Remote Guarding – Red Flags

What Every Client Should Demand Before Deploying Remote Guarding

Why This Matters

Remote guarding does not increase security risks from camera malfunctions or analytics failures. While some systems perform better than others, overall, the products and services available today improve security programs and make sites safer. However, they can also significantly and unknowingly raise risks related to security, privacy, compliance, and reputation, depending on how operations are managed, who oversees them, and the standards, policies, procedures, and controls in place. Failures often arise from management choices and the standards they follow.

As the adoption of Remote Guarding becomes mainstream, concerning trends are emerging. Despite more reliable technology that seems effective and lower costs, many vendors are struggling to scale and operate from Remote Security Operations Centers (RSOC), which are often under-governed, loosely controlled, and poorly staffed. Clients have simply traded one risk for another.

Where Exposure Actually Occurs

Most vulnerabilities in remote guarding are not technical—they are **structural**. They occur where visibility, access, and human interaction meet. Not during installation. Not during detection. But during continuous **operation.**

Remote Guarding RSOC Red Flags

The following are the most common signs that a Remote Security Operations Center (RSOC) might be increasing risk instead of reducing it, or even creating new, unexpected, and hard-to-detect risks that are difficult to mitigate.

1. **Standards, Certification, and Compliance That Can't Be Verified**
   If a provider cannot clearly demonstrate independent certification, third-party audits, or compliance with recognized security frameworks, you are making assumptions. Professional, secure environments don't rely on trust—they depend on **verification**.

2. **Unclear Operating Environment**
   Where are your cameras actually monitored? If the answer is vague, inconsistent, or overly simplified, that's a concern. A legitimate RSOC operates within a **controlled, access-restricted environment —** not an undefined or distributed setting.

3. **Lack of Roles-Based Access Control**
   Not everyone should have access to everything. If live feed access becomes too widespread, poorly managed, or not clearly defined by role, your system risks

oversharing instead of protecting. Visibility should be **deliberate, limited, and well-controlled.**

4. **No Reliable Audit Trail**
   If activity cannot be traced—who accessed what, when, and why—there is no accountability. Without accountability, there is no control. A professional RSOC sees auditability as a fundamental **function, not an afterthought.**

5. **Undefined Data Handling**
   If policies regarding recording, storage, and sharing of video are unclear, undocumented, or inconsistently enforced, sensitive information becomes vulnerable. Video is not just footage—it is **data with legal and reputational consequences.**

6. **Operator Risk Is Ignored**
   Technology is only as well-managed as the people operating it. High turnover, minimal vetting, or lack of formal training create instability in what should be a carefully controlled environment. Consistency and discretion are not optional—they are **essential.**

7. **No Clear Jurisdictional Awareness**
   If a provider cannot explain how they handle privacy obligations across different jurisdictions, you could be unknowingly exposing yourself to regulatory risk. Compliance isn't a one-time task — it needs to be **integrated into daily operations.**

8. **Overreliance on Technology, Lack of Oversight in Governance**
   Advanced analytics and AI are often emphasized as key features. However, technology does not replace governance. If the focus is only on detection capabilities without equal attention to control and oversight, a vital element is missing.

What "Good" Looks Like

A well-designed RSOC is not only operational but also **disciplined**. It can clearly demonstrate consistency:

- Roles-based systems access control with reportable and auditable multi-factor authentication
- Controlled operating environments with managed access control and cameras.
- Structured and continuous onsite management and supervision.
- Comprehensive activity logging and accountability.
- Defined, documented, and auditable hiring, vetting, and training programs.
- Compliance with local, state, national, and international data protection and privacy requirements.

A Simple Reality

Remote guarding isn't inherently risky, but it greatly depends on the environment it operates in. Often, that environment receives less attention and is less secure than it should be, leading to a range of unexpected, unseen, and unknown new risks.

Final Thought

If you don't fully understand how your RSOC works, you don't genuinely understand your security program or risks. And—**you've outsourced more than just monitoring.**

Let's talk – Contact us at prf@s6rg.net or visit us at www.s6rg.net

About S6RG

Founded in 2012, **S6RG** is a strategic advisory firm that specializes in **physical risk, security architecture, and resilience planning** for organizations and private clients operating in complex or high-consequence environments.

We collaborate with clients to **identify, model, and mitigate physical risks** that typical security programs often overlook. Our method combines risk analysis, security engineering, governance, and operational strategy into a unified protection framework that withstands both foreseeable threats and unexpected events.

SBA U.S. Small Business Administration SERVICE-DISABLED VETERAN-OWNED CERTIFIED

S6RG is a Service-Disabled Veteran Owned Business certified by the U.S. Small Business Administration (SBA).

SBA SERVICE-DISABLED VETERAN-OWNED CERTIFIED