Stakeholder Q&A: Understanding CySPAG for Specifiers, Consultants, and IT Departments

What is CySPAG?

CySPAG (Cyber Security Product Assurance Group) is a UK-based self-declaration scheme developed by the BSIA to promote cybersecurity best practices in the professional security sector. The scheme is designed to showcase that manufacturers and installers of security systems follow secure design, deployment, and lifecycle management practices.

Questions Specifiers & Consultants Might Ask

1. What does CySPAG compliance guarantee?
It ensures that manufacturers and installers adhere to BSIA-defined cybersecurity practices, including secure product design, update of IOT mechanisms, and responsible installation.

2. Is CySPAG recognised by UK government or regulatory bodies?
CySPAG aligns with UK cybersecurity principles and complements legislation like the PSTI Act, but it is not a formal government certification.

3. Can CySPAG be used as a procurement requirement?
Yes. Specifiers can include CySPAG compliance as a criterion in tenders to ensure cybersecurity accountability.

4. How does CySPAG compare to other schemes like UL 2900 or ETSI EN 303 645?
CySPAG is sector-specific and self-declared, whereas UL 2900 and ETSI EN 303 645 involve third-party testing and broader IoT coverage.

5. Is there a registry of CySPAG-compliant products or installers?
Currently, compliance is self-declared and documented via BSIA Forms 343 and 369. A public registry may be considered in future iterations.

Questions IT Departments Might Ask

1. Does CySPAG ensure secure network integration?
CySPAG promotes best practice of secure installations, including network segmentation, credential management, and update protocols. All systems should be tested by the solution provider.

2. Are CySPAG-compliant products tested for vulnerabilities?
CySPAG relies on manufacturer self-declaration rather than independent testing. It encourages vulnerability disclosure and patching.

3. How does CySPAG address supply chain risks?
Manufacturers must declare secure sourcing and firmware integrity practices, helping mitigate supply chain vulnerabilities.

4. Is CySPAG suitable for high-compliance environments (e.g., NHS, finance)?
It provides a strong baseline but may need to be supplemented with schemes like ISO/IEC 27001 or UL 2900 for regulated sectors.

5. How does CySPAG support lifecycle management?
It requires manufacturers to commit to update support and installers to inform clients about product lifecycle and patching.

Strategic Considerations

Is CySPAG scalable for enterprise deployments?
Yes, especially when combined with internal cybersecurity policies and procurement controls.

How often is CySPAG updated?
The BSIA reviews and updates CySPAG documentation periodically to reflect evolving threats and standards.

Can CySPAG be integrated into broader risk frameworks?
Yes. It complements existing cybersecurity frameworks and can be mapped to ISO, NIST, and ETSI standards.