are rectified.

BSI Kitemark™ [19]:
The BSI Kitemark™ provides comfort and confidence to users of products or services across a whole range of sectors. Recognition of the BSI Kitemark™ is high. Two thirds of all UK consumers associate it with quality, assurance, reliability and trust. 93% of adults believe BSI Kitemark™ products are safer and 75% say the BSI Kitemark™ will help make choosing between products easier.


*Figure 12. BSI Kitemark for Residential IoT Devices*

### 3.3 IoT Product Testing in Australia

Another example for IoT product testing and certification is the process identified in Australia. IoT product manufacturers may wish to submit their products for testing by an accredited test laboratory, either under the National Association of Testing Authority (NATA) scheme or under the Australian Government in the Australasian Information Security Evaluation Program (AISEP) [18]. Formal testing will, if successful, result in the award of a test certificate and provide evidence of independent security assurance to customers.

Currently there is no mandated requirement for security testing, but the high profile of cyber attacks involving internet of things devices makes this a key area of consideration for users. Having evidence that a device has been security tested will be a competitive advantage.

In order to provide security and privacy confidence in IoT devices designed, manufactured, or deployed in Australia, the IoTAA will release a security testing procedure based on the Online

Trust Alliance Framework which will be available for accredited organizations to use to recommend the issue of an IOTAA Security and Privacy Trustmark.

There are currently three sets of published criteria that can be used for testing IoT devices:

1- The IoT Security Foundation has proposed a compliance scheme based on evaluation against their Security Compliance Framework.

In addition, the IoT Security Foundation [15] has proposed a compliance regime for demonstrating security in IoT devices and systems. This classes an IoT product into one of five classes – Class 0 to Class 4 - as shown in Table 3.

| **Class** | **Impact of Compromise** | **Confidentiality** | **Integrity** | **Availability** |
|---|---|---|---|---|
| 0 | Minimal | Basic | Basic | Basic |
| 1 | Limited impact on an individual or organisation | Basic | Medium | Medium |
| 2 | Significant impact on one or more individuals or organisations | Medium | Medium | High |
| 3 | Significant impact to sensitive data | High | Medium | High |
| 4 | Personal injury or damage to critical infrastructure | High | High | High |

*Table 3: IoT Security Foundation Classes*

2 - The Open Web Application Security Project (OWASP) [20] has developed a testing guide for IoT products. It covers sixteen IoT Principles of Security and provides a framework for testing ten different vulnerabilities.

3 - The Online Trust Alliance (OTA) framework provides measurable requirements, which can be used as a starting point for selecting security testing requirements [21]. The framework consists of eight categories of actionable principles. These principles include; authentication, encryption, security, updates, privacy, disclosures, control and communications. It also considers stakeholders who will have a collective responsibility for developing a secure solution.

IoT device manufacturers could select the relevant criteria for their device from these three documents, in addition to any device specific functionality not otherwise covered. These criteria will then form the Initial Claims Document for the security testing.

### 3.4 IoT Product Certification in the Netherlands / The European Union

As part of the EU negotiations, the Netherlands is strongly promoting the rapid adoption of the Cybersecurity Act (CSA) and the active development of a European Cybersecurity Certification framework for ICT products and services [22].

Moreover, the Dutch government supports the swift adoption of mandatory certification for specific product groups, i.e. products that present the greatest risk or the most problems in practice. In the long term, mandatory certification or compliance with a ***CE marking*** for all products with Internet connectivity should be implemented through gradual expansion.

