Loss Prevention Standards – Cross Classes

Cyber Security: The Internet of Things

Version: 1.1
Date: 4th April 2024

The Internet of Things (IoT) connects countless devices and systems, expanding the potential for cybercriminal activity greatly. This document outlines recommendations specifically for securing IoT devices and networks against threats that could lead to cyber-attacks.

AVIVA

Cyber Security: The Internet of Things

Introduction

The Internet of Things (IoT) describes the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

Where did the IoT Start?

Connecting devices via the internet, effectively making them what is now known as smart devices was first completed in 1982.

- A soft drink vending machine at Carnegie Mellon University became the first internet-connected appliance. It was able to report its inventory and determine whether newly loaded drinks were cold enough.

This concept and technology have developed, with applications in industry, retail, many other business sectors, within vehicles and in the home.

The term Internet of Things was widely understood to be coined by Kevin Ashton of Procter & Gamble. It is estimated that the IoT was born around 2008/09 and defined it as being born at the point in time when there were more things connected to the internet, than people.

Today, almost any physical object can be transformed into an IoT device if it can be connected to the internet, and therefore be remotely controlled or communicate information. A light that can be switched on using a smartphone app is an IoT device, as is a motion sensor, or a smart thermostat, or even an internet-enabled coffee machine.

IoT is the present and is certainly the future. A USA based technology analyst company, predicts that in total there will be 55.7 billion connected IoT devices by 2025. They also predict industrial and automotive equipment will represent the largest opportunity of connected things and sees rapid development of smart homes and wearable devices soon.

As the price of sensors and communications continues to drop, it will become cost-effective to add more devices to the IoT, even if there's little obvious current benefit to users. As the number of connected devices continues to rise, living and working environments will become filled with smart products. As a result, it is essential that businesses and individuals are aware of the possible security issues, and best practice guidelines for ensuring the security of these devices and systems.

The Applications

Current, and future applications for IoT devices can be seen in Consumer, Industrial, Organisational, and Infrastructure areas:

Consumer

Generally:

- Lighting, heating and air conditioning systems, media/entertainment, fire and security systems and camera systems.
- Smart speakers, video doorbells, coffee machines, refrigerators, washing machines, and children's toys in addition to computers, tablets, and mobile telephones, etc.

To help support elderly or infirm persons:

- Items such as home systems using assistive technology to accommodate an owner's specific disabilities can be used.
- Voice control for users with sight and mobility limitations, and alert systems can be connected directly to cochlear implants, worn by hearing-impaired users.
- Items such as sensors that monitor for medical emergencies such as falls, or seizures can be employed.

Even simple children's toys are steadily becoming more internet-enabled… through to gaming consoles, etc. that have quite sophisticated connectivity.

Industrial

- Manufacturing devices can be equipped with sensing, identification, processing, communication, and networking capabilities.
- Digital control systems to automate processes, operator tools and service information systems to control plant safety and security.
- Maintenance, stock control, and basics such as heating, etc., are some of the industrial applications for IoT devices.

As an example, IoT applications in farming would include collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content, to optimise activity and farm production.

Organisational

Transport: IoT devices assist smart traffic control, smart parking, electronic toll collection systems, logistics and fleet management, vehicle control, safety, and road assistance. These are designed to help improve safety on the roads and flow of traffic and collect a huge amount of data.

Healthcare: Termed the Internet of Medical Things (IoMT), this is an application of the IoT for medical and health related purposes. The basic purpose being the connection of available medical resources and healthcare services.

One huge benefit to healthcare services and to users, is that IoT devices can be used to enable remote health monitoring and emergency notification systems, e.g., monitoring specialised implants, such as pacemakers, and conditions such as blood pressure.

IoT devices are used in laboratory work and diagnostics. The advances in plastic and fabric electronics have enabled ultra-low cost, single use IoMT sensors to be used.

This amount of readily available patient data, can be used to make great improvements in many areas, including treatments, waiting lists and priorities, and assessing trends, etc., but as a result security is clearly paramount.

Maintenance: Building Management Systems are used to monitor and control the mechanical, electrical, and electronic systems, including heating and access control used in various types of buildings, often via connected IoT devices.

Infrastructure

- Monitoring and controlling operations of urban and rural infrastructures such as bridges, railway tracks and on, and offshore windfarms, is a major application of the IoT. The IoT infrastructure can be used for monitoring events or changes in structural conditions that can compromise safety and increase risk.
- Control of waterways, as in New York City, to connect all the city's vessels and be able to monitor them live 24/7. This has brought large improvements in safety, efficiency, and ticketing, etc.

