IOT – the Achilles Heel of cyber security

Dr David Brewer, FBCS, CITP

Director, IMS-Smart Limited

Agenda

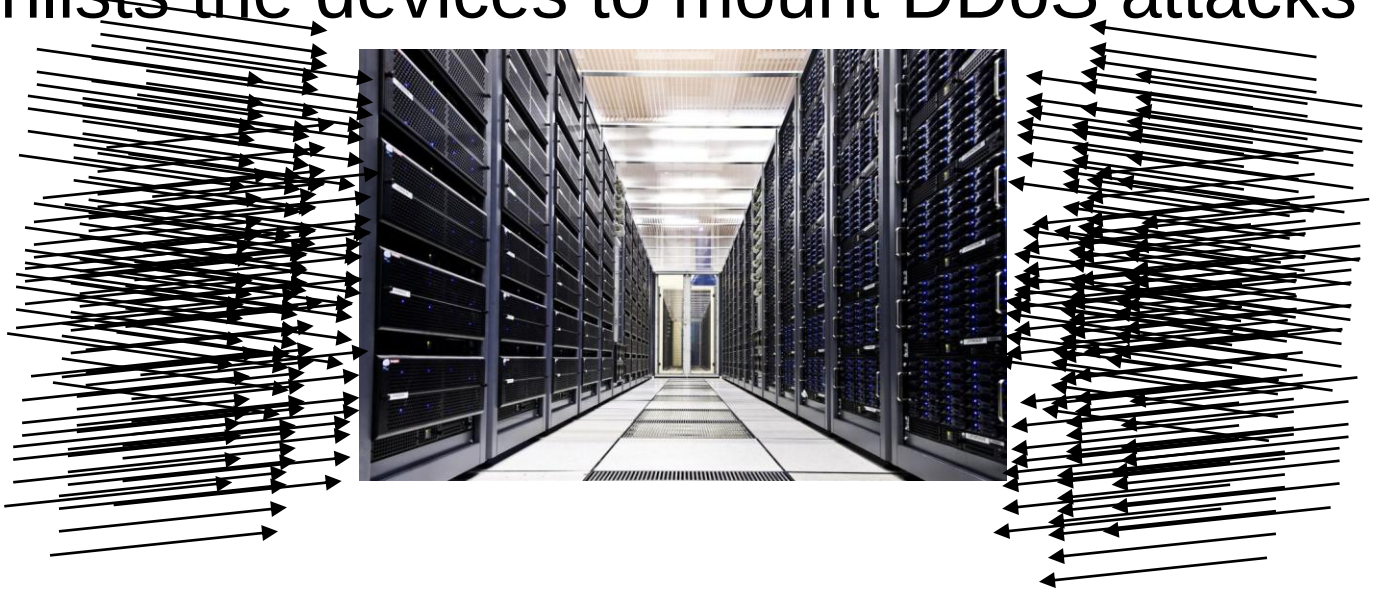
- Benefits of the Internet of Things
- Security risks – the Dyn Incident
- The issue
- The way towards a solution
- Summary

The Dyn incident – what happened

- Dyn is a DNS service
- Suffered DDoS 21 October
- Attack involved “tens of millions” of internet addresses
- Security firm Flashpoint confirmed attack used “botnets” infected with the “Mirai” malware

The Dyn incident – Mirai

- Scours the Internet for IoT devices
- Exploits easy-to-guess usernames and passwords
- Enlists the devices to mount DDoS attacks



The Dyn incident – the victims

- Well, not the owners of the enlisted smart devices
- But the users of Dyn
  - *Organisations such as Twitter, Spotify and Reddit*
- And the people that use these sites

The issue

- The attackers don’t own the infected devices
- The owners of the infected devices are not affected
- They don’t even know that their device is being used in this way
- Do they even care?

The way towards a solution

"For cyber reliance in such cases, one needs to look at the whole cyber eco system, and how each actor within the system interacts and can contribute to the problem and the solution"

Sabrina Feng, Rapporteur, ISO SC27 WG1 Cyber Security Study, October 2016

Can we look at the whole eco system?

- An organisation is “a person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives” [ISO]
- Most people think of a company as an organisation
- But what about
  - *A subset of a legal entity?*
  - *Sets of subsets of legal entities?*
  - *A whole nation state?*
  - *The whole world?*