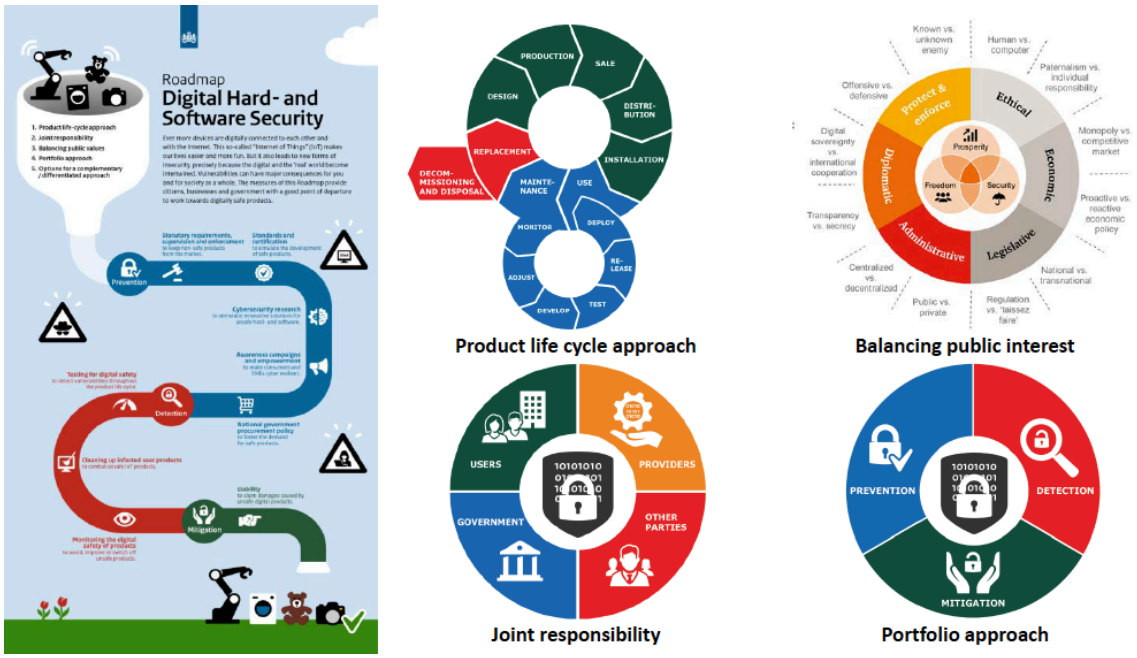



*Figure 13. Roadmap for Hardware and Software Security – The Netherland*

### 3.4.1 EU Framework: Security Certification of ICT Products and Services

The proposed Cybersecurity Act (CSA) is the European Commission's attempt to create, amongst others, a harmonized framework for the cybersecurity certification of ICT products and services within the EU. The absence of reciprocal agreements on standards and certification systems forms a barrier to creating an European market for cybersecurity products and services. It limits the scale for providers, and reduces choice and creates increasing uncertainty for procurers.

This can be changed through common European certification of products and services, indicating that they are resilient (at a specified security level) to threats to their availability, authenticity, integrity and reliability of data or of the functionalities and services being offered. The CSA aims to target fragmentation and foster the harmonization and reciprocal acknowledgement of cybersecurity certification at European level.

Once a European certification framework has been adopted for a product or service, national government schemes will become redundant and Member States will no longer need to develop their own certification programs.

### 3.4.2 ENISA Good Practices for Security of Internet of Things

Towards the end of 2018, the European Union Agency for Network and Information Security (ENISA), which is a center of network and information security expertise for the EU, published a comprehensive report on “Good Practices for Security of Internet of Things”, focusing on the context of Smart Manufacturing *(Industry 4.0)* [23].

ENSI defines Industry 4.0 as “a paradigm shift towards digitalized, integrated and smart value chains enabling distributed decision-making in production by incorporating new cyber-physical technologies such as IoT”, (Figure 14).

Industry 4.0 is gaining acceptance and is rapidly becoming a reality, making use of intelligent, interconnected cyber-physical systems to automate all phases of industrial operations. This evolution is spanning phases of design, manufacturing and operations, with a great impact on consumers’ and citizens’ safety, security and privacy due the extremely wide threat landscape, resulting from the cyber-nature and the inherent autonomy of Industry 4.0 and IoT.

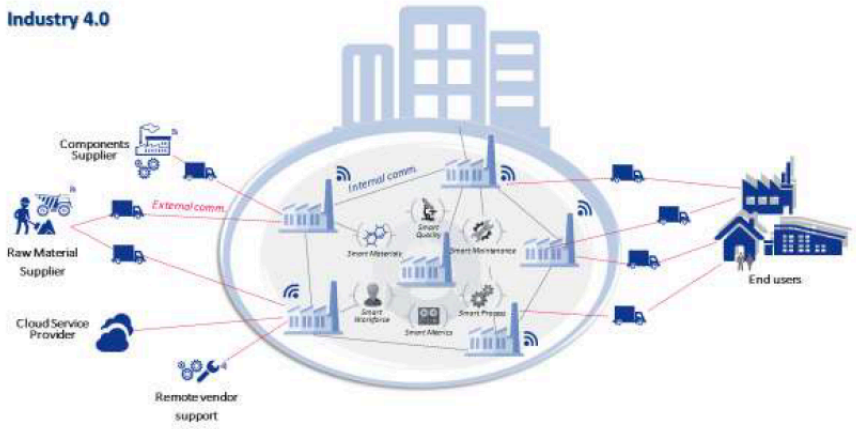



*Figure 14. Communications Relationships in Industry 4.0*

A key focal point of the ENSI report is the development of Security Measures for IoT in Smart manufacturing. The approach behind this is to provide guidelines and recommendations for Operators, Manufacturers and Users of Industrial IoT (IIoT). Applying these guidelines can help prevent or properly respond to potential cyber attacks and ensure overall security and safety of the industrial IoT environment.