Another major impact of IoT is the 'Smart City.' A project in Santander, Spain, for example, shows what future projects could look like. This city of 180,000 inhabitants has already seen 18,000 downloads of its city smartphone app. The app is connected to 10,000 sensors that enable services like parking search, environmental monitoring, digital city agenda, and more. Other towns and cities have similar systems in some form of development and with IoT increasing, it can be expected that more will investigate the benefits.

The biggest and highest profile example of a 'Smart City' is Barcelona. The high-tech improvements seen throughout Barcelona using IoT include street-lighting, waste disposal, the bus system, irrigation, and more. As a result, Barcelona is viewed worldwide as the quintessential Smart City.

Energy and the impact of IoT also comes under the infrastructure heading. Energy-consuming devices, lights, household appliances, motors, etc. can now be monitored and scheduled for efficiency and cost effectiveness, and the data available from smart meters, etc., can help suppliers assess requirements for areas, businesses, or individual homes.

There are also significant environmental aspects and monitoring of weather, earthquake zones, etc., which are assisted and improved by use of IoT.

Cyber Security and IoT

The IoT presents several security challenges. The UK Code of Practice for Consumer IoT Security led onto the European Telecommunications Standards Institute (ETSI) EN 303 645. This European Standard sets out recommended levels of cyber security provisions for consumer IoT. This puts the onus on the manufacturer or service provider of IoT devices or components to ensure a level of security, which includes:

- No universal default passwords.
- Implement a means to manage reports of vulnerabilities.
- Keep software updated.
- Securely store credentials and security-sensitive data.
- Communicate securely.
- Minimise exposed attack surfaces.
- Ensure software integrity.
- Ensure that personal data is protected.
- Make systems resilient to outages.
- Examine system telemetry data.
- Make it easy for consumers to delete personal data.
- Make installation and maintenance of devices easy.
- Validate input data.

The National Cyber Security Centre has further provided end users with security advice for IoT devices.

The key points are summarised below:

Device Set-up

The customer should check reviews, etc., before a purchase. Refer to the manufacturer's documentation and 'Get Started' guide, or similar. This is likely to be a hard copy of the device, and/or on the manufacturer's website. It could also come as part of a smartphone app needed for the device.

Default Settings

These should be checked, as devices could come with basic, easily found or guessed, default usernames and passwords. These need to be changed immediately to a more secure format.

Managing an Account

One basic recommendation with cyber security is Multi-factor Authentication or Two-factor Authentication. If an IoT device to be connected has this function, it is strongly recommended it is used. Having a second step to authentication and access to a device or account puts in an extra barrier against cybercrime. If a password is compromised the second factor for authentication will still be required before access can be gained.

Update the Device

Again, this is an essential part of general cyber protection, and applies the same to IoT devices. Updates to software should be actioned as soon as they become available, as they also include the latest security improvements. These could be made available to cover known vulnerabilities, so getting them activated in a timely manner, helps protect against cyber criminals attempting to act on known weaknesses.

✓ If a device can be set to automatically update, this is advisable.

Reporting an Incident

If it is felt a device has been compromised, tampered with, or accessed, the manufacturer's website should direct customers on what they need to do to report an incident.

If there is any concern that a device could have been compromised the recommended route is to:

1. Perform a factory reset.
2. Strengthen passwords.
3. Include multi-factor authentication.

In the UK, the Police are also keen for all cyber incidents to be reported to ActionFraud, to help raise awareness of issues, and to support any action required to secure such devices.

For other countries please report cyber incidents to your relevant cyber security authorities.

Selling or Throwing Away Replaced Devices

As devices come to the end of their use, or are replaced by a new model, etc., personal data needs to be removed, and the best way to do this is to complete a factory reset and wipe the device clean. This is considered essential.

The manufacturer's website or user guide will show how to complete a factory reset.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- National Cyber Security Centre
- UK Government: Code of Practice for Consumer IoT Security
- UK Government: Secure by Design
- ETSI
- ETSI European Standard 303 645
- ActionFraud
- Information Commissioner's Office

Additional Information

Relevant Loss Prevention Standards include:

- Cyber Security - Cyber Essentials Accreditation
- Cyber Security – Ransomware
- Cyber Security - Respond and Recover
- Cyber Security - Social Engineering
- Cyber Security - Top 12 Tips to Protect Against a Cyber Attack
- Cyber Security - Homeworking

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

4th April 2024

Version 1.1

LOSS PREVENTION STANDARDS