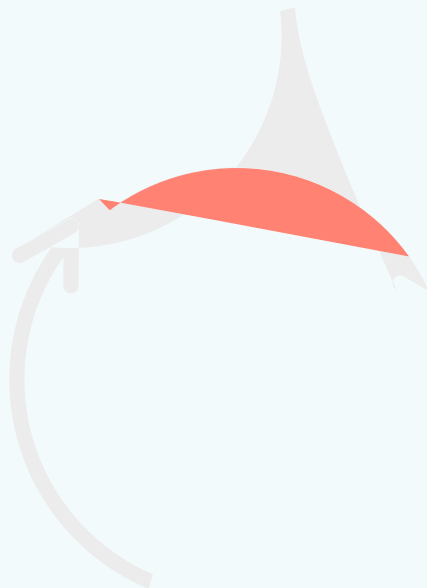


IoT and OT Ecosystem – Top Tips



responsible disclosure practices. Additionally, ensure you have a thorough testing regime which looks at negative testing (i.e. ensuring the device doesn't do things it shouldn't) and security testing to identify vulnerabilities.

Use Secure by Design and Default principles

Ensure security is embedded in your software development processes, to have the best chance of delivering a secure product. When deploying the devices, ensure the default settings are the most secure, for example;

- No default passwords, and force password changes on first login
- Disable insecure protocols
- Enable encryption as default where possible

These can be re-used across a range of clients with similar needs, allowing you to reduce the time needed for design and likelihood that risks could be introduced through deployment.

The patterns should include options for a range of resilience, backup and monitoring solutions that can be integrated into the overall installation.

For Consumers

Understand your responsibilities

Identify whether you have any legal responsibilities, for example if the devices collect personal data, and address these through technical and procedural controls.

Identify and manage risks

Understand how you use the solutions, and the associated risks. Where a risk is above your risk appetite, ensure that there are additional controls or mitigations to address this. If that is not possible, ensure your detection system would identify the risk if it is realized.

Understand and monitor the support model

If you are being supported by the Installer or Manufacturer, ensure you understand what support model is being paid for and check that it is being provided as expected. Identify where any provided support model does not address any of your responsibilities or risks and understand how you will close that gap.

Clearly define how your internal IT teams will work to support the connected OT (if at all) and where the lines of responsibility and escalation lie.

Use an asset register

Create an asset register which allows you to know what devices you have, their functions and data, where they physically are, and who has access to them. Assign a senior stakeholder to have overall accountability for the devices and any associated obligations and risks.

Monitor for 'Shadow OT'

Identify any areas where unauthorized OT devices may be introduced. Have clear and strong guidance on how new technologies are approved and formally introduced to your network, with training and education for staff.

Find out more

EMEA

Call: +353 1 210 1711

Email: cyber.ie@bsigroup.com

Visit: [bsigroup.com/cyber-ie](https://www.bsigroup.com/cyber-ie)

UK

+44 345 222 1711

cyber@bsigroup.com