The recommendations and guidelines are classified into three main groups (see Figure 14):

- Policies
- Organizational practices
- Technical practices


*Figure 15. Good Practices Overview*

3.5 CTIA Cybersecurity Certification for IoT Devices

In 2018, CTIA published the CTIA Cybersecurity test Plan for IoT Devices [24]. This plan identifies testing requirements for CTIA Cybersecurity Certification of managed Internet of Things devices. In this case, an IoT device contains an IoT application layer that provides identity and authentication functionality and at least one communications module supporting either LTE or WiFi connectivity.

The test plan defines the Cybersecurity test that will be conducted by CTIA Authorized test labs (CATLs) on devices submitted for CTIA Cybersecurity Certification. An IoT device connects to at least one network to exchange data with other devices, vehicles, home appliances, infrastructure elements, etc. The device might include hardware, software, sensors, actuators and network connectivity.

CTIA Cybersecurity Certification is defined in three categories. The first category identifies core IoT device security features, and the second and third categories identify security elements of increasing sophistication, complexity and manageability.

While the test plan aims at ensuring compatibility across Cybersecurity systems through using the widest adopted standards, it mandates a number of critical standards including: AES key size standards, end-to-end encryption standards, syslog standards, etc. An AES with a minimum of 128-bit key is expected by the test plan, to ensure interoperable cryptographic capability among all devices tested. However, devices my also support other algorithms and key sizes that provide the same or more cryptographic security.

Table 4 provides and overview of the Cybersecurity test cases per IoT device category.

| | |
|---|---|
| **Category 1 IoT security features** | |
| | Terms of Service and Privacy Policies |
| | Password Management |
| | Authentication |
| | Access Controls |
| | Patch Management |
| | Software Updates |
| **Category 2 IoT security features** | |
| | Cat. 1 IoT security features |
| | Audit Log |
| | Encryption of Data in Transit |
| | Multifactor Authentication |
| | Remote Deactivation |
| | Secure Boot |
| | Threat Monitoring |
| | IoT Device Identity |
| **Category 3 IoT security features** | |
| | Cat. 1 and Cat. 2 IoT security features |
| | Encryption of Data at Rest |
| | Digital Signature Generation and Validation |
| | Tamper Evidence |
| | Design-in Features |

*Table 4. CTIA IoT Cybersecurity Test Cases*

### 3.6 Canadian Standards Association (CSA) Group Cyber Verification Program

The CSA Group is currently developing a program and national standard that is aiming to address the product and organization security aspects. The Cyber Certification Program (CVP) consists of several aspects including a self-assessment, onsite audit, and formal product testing and evaluation. This program is built on the premise that an insecure organization cannot build a secure product. Security practices must be embedded into the organization's operations and development processes.

The assessment aspects consider 6 domains and 18 practice areas within these domains. The current self-assessment consists of 198 binary questions that once completed in connection with audit will provide a maturity rating for the organization.

The program has been field testing and has resulted in Notice of Intent (NOI) being filed in Canada that will lead to a standard being developed for the Canadian market place. This will include the ability for vendor organizations to perform an attestation to this standard.

### 3.7 Underwriters Laboratories (UL) 2900

UL has a series of standards that will formally evaluate a product against specific criteria to determine that the vendor is following and has correctly implemented the list of controls. These includes medical products and devices, currently. The testing and evaluation process is quite stringent and will provide buyers the assurance that formal testing including penetration testing

has been conducted against a product.

### 3.8 ISO/IEC Standards

There are several standards that maybe considered products and organizations to determine their security posture. Keep in mind that these may not necessary result in a label but a certificate of product or organizational testing and evaluation.

ISO/IEC 27001 – Is a standard and certification process that will indicate that an organization has formally implemented and maintains an information security management system or ISMS. An ISMS is a formal system of process, procedures and controls that identify and mitigate the risks associated with the organization. The controls are defined in the standard and guidance is provided on how to implement the necessary risk management framework within an organization.

ISO/IEC 9001 – Is a standard and certification process that will indicate the process maturity of an organization in order to deliver a product or service. This includes an approach that states what they do, do what they say, and be able to prove it by creating process artifacts.

ISO/IEC 15408 – Common Criteria is a formal product assessment methodology that provides assurance to product based on confidentiality, integrity and availability. It can assess both hardware and software and is typically a requirement for government and higher security technology deployments. The result is objective testing using an evaluation process that will consider either the Evaluation Assurance Level (EAL) or Security Assurance Requirements (SAR) to provide the buyer with a rating that indicates that vendor meets a specific target level.

### 3.9 CyberNB Cyber Essentials

This program is built on the UK program with the same title and objectives. The province and several partners have adopted this framework as a means to validate that organizations have a minimum set of security requirements that they can demonstrate that have been deployed. The focus is on IT controls within the organization and targets SMBs for deployment of these controls.

## Enforcement

It is important to understand that certification is not a guarantee of product security nor privacy. Certification of any product or organization is based on a standard, usually international in context, that is used to conduct formal testing on a product or organization.

