ICS Security DOs and DON'Ts

As experts in cyber security, we discuss some common points about the ICS environment

Remember the three pillars of information security:

1. Technical

This section highlights the technological defences that you can put in place in order to protect your infrastructure. Information security can be defined by the CIA rule - Confidentiality, Integrity and Availability.

2. Physical

As well as threats from bad actors on the internet, your data and systems need to be protected from accidental or deliberate misuse on site. Robust physical systems need to be in place to prevent unauthorised access.

3. Managerial

It is vital to your business that your systems remain secure. To this end, the business must be proactive in ensuring that there is a focus identifying and resolving risks posed by malware and other threats.

1. Technical

Dos

- Segregate operational systems from corporate IT systems
- Networks should be separate and only those services that need to traverse zones should be allowed through managed access controls
- Use specific engineering laptops for engineering jobs. Avoid the risk of contaminating the operational networks
- Restrict access to external systems from operational systems
- Understand and control remote access. Be sure to know where all external links to you operational networks are and that they are managed carefully
- Use individual login accounts wherever possible
- Keep login accounts up to date. Close down accounts when staff leave the business
- Control use of USB devices
- Keep systems patched to the latest versions

Don'ts

- Leave servers and workstations logged in
- Leave default users accounts and passwords active. Always change the default admin account password on all new systems
- Don't put login account passwords on display

capula

2. Physical

Dos

- Understand the basic tenets of physical security
  - Deter
  - Delay
  - Authorisation
  - Detect
  - Identify
  - Respond
- Keep systems in locked cabinets to prevent unauthorised local access
- Place operational systems in secure rooms and restrict access to only those who need it
- Be aware of physical intrusion devices, such as key loggers, wi-fi access points

Don'ts

- Leave cabinets open or unlocked after a job is complete or you're leaving the area for a while
- Allow access to restricted areas to unau thorised personnel
- Ignore possible cyber-related motives if a break-in is discovered. Theft may just be a cover for another motive especially on unmanned sites

3. Managerial

Dos

- Ensure that appropriate policies and procedures are in place and, importantly, are communicated across the business
- Create business continuity and disaster recovery plans
- Run test exercises regularly to familiarise staff
- Keep the plans up to date

- Know your incident handling process
  - Preparation
  - Identification
  - Containment
  - Eradication
  - Recovery
  - Lessons Learned

Don'ts

- Offload cyber security responsibiity to one person or team **Everyone contributes**
- Allow policies and procedures to gather dust. Technology changes rapidly so perform reviews regularly
- Assume that buying the latest security tools solves all risks. These technologies are only one layer in you cyber defences

Capula Limited | Orion House | Stone | Staffordshire ST15 OLT
t: +44 (0)1785 827000 e: sales@capula.co.uk
www.capula.co.uk