

ISPANZ POSITION PAPER

THE INTERNET OF THINGS (IoT)

Two years ago we issued the first edition of this Position Paper. At that time we outlined the growing problem of security for devices making up the Internet of Things (IoT). We encouraged our members to make their customers aware of the security issues associated with IoT devices and be in a position to advise them appropriately. The security of IoT devices has only become more problematic and complex since then.

Consumer devices with internet connectivity have proliferated and security has not kept pace. Whilst two years ago we were concerned that many devices had no security, today many devices have their security compromised through inattention or poor password management by owners. Hackers steal email addresses and passwords in bulk from a website or service and post these on line. Those with malicious intent then check to see if those credentials work elsewhere, which they often do because people do not want to remember many different passwords. This is known as ‘credential stuffing’. Credential stuffing, coupled with software such as Snipr, makes it simple for hackers to access people’s personal devices in their homes and offices. In one high profile case a Nest security camera in a child’s bedroom was hijacked and used to play pornographic soundtracks to the young child.¹

¹ <https://www.stuff.co.nz/technology/112249828/how-nest-designed-to-keep-intruders-out-of-peoples-homes-effectively-allowed-hackers-to-get-in>

This global problem is attracting the attention of governments and regulators around the world. For example, the UK's 'Secure by Design' code of practice has three top security requirements, which are:

- IoT device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
- Manufacturers explicitly state the minimum length of time for which the device will receive security updates through an end of life policy.

The UK is looking to introduce a labelling scheme which will tell consumers how secure a device is. Retailers would only be able to sell products with an IoT security label.²

ETSI, the European Standards Organisation, has launched Technical Specification 103 645 on the cybersecurity of internet-connected consumer devices.

ISPANZ Position

ISPANZ supports New Zealand adopting legislation to protect users of IoT products along the lines proposed by the UK.

ISPANZ supports the development of appropriate joint Australian and New Zealand standards on the cybersecurity of internet-connected devices.

² <https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices>

ISPANZ encourages its members to educate their customers on IoT vulnerabilities and on the importance of good password management to avoid becoming subject to credential stuffing based attacks.

END