While under development, no standard for IoT controls currently exists that can be used to definitively address the IoT security and privacy issues. As a result, there are other aspects that be can be evaluated under a formal audit and product testing that can validate that both a company and product are being securely developed.

It is important to keep in mind that a company can and will falsify a label as well and buyers need to determine if a label has been counterfeited. This might represent a bigger issue for consumers who are now being educated that a label is to be accepted as the means to

determine assurance. The motivations for counterfeiting include costs, attempting to gain market share, or grey market goods. To better protect the buyer, we would suggest labelling requirements that include a "live" portion. This live portion will allow a potential buyer to determine the following:

1. A machine readable code that will redirect the user to a live internet portal. i.e. QR code

2. The internet portal should contain the following as minimum:

    a. Company name

    b. Product

    c. Current model version

    d. Current firmware version

    e. Current MUD file or equivalent version

    f. Certifying company

    g. Date of certification or last assessment

## Empowering consumers through education (OTHER WORK GROUP)

While many of the resources may provide technical information, there is information that consumers need to consider when considering specific products or solutions and potential risks with the usage of these.

*Privacy*

Office of the Privacy Commissioner (OPC)

*Security*

Online Trust Alliance (OTA) including decision buying and risk aspects for consumers.
Consumer Reports provides The Digital Standard for details on security aspects of products.
UK Government with several initiatives for products
NIST provides content for products and services however it tends to more technical in scope.

## Definitions

[as required]

## Summary of Work

Over the last year this group has conducted multiple meetings both online and in-person. This report presents the primary findings for product labeling and the need for more joint efforts not just in Canada but globally on security and privacy requirements for IoT. The research part of this report clearly indicates how fragmented the market is for labeling and how few standards actually exist that will provide consumer assurance that a product has been securely designed, built, tested and evaluated.

At this point, there is no formal regulatory requirement for products to be cyber secure or safe. We hope that this paper will begin to change this and will lead to vendors looking to provide evidence of their security posture using formal assessment and labeling.

Our key findings for this working group include:

1. Need for rules on what a security label should look like and the information it will contain;
2. Consumers need more education on types of labels and what they actually mean for security and privacy implications;
3. Canada needs to find ways to work globally to eliminate duplication of effort for security and privacy labeling;
4. We need to consider compliance to Canada laws for PIPEDA and CASL for vendors and how this is reported to consumers or integrated into a label;
5. While labeling for most products should be voluntary in some sectors it should be mandatory where personal safety could be at risk.

# Key Outputs and Recommendations

## Finding One: Comparison of Types of Labels for IoT Device Security

This table provides a comparison between the different types of labels, focusing in their suitability as a label for IoT device security (Table 5).

| Type of Label | Pros | Cons | Notes |
|---|---|---|---|
| Graded/Colour Graded | - Attracts the attention of consumers<br>- Helps consumers compare the security of different devices | To be effective the display needs to be mandatory for manufacturers | Could be introduced at a later stage in a mature IoT Security market |
| Binary<br>(Seal of Approval) | - Easy for customers to interpret<br>- Preferred by consumers | - Less effective in guiding consumer choice<br>- Gives (false) sense of security and that no additional action from consumer is needed<br>- Does not automatically reflect current security status or new product vulnerabilities. | - Example is BSI Kitemark in the UK<br><br>- Combine binary/seal of approval label with other informative label (e.g. Live Label) |
| Informative | Communicates critical information to consumers<br>- Provides helpful indicators of a device's security readiness<br>- More suitable for voluntary label introduction | - Need to limit information displayed to most relevant information | Suitable for market introduction and to help build consumer understanding and trust. |
| Live Label<br>(e.g. QR code) | - a form of informative label<br>- QR codes are gaining adoption from manufacturers as marketing tools<br>- Provides link to current information on | - Requires consumer to scan QR code and spend time going through relevant information | Suitable for market introduction and to help build consumer understanding and trust. |

| | | | |
|---|---|---|---|
| | product security<br>- Allows consumer to get information beyond security compliance, e.g.<br>- Deployment recommendations,<br>- Data collection/sharing information,<br>- Latest vulnerabilities | | |

*Table 5. Comparison of types of Labels for IoT Device Security*

## Finding Two: Determining the Labels to be Considered

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 conflicting information available. Therefore a decision-making model can be provided to help users and businesses identify and assess any labelling used on an IoT device. The model also illustrates that there are different risk aspects of IoT devices in other sectors. The diagram that follows provides with high level flow and the details that follow provide the necessary guidance for each user group to best determine the labels that should be considered (Figure 16).

