CySPAG for Installers - Frequently Asked Questions

What is CySPAG for Installers trying to address in the security industry?

CySPAG for Installers is tackling a critical and often overlooked issue in the security industry: the **cyber resilience of physical security systems**. Here's a breakdown of what CySPAG is trying to address:

1. The Cyber Gap in Physical Security

- Many installers focus on physical setup—cameras, access control, alarms—but overlook the **cyber vulnerabilities** these devices introduce.
- IP-connected systems are now standard, but without proper configuration, they can be entry points for hackers.

2. Installer Responsibility in Cyber Hygiene

- Installers are often the last line of defense before a system goes live.
- CySPAG emphasizes that installers must:
    - Change default passwords
    - Disable unused services
    - Ensure firmware is up to date
    - Document configurations securely

3. Reducing Risk for Clients

- Poor cyber practices can lead to:
    - Data breaches
    - System downtime
    - Legal liabilities for clients
- CySPAG helps installers protect their reputation and their clients by promoting **secure-by-default** installations.

4. Lack of Standardised Guidance

- Until now, there's been no unified framework for installers to follow regarding cyber assurance.
- CySPAG provides **clear, practical guidance** tailored to the installer's role—not just manufacturers or IT teams.

5. Bridging the Gap Between IT and Security

- Installers often work in environments where IT teams expect secure integration.
- CySPAG helps installers speak the language of cybersecurity and collaborate more effectively with IT professionals.

Why It Matters

- **Cyber threats are evolving**—ransomware, botnets, and remote exploits are targeting physical security systems.
- **Installers are key enablers** of secure environments. Their actions during setup can either harden or expose a system.
- **CySPAG empowers installers** to be proactive, informed, and aligned with best practices—making them part of the solution, not the risk.

CySPAG for Installers - Frequently Asked Questions

How can the CySPAG for Installer Scheme help insurers clients, specifiers and end users of security systems deployed on IOT networks?

CySPAG for Installers plays a vital role in safeguarding clients, specifiers, and end users by ensuring that security systems deployed on IoT networks are not just physically robust—but **cyber resilient**. Here's how it helps each stakeholder:

For Insurers

- **Risk Reduction**: CySPAG ensures that installers follow verified cybersecurity protocols, reducing the likelihood of breaches and claims.
- **Audit Trail**: The scheme includes documentation and audit processes that insurers can use to assess risk exposure.

For Clients & End Users

Enhanced Cyber Protection

- Installers following CySPAG guidance ensure systems are configured securely from day one.
- This reduces the risk of data breaches, unauthorized access, and system hijacking.

Secure-by-Default Installations

- Default passwords are changed, unused services are disabled, and firmware is updated—minimizing vulnerabilities.
- Clients benefit from systems that are hardened against common cyber threats.

Reduced Liability & Downtime

- A compromised security system can lead to reputational damage, legal issues, and operational disruption.
- CySPAG practices help prevent these outcomes by embedding cyber hygiene into installation.

For Specifiers & Consultants

Confidence in Compliance

- CySPAG aligns with emerging standards and best practices for cyber assurance in physical security.
- Specifiers can confidently recommend solutions that meet regulatory and client expectations.

Improved Integration with IT Infrastructure

- Installers trained under CySPAG understand how to deploy systems that work securely within enterprise networks.
- This reduces friction between physical security and IT departments.

Better Documentation & Transparency

- CySPAG encourages proper documentation of system configurations and cyber controls.
- Specifiers gain clearer visibility into how systems are deployed and maintained.

For IoT-Connected Environments

Secure Connectivity

- IoT devices in security systems (e.g., cameras, sensors, access control) are often networked.
- CySPAG ensures these endpoints are deployed with secure settings, reducing the attack surface.

Awareness of Threat Vectors

- Installers are trained to recognize and mitigate risks like open ports, outdated firmware, and weak credentials.
- This proactive approach protects the broader IoT ecosystem from cascading vulnerabilities.

The Bottom Line

CySPAG for Installers transforms the installation process from a technical task into a **strategic layer of cyber defense**. It empowers installers to deliver systems that are not only functional—but **secure, compliant, and future-readv**.

CySPAG for Installers - Frequently Asked Questions

How can I join CySPAG for Installers Scheme?

How to Join as an Installer

To become a **CySPAG Registered Installer**, your organisation must:

- Submit a declaration showing compliance with the CySPAG 10-point plan and BSIA Form 369.
- Complete **Annex C** of the registration form.
- Provide proof of cybersecurity practices, including secure installation, update management, and vulnerability disclosure.
- Pay the registration fee, which depends on organisation size and BSIA membership.

Employees	Non-BSIA Member	BSIA Member
0–25	£99.00	£80.00
26–249	£199.00	£160.00
250+	£299.00	£240.00

Submit via Website or Email

Once you submit your initial enquiry and via the CySPAG website or via email info@cyspag.co.uk or technical@bsia.co.uk a member of the BSIA team will provide you with a copy of Form 369 and will be able to guide you through any of the 10 point plan should you have any questions.

Once accepted your organisation will be listed on the CySPAG website and granted use of the CySPAG registered Installer logo. Annual renewal is required to maintain your CySPAG status.

***The CySPAG scheme and 10 point plan is a copyrighted scheme by the BSIA and unauthorised use will result in legal action.