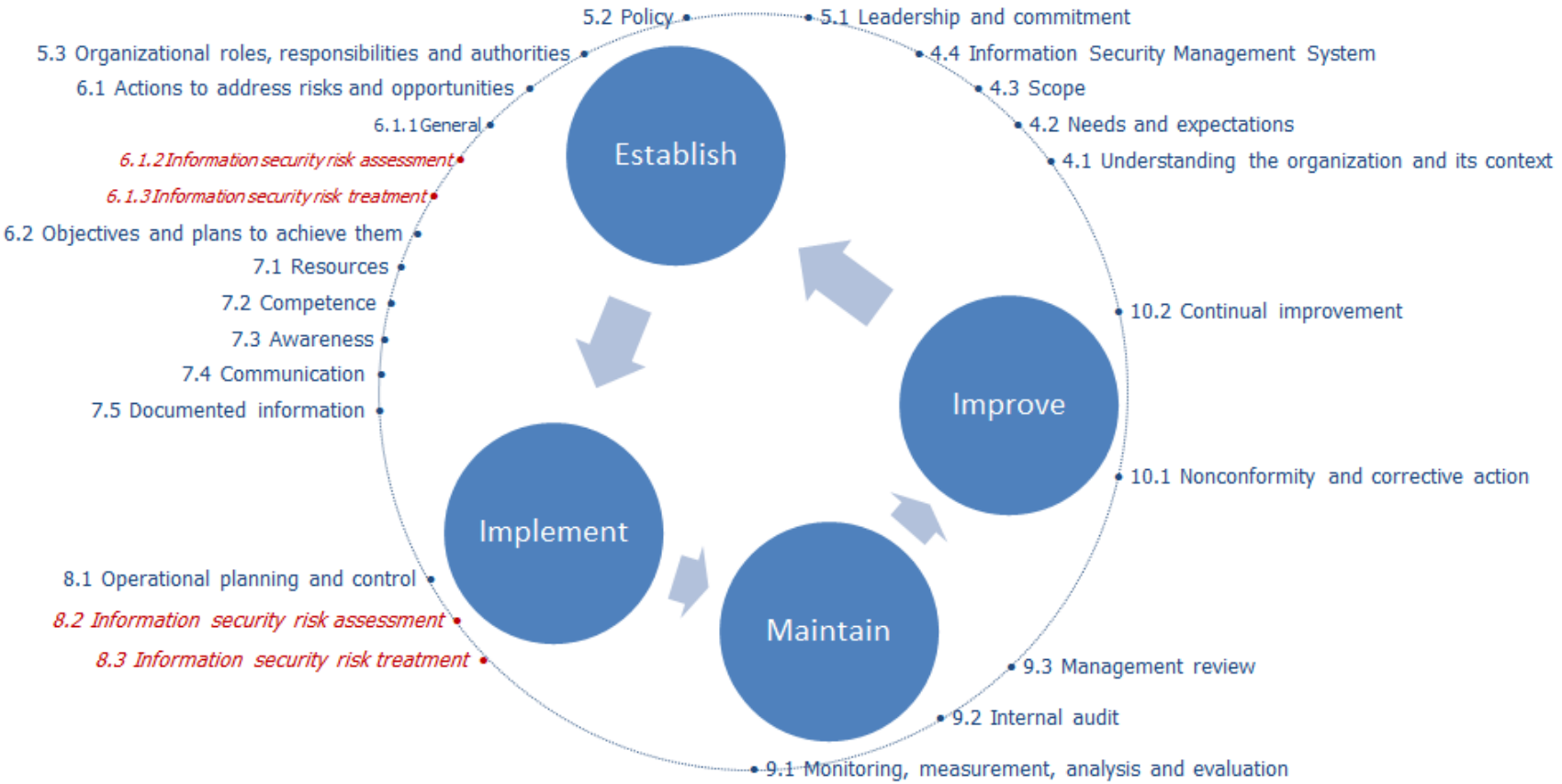
Information security in this context

- ISO/IEC 27001 is *the* standard for IS management
- It applies to an organisation
- So why not:
  - *Treat the nation state as a hierarchy of organisations*
  - *Subsets within subsets*

What is ISO/IEC 27001?

- International standard for information security management (2nd edition 2013)
- Designed for organisations to adapt to their business
- Specifies *what* not *how*
- Minimal requirements for documented information
- Emphasis is on results, not good intentions

Structure of the standard



Focus in risk management

- Consider risk in terms of events and consequences [ISO 31000 - Risk management - principles and guidelines]
- Study the cyber security problem for the whole cyber eco system at the national level
- Produce the Risk Treatment Plan (RTP)
  - *For such cyber issues*
  - *For the whole nation*

Risk treatments plans

- Associates events with consequences
- Determines necessary controls to modify risk (i.e. modify likelihood of occurrence and severity of consequence)
- **PREVENT**: a control that is intended to prevent the occurrence of an event that would otherwise lead to the occurrence of one or more consequences
- **DETECT**: a control that is intended to detect an occurrence of the event;
- **REACT**: a control that is intended to limit the consequence(s)

So why not just publish the RTP?

- There is more to defeating this type of attack
- We need to build a community
- People and organisation must feel part of it
- The RTP is prevent-detect-react
- The ISMS runs on a continuous improvement cycle
- Need to measure performance and effectiveness
- The threat landscape will change

Vision

- A hierarchy of ISMS
- The top level ISMS only deals with issues that affect the whole cyber eco system
- Lower levels inherit these RTPs
- Lower levels can adapt (augment) them
- Lower levels are free to create their own RTPs to deal with their own private issues

Summary

- Seen IOT devices turned into a DDoS weapon
- IOT owners are innocent participants
- For solution need to consider whole cyber eco system
- Can do this using ISO/IEC 27001 with organisation = nation state…

… a blue print for real cyber security

Any questions?