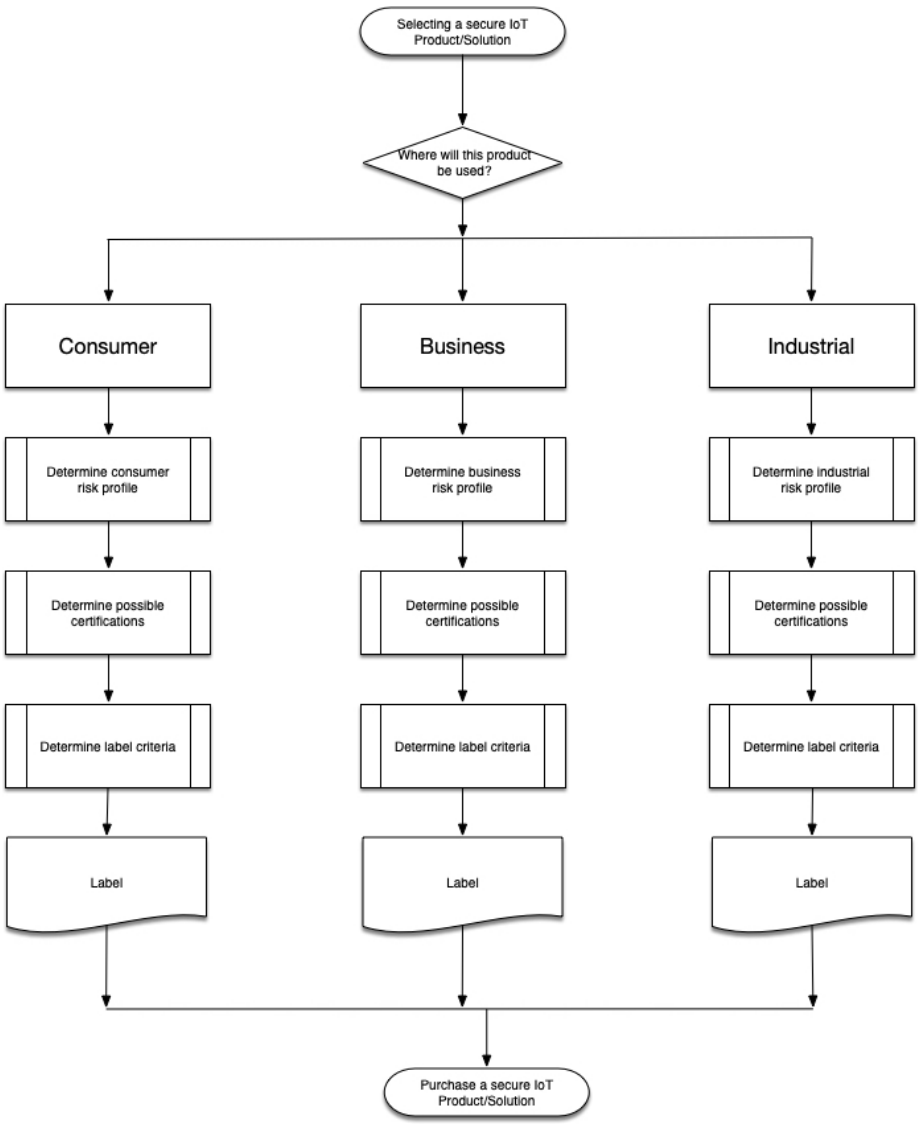



*Figure 16. Process for determining Labels to be Considered*

Where will the product be used?

For many IoT solutions they are targeting three separate sectors; consumer, business and industrial. We have used these three sectors as they represent three very distinct risk profiles for the end user. Recognizing that these risk aspects exist and must be used as differentiator will help the vendor and buyer of these solutions to meet label requirements. The scope of this paper while it considers the industrial sector focuses only on the consumer and business sectors.

Risk Profiles

In order to make informed buying choices, consumers should be able to demonstrate that they have considered and evaluated the risks created when they chose an IoT solution vs. a non-connected alternative. This is to say that consumers should be able to develop a ‘risk profile’ for the device.

These criteria consider some of high-level risks that are associated with each level of product category. The only way to fully quantify the risk of a 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 aspects to determine the risk of exposure to each of these. The lack of details from the vendor should be considered that they are 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*

a. Confidentiality – Can the vendor provide details to how the design of the solution or product will protect the confidentiality of the data being collected, processed and stored?

b. Integrity – Can the vendor provide details to 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.

c. Availability – Can the vendor provide details to 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 it and use it?

d. Safety – Can the vendor ensure the product will function as anticipated and not become a hazard due to a device failure which may include fire, electrocution, burning, melting, emit harmful vapour, or emit harmful radio signals.

e. Reliability – Can the vendor provide details to how the device or solution will ensure that it will provide a specific or targeted state of being reliable?

For the section in the table that follows the consumer should consider these attributes as they review the questions for consideration. This approach should help to provide a context to the features that will be implemented in a device or solution.

