HiveWatch

Your Guide to Field Resources and Guarding Relationships

While guarding dates back to the Romans, many of the duties haven't changed much since then (even though business needs have).

Today, security teams are increasingly asked to do more with less, while effective guards seem to be a scarce resource. Too often the true measure of a guard's effectiveness only becomes apparent after an incident, and by then it may be too late!

> **Watch our webinar "Doing More with Less: How to Optimize Your Security Programs to Maximize Your Budget" here.**

And what about the organizations that don't or simply can't use guard services? These organizations still need someone on site taking ownership of physical security. In such cases, employees are often tasked with security duties outside of their job title. These other 'site liaisons' are required to fill the security gap, a job often met with hesitation and even resistance.

Despite the differing titles and roles, guards and other field resources share a common purpose – ensuring the safety and security of the organization. As a result, managing these resources effectively and efficiently becomes critical. Motivating them, setting clear expectations, and ensuring they are meeting those expectations requires a strategic combination of technology and people management.

DEFINING FIELD RESOURCES

Before diving into how to best manage field resources, it is important to define them.

Field resources will look different for every organization dependent on the organization's size, budget, location(s), etc. Generally, they will include one or more of the following:

In-House Guards

In-house guards are security personnel directly employed by the organization. These guards receive salary, time off, and other benefits just like other employees.

Pros:
- Have a more thorough understanding of the company's specific needs
- Have greater organizational buy-in as they are more embedded in company culture
- Allow for greater control over training and performance

Cons:
- Often more expensive due to the insurance the organization needs to have
- Potential for burnout because of monotony, leading to decreased effectiveness
- May require an additional full-time employee to manage guard compliance

Contracted Guards

The high costs and liability concerns associated with in-house guards may mean that many organizations choose to hire contracted guards. In this case, guards are employed by a third-party guarding service and deployed on-site at the contracting organization.

Pros:
- Brings specialized expertise and training provided by the third-party management company
- Allows organizations to scale security up or down as needed during temporary events or times of political/social unrest
- Offers cost flexibility by avoiding expenses associated with full-time staff

Cons:
- Contracting company has less oversight and control
- Quality can vary from provider to provider and even guard to guard
- May experience high turnover rates, resulting in a less consistent security presence

Virtual Guarding

Virtual guarding uses a combination of technologies such as video surveillance, artificial intelligence (AI), and remote monitoring to oversee physical security. Typically provided by a third-party service, virtual guarding leverages the contracting company's resources to remotely monitor live feeds and respond to incidents in real time.

Pros:
- Brings specialized expertise and training provided by the third-party management company
- Allows organizations to scale security up or down as needed during temporary events or times of political/social unrest
- Offers cost flexibility by avoiding expenses associated with full-time staff

Cons:
- Contracting company has less oversight and control
- Quality can vary from provider to provider and even guard to guard
- May experience high turnover rates, resulting in a less consistent security presence

Site Liaisons

Site liaisons are those employees that work for the organization but not primarily in a security role. They might be a receptionist, general manager, or administrative assistant tasked with handling on-site physical security incidents. This approach is most common among small businesses and smaller satellite operations within larger organizations.

Pros:

- ✓ Cost-effective solution for organizations with limited security budgets and low risk
- ✓ Does not require additional salaries or significant investment in training
- ✓ Familiarity with the organization's operations allows for a quicker response to incidents

Cons:

- ⚠ May lack experience in handling security incidents
- ⚠ Primary job responsibilities may conflict with security duties, leading to job dissatisfaction
- ⚠ Limited effectiveness if not properly supported with clear expectations, communication tools, and/or remote support

Hybrid

Most organizations deploy a hybrid approach, combining various field resources to create a solution tailored to their needs, budget, and risk profile. This model leverages the strengths of each resource while addressing their weaknesses.

For example, in-house guards handle day-to-day operations and build company-specific knowledge, while contracted guards provide additional support during peak times or special events. Similarly, virtual guarding serves as a complement to all available field resources, offering continuous surveillance when on-site resources are stretched thin. Site liaisons then act as a first line of response, integrating with both in-house and third-party resources to address immediate security concerns.