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

1. No default user accounts and passwords – With 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 to data being collected, processed, and stored for service users. This includes data breach protocols and 3rd 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 receiving 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 ones 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 prior to installation.

8. Vendor should provide specific dates that products will be provided support – The vendor should be very clear and concise to the date or period that a product will be support for software updates. When possible, users should be notified that a product has reached it end-of-life for software support.

Based on these previous attributes the consumer is better educated to make a final educated decision on a selection of a product or solution. The following table outlines potential threats and additional considerations that will help to determine if 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 3rd party assessments and attestations<br>- Vendors lack of governance for security and privacy<br>- Vendor 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 3rd parties |
| Business | Data breach of infrastructure, account compromises for users and administrators, | - 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 |

| | | |
|---|---|---|
| | weaponizing of infrastructure and devices, source code and firmware compromises | - Policies and procedures that do not include incident handling during data breach situations<br>- Failure to identify a either a data breach, device compromise, or user account compromise |
| Industrial | Secure operation of device in-field, 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 of events |

*Table 6. Risk Considerations for Consumer before Purchase of IoT Device*

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 base on vendor reputation or the recommendation of friend. 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 usability needs.

| *Sector* | *Certification* | *Considerations* |
|---|---|---|
| *Consumer* | *Electrical* | *Where was the device manufactured? Some regions will require products to undergo electrical certification for these products this may include the CE mark.*<br><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 provide a means to show the vendor has undergone formal assessment to a regulatory framework and does have a minimum level of maturity for organizational processes.* |
| | *Safety* | *If this device was 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 this have an impact to you the buyer?*<br><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 have a quality management process in place?*<br><br>*Look for ISO 9001 or ISO 14001. These symbols will indicate formal assessment against these processes for process and manufacturing assurance for the vendor.* |
| | *Security* | *Do you want to purchase a product that undergone security and product testing?*<br><br>*Look for the BSI Kite Mark to represent organizations who 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><br>*UL 2900 will also provide a means to determine that a product has undergone a formal product assessment. While the vendor processes other than development are not considered it still provides a mean 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 product that has been security stress tested?*<br><br>*Look for a indications that penetration tests have been conducted either on the web site or product documentation. Note of Caution: Not all penetration tests are equal as there are no formal standards on methodology or tools being used. As such, it can be a one* |

| | | |
|---|---|---|
| | | *and done approach versus a continuous improvement program within the organization.* |
| *Business* | *Electrical* | *Same as consumer* |
| | *Safety* | *Same as consumer* |
| | *Security* | *If you need to have a product that will provide a level assurance for operating environments such as government, telecommunications, or high risk operating environments?*<br><br>*Look for Common Criteria ISO 15408 with protection profiles that align to the product base functionality.*<br><br>*UL2900 Series can also be used determine if a product has been assessed for specific security design features and flaws. Privacy is not included in this assessment.* |

*Table 7. Certification Considerations for Consumer before Purchase of IoT Device*

Determine Potential Labels

The list that follows provides some product categories and the possible product labels that current exist. While not full proof, it does provide a level of assurance that the vendor takes assessment and evaluation important. As such, they have decided to obtain formal certification which indicates a level of business, process, and product maturity. These certifications are not a guarantee of security and privacy safety but that product has undergone a certain level of evaluation.

a. Home appliances

- Electrical certification multiple CAN, US and IEC standards
- Security testing and evaluation UL 2900 or equivalent
- Attestation to CSA CVP or equivalent
- OTA, Consumer Reports, BSI Kite Mark or equivalent

b. Security and safety

- Functional safety certification to IEC 61508
- Security testing to ISO 15408 *for mission critical environments
- Security testing and evaluation UL 2900 or equivalent

- Attestation to CSA CVP or equivalent
- OTA, Consumer Reports, BSI Kite Mark or equivalent

c. Lighting

- Electrical certification multiple CAN, US and IEC standards
- Security testing and evaluation UL 2900 or equivalent
- Attestation to CSA CVP or equivalent

d. Entertainment

- Electrical certification multiple CAN, US and IEC standards
- Security testing and evaluation UL 2900 or equivalent
- Attestation to CSA CVP or equivalent
- OTA, Consumer Reports, BSI Kite Mark or equivalent

e. HVAC

- Electrical certification multiple CAN, US and IEC standards
- Functional safety certification to IEC 61508
- Security testing and evaluation UL 2900 or similar
- Attestation to CSA CVP or similar

f. Utility

- Functional safety certification to IEC 61508
- Electrical certification multiple CAN, US and IEC standards
- Security testing and evaluation UL 2900 or similar
- Attestation to CSA CVP or similar

Regardless of the sector or product, there are two standards that an organization can target which will provide a level of process maturity for product quality and security management. These are ISO 9001 for a quality management system and ISO 27001 for an information security management system. If a vendor has one or both of these it should be regarded as a higher level of assurance to a product and that the necessary security controls have been deployed.

## Finding Two: Live Label Requirements and Structure

As many of the labels represent a static view of product a specific time within the product lifecycle, there is a need to ensure that dynamic view of the product is available to users. The concept of a “live label” is not new however based on the discussions within the ISOC Multistakeholder process it become clear that this a different approach to labeling is required. A static label will provide a near real time view of any product security risks. As many products who undergo formal testing and evaluation there will be aspects of the software components that could provide no risks one day but due to a zero-day discovery and/or malware the component and possibly the product will be prone to compromise. The need to be able to provide a single source of information for product buyers is becoming more critical. As many vendors do current offer support sites the additional elements being recommended are not a

far reach to meet the necessary requirements but will offer a comprehensive view of the an IoT products risks.

Requirements:

a. A web page accessible by secure means

b. The web page will contain specific details to each or a group of products provided by the vendor. This shall include:

    a. Product firmware updates

    b. Product security alerts and announcements including any CVE's and CVSS registrations

    c. Policies for privacy and vulnerability disclosures, including any recent changes to data collection policies or practices

    c. Contact details for either phone, web, or email support that will result in a minimum response of 72 hours

c. The web page should contain additional details that include:

    a. HowTo and user guides for secure setup and configuring the IoT device(s)

    b. References to updated certifications and/or attestations obtained

d. The web page may contain supporting details that include:

    a. 3rd party organizations who conducted formal testing and assessment to recognized standards and attestations

    b. Alert levels for cloud hosting and online system availability

e. Use an electronic coding scheme that will allow users to quickly find the "live label" web site

f. Additional fail safes that will prevent the counterfeiting of labels placed on products

A security product label should have the following aspects:

1. Clearly identify the organization who performed the formal testing and assessment

2. Clearly identify the standard and product being tested and assessed

3. Holographic, embedded RFID tag or other means to prevent counterfeiting

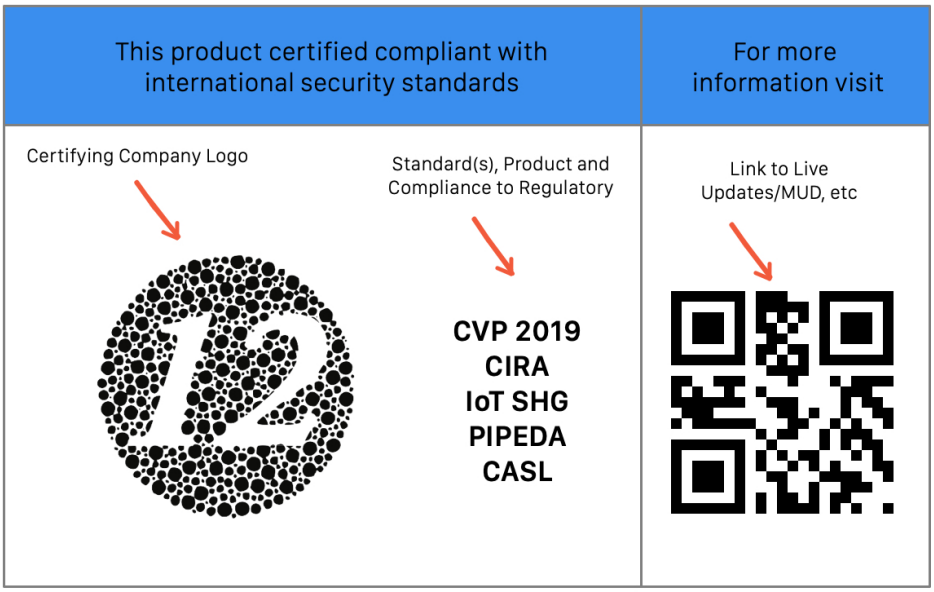
3. Have a machine readable code that can be used to provide update to date and live information on the specific instance of the product. This can be hosted on current company or product website. This should include the following:

    a. Product model and/or version number

    b. Latest product firmware version number

    c. CVE's or CVSS references

d. Security configuration guide




Reference Sample ONLY

The reference example above indicates what a proposed “live” label might look like. This indicates the 3-key elements including the name of certifying company, product, standard, compliance, and link to live site. While not completely full proof it does provide additional information that user can us the validate a label. If the vendor attempts to falsify all of these details it would clearly indicate a liability situation.