A well-coordinated hybrid approach ensures that organizations benefit from flexibility, cost-efficiency, and comprehensive coverage. By strategically combining these resources, organizations can create a robust, adaptable security framework that meets their unique needs.

Hybrid Approach In Practice

Managing field resources becomes more complex among larger (and more complex) organizations. Consider a multinational aerospace corporation with multiple outposts in different countries, each varying in size, risk, and compliance requirements. In this case, the organization would consider the following hybrid approach:

- In-house guards deployed at key locations where high security and integration with specific protocols are crucial, such as corporate headquarters or sensitive research facilities.

- Contracted guards employed at sites with varying risk profiles, providing temporary staffing solutions as needed. This often involves working with multiple vendors, each with their own rules of engagement.

- Virtual guarding services used for continuous monitoring across all sites, or even larger sites where on-site guards can't quickly access areas.

- Site liaisons handle smaller or remote outposts where full-time security is not required.

The specific combination and deployment of field resources depends on your organization's unique needs and circumstances. Regardless of these factors, it is important to build strong relationships with each field resource group to maximize their potential. Knowing what makes each group "tick" helps to tailor management approaches and communication strategies. It also creates shared trust that ultimately benefits your organization's overall security posture.

WAYS TO BUILD STRONG RESOURCE RELATIONSHIPS

It's no secret that finding and keeping reliable guards is difficult in the current environment. According to the Service Employees International Union, the largest private security officers' union in the country, the national annual turnover rate for security guards is estimated to range from 100% to 300%. This can be attributed to several factors including low wages paired with high risk. As such, building a solid relationship with your guards and other field resources is imperative if you want to attract and retain top talent.

Here are 10 ways you can build strong relationships with your field resources:

1. **Motivate with intention:** Guarding is very much still seen as an entry-level position with historically low wages. Money can be a great motivator, especially for contracted guards, while in-house guards will appreciate a clear path to career growth.

2. **Communicate clearly:** Provide concrete examples and practical tools to make expectations as clear as possible. Show, don't just tell.

3. **Set reasonable expectations:** It is not reasonable to expect a 5-minute response time of a guard working on a 1,000-acre campus. This is why Service Level Agreements (SLAs) guided by data are critical when contracting guard services – but more on that later.

4. **Be inclusive:** This is especially critical when it comes to contracted guards. Include them in things like company events to foster a sense of belonging and loyalty.

5. **Promote open dialogue:** Create a point person with whom field resources can speak candidly. This point person can help with answering day to day questions, scheduling concerns, addressing internal drama, etc.

6. **Provide training:** Regardless of the resource, it is important to invest in additional training such as situational awareness, negotiation, communication, and more. This investment has long term ROI by increasing both effectiveness and retention.

7. **Increase engagement:** Many guards entering the workforce are Millennials and Gen Z, who may require more stimulation to stay engaged. Allowing them to listen to music on their guard tour or gamifying their tasks can help keep them motivated and focused.

8. **Manage with respect:** Disrespect in the workplace can be enough to turn a good guard into a bad actor. Ensure you treat all your resources, third-party or otherwise, with respect to maintain a positive, productive environment.

9. **Define boundaries:** It is not the role of a contracted guard to take out the trash nor is it a receptionist's responsibility to physically engage a trespasser. Ensure each field resource understands their specific duties to prevent misunderstandings and unmet expectations.

10. **Educate internal teams:** It is important that internal teams outside of security also understand the role of each field resource. Bringing them into the conversation helps foster a collaborative environment where everyone respects the boundaries and responsibilities of security personnel.

Effective management and communication are key to aligning your resources and maintaining a cohesive security strategy across an organization. But this begs the question: How do you standardize management and communication across a combination of field resources to create uniformity where none seemingly exists?

Answer: Data.

USING DATA TO IMPROVE YOUR FIELD RESOURCES

Regardless of the type of field resources you deploy, it's safe to say that a large amount of manual work is being done by these resources to identify, respond to, and track security incidents. Not only does this cause inefficiencies in the security workflow, but also makes it difficult to track the efficacy of such resources.

Every organization's security workflow and incident management reporting will also look different based on their specific needs, industry standards, regulatory requirements, etc. In most cases, incident reports are there to track things like the nature and frequency of incidents, response times, resolution outcomes, and any patterns or trends that may emerge. This data is crucial for assessing the performance of field resources, identifying areas for improvement, and refining security protocols to enhance overall effectiveness.

But while you may think your incident reports are providing you with the accurate data you need, you may want to think again.

The data provided by various reporting tools is often inconsistent, inaccurate, and inapplicable. When contracting multiple guard services, reports are likely to be delivered in different formats with varying metrics. Some may come in an Excel spreadsheet, others via proprietary software. Integrating such data into **your existing tech stack** then becomes extremely difficult, if not impossible. Additionally, site liaisons may be gathering different data or not gathering data at all, creating challenges in aggregating and analyzing information effectively.

Finally, consider that many incident reports are filled out after an incident has occurred, not as it happens. And given that contracting organizations have historically had little control over their third-party reporting, you have to trust these reports are accurate.

This lack of consistency and delayed reporting makes it difficult to make informed decisions in real time, as there is no reliable way to confirm data accuracy.

But here's what can happen when you are armed with the most accurate and consistent data.

Accurately Evaluate Your Current Resources

- Assess the performance of each field resource by analyzing accurate data on dispatch rates, response times, and the frequency of their dispatches. This allows for a granular evaluation of which guards are the most responsive and effective.

- Evaluate the effectiveness of current guard posts and tour designs. Adjusting the placement of posts or the scheduling of **Guard Tours** based on incident data optimizes guard coverage and response times.

Improve Your Field Resources

- Use data to identify training needs or performance issues. For instance, if certain guards are consistently slow to respond or have high incident resolution times, implement targeted retraining or adjustments in staffing.

- Having a single source of truth allows for more confident decision-making. This includes decisions related to staffing, resource allocation, and operational adjustments.

Integrate With Existing Security

- With consistent data, security incidents from multiple sources can be consolidated into one platform, avoiding the fragmentation often seen with different guard companies and security systems.

- Whether the incident comes from a camera feed, an access control alert, or a manual report, there is a single source of truth and consistent reporting format.

Move to a Predictive Security State

- Use historical data to predict potential security incidents and allocate resources more effectively. By understanding patterns and trends, you can proactively address vulnerabilities before they escalate.

- Implement predictive analytics to anticipate high-risk areas or times, enabling preemptive measures and optimized resource deployment.

> Building an effective security program is essential. Download our guide "Your Guide to: Security Program Effectiveness" **here.**

Justify Security Spend

- Use data to demonstrate the value and necessity of security investments when advocating for increased security spend.

- Accurate records provide tangible evidence of security operations, helping to justify expenses

> Part of justifying security spend is speaking the language of your leadership. Watch our webinar "Speaking the C-Suite Language: Navigating Buy-in for Security from Decision Makers" **here.**

Create and Enforce SLAs

- Leverage detailed data to establish performance SLAs with your guarding vendor that include metrics such as timely responses, zero open shifts, effective incident resolution, and accurate closure.

- This data can then be used to objectively measure adherence to these SLAs, ensuring that all tasks are completed as expected and within agreed timeframes.

For example, if your SLA denotes that mean time to resolve incidents will be 15 minutes or less, but certain sites are trending closer to 20 minutes, you can demand corrective action and mitigation plans from your vendor as outlined in the SLA. Take it one step further by tying bonuses or other rewards into meeting or exceeding SLA targets. This approach not only motivates better performance but also helps align third-parties with internal organizational objectives.

Looking for more info? **Watch our on-demand webinar** "How to Transform Traditional Guarding Infrastructure for Modern Security Demands."

Question to Ask Your Guarding Vendors Regarding SLAs

Go beyond the basics (confirming insurance, licenses, standard operating procedures) to determine the specific performance metrics, response protocols, and accountability measures that your guarding vendors will adhere to.

1. What tools or devices do you use to ensure accurate and consistent reporting? Who is responsible for these tools?

2. What Key Performance Indicators (KPIs) are guaranteed (mean time to acknowledge an alarm, mean time to resolve, number of open shifts, etc.)?

3. How do you track and report on response and resolution times for incidents? Does this system work in real time?

4. How is the data gathered from your reporting system delivered and what happens to the data upon termination of the agreement?

5. How do you handle non-compliance with SLAs?

6. What incentives or penalties are included in the contract to ensure SLA adherence?

7. What is your policy for replacing guards who fail to meet SLA standards within a specified timeframe?

OPTIMIZING FIELD RESOURCES WITH HIVEWATCH

In the complex (and often confusing) world of field resource management, let **HiveWatch** be your guide.

HiveWatch is a comprehensive **GSOC Operating System** designed to enhance the efficacy of your security operations by automating and standardizing processes related to field resource management. By leveraging HiveWatch, you can precisely tailor your field resources over time through data-driven insights and performance evaluations.

HiveWatch starts by **consolidating various functions** used by field resources into a single application. This unified approach allows multiple users –without restriction on the number of users– to report on various types of incidents directly from their mobile devices. This means that regardless of role, everyone is equipped to report security, safety, or compliance issues seamlessly through the same intuitive interface.

It also means that the **data gathered** (incident acknowledgments, response rates, time to resolve, etc.) is standardized across an organization regardless of location, user, etc. By centralizing field resource management, HiveWatch enhances coordination across multiple sites and providers, providing consistency and continuity in your security operations.
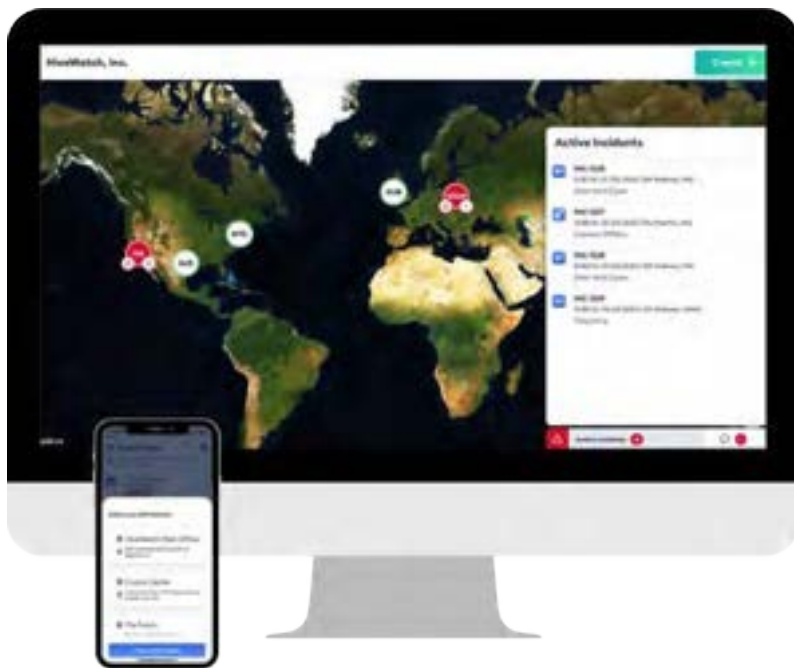
HiveWatch then uses this **standardized data** to deliver actionable reports and insights related to all aspects of field resource operations.

- The site liaison responsible for security has a high number of alarms that go ignored? It's probably time to sit down with them and clarify expectations.
- One area of your facility has more regular alarms than the others? Perhaps that area needs more frequent guard presence than others.
- One of your in-house guards has a higher mean time to acknowledge than their coworkers? It might be time for a raise or promotion.

With HiveWatch, you are equipped with the accurate, consistent data you need to optimize your field resources and ensure their continued efficacy. This moves you from a reactive state of security to a proactive and even predictive one.

Lastly, HiveWatch integrates with your existing tech stack to support dynamic communication between field resources and central security operations. For example, when a security incident is detected, HiveWatch can