## Next Steps

This are listed in no particular order of importance.

a. Approach and collaborate with other organization focusing on IoT security and privacy such as the IoT Security Foundation, IoXT, IoTAA, and EU in an attempt to reduce the amount of fragmentation in the market for initiatives and labels to avoid consumer confusion;
b. Continue influencing the standards effort through the ISO/IEC for International standards and SDO's with similar projects and interests;
c. In collaboration with OTA, approach key vendors and solution providers to raise awareness on the need for security certification and device labels;
d. Determine the best organization to provide a formal specification of the "live label" to. This could be IETF or similar for the specification. This includes further developing the Live label (QR codes) proposal through collaborating with other organizations such as the OTA;
e. One consideration to elevate the proposed voluntary labelling framework is the way it provides a model for consumer IoT device manufacturers to demonstrate their compliance with existing Canadian law and regulations in this space, including but not limited to the *Canada Consumer Product Safety Act*, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), and the *Canadian Anti-Spam Legislation (CASL).* The final year-one report of the Canadian IoT initiative could highlight the existing requirements in this space at the outset of the paper to situation proposed outcomes such as the labelling framework. This also reveals that the 'gap' is the lack of a clear and consistent way for manufacturers to indicate that they complete the certification with certain standards, and provide additional information, that makes them compliant with these laws. This in turn situations the proposed voluntary labelling framework as a flexible, user-friendly framework to apply in order to advertise their compliance and effort put towards reducing risks associated with IoT devices.

# References:


[1] PETRAS IoT Hub, Rapid evidence assessment on labelling schemes and implications for consumer IoT security, October 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747296/Rapid_evidence_assessment_IoT_security_oct_2018.pdf

[2] Kahneman D, Egan P. Thinking fast and slow. New York: Farrar, Straus and Giroux.; 2011.

[3] Cecchini M, Warin L. Impact of food labelling systems on food choices and eating behaviours: a systematic review and meta-analysis of randomized studies. Obes Rev. 2016;17:201–10. doi:10.1111/obr.12364

[4] Feunekes GIJ, Gortemaker IA, Willems AA, Lion R, van den Kommer M. Front-of-pack nutrition labelling: Testing effectiveness of different nutrition labelling formats front-of-pack in four European countries. Appetite. 2008; 50:57–70. doi:10.1016/j.appet.2007.05.009.

[5] Szanyi JM. Brain food: Bringing psychological insights to bear on modern nutrition labeling efforts. Food and Drug Law Journal. 2010;65. http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/foodlj65&section=9. Accessed 24 May 2018.

[6] Koenigstorfer J, Wąsowicz-Kiryło G, Styśko-Kunkowska M, Groeppel-Klein A. Behavioural effects of directive cues on front-of-package nutrition information: The combination matters! Public Health Nutr. 2014;17:2115–21.

[7] Department of Digital, Culture, Media and Sport (DCMS), Secure by Design Report, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

[8] Dong-Hee Shin, Jaemin Jung, Byeng-Hee Chang “The psychology behind QR Codes: User experience perspective” ,Science Direct, Computers in Human Behavior 28 (2012) pp 1417-1426.

[9] Phaisarn Sutheebanjard, Wichian Premchaiswadi, “QR Code Generator”, IEEE 2010 8th International Conference on ICT and Knowledge Engineering (24-25 Nov. 2010) pp 89-92.

[10] Sumit Tiwari, An Introduction to QR Code Technology, IEEE International Conference on Information Technology (ICIT) 2016, **DOI:** 10.1109/ICIT.2016.021

[11] ScanLife.com, “QR Code Adoption: Trends and Statistics”, www.scanlife.com

[12] QR Code Statistics 2018: Latest Numbers On Global QR Code Usage, (https://scanova.io/blog)

[13] Scanbuy, QR Codes Use Cases, http://www.scanlife.com/case-studies/

[14] Department of Digital, Culture, Media and Sport (DCMS), Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747977/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf

[15] IoT Security Foundation, Establishing principles for IoT Security, https://iotsecurityfoundation.org/wp-content/uploads/2015/09/IoTSF-Establishing-Principles-for-IoT-Security-Download.pdf

[16] Department of Digital, Culture, Media and Sport (DCMS), Code of Practice for Consumer IoT Security, 2018, https://www.gov.uk/government/publications/secure-by-design

[17] U.S. Department of Homeland Security, Strategic Principles for Securing the Internet of Things, 2016, https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[18] IoT Alliance Australia, Internet of Things Security Guideline, 2017, http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

[19] British Standards Institution. BSI launches Kitemark for Internet of Things devices, 2018. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2018/may/bsi-launches-kitemark-for-internet-of-things-devices/.

[20] Open Web Application Security Project (OWASP), Principles of Security, www.owasp.org/index.php/Principles_of_IoT_Security

[21] [16] Online Trust Alliance (OAT), IoT Trust Framework, https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

[22] Ministry of Economic Affairs and Climate Policy, The Netherlands, Roadmap for Digital Hard-and Software Security, 2018, https://www.government.nl/documents/reports/2018/04/02/roadmap-for-digital-hard--and-software-security

[23] ENISA, Good Practices for Security of Internet of Things, 2018, https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

[24] CTIA, CTIA Cyber Security Certification Test Plan for IoT Devices, 2018, https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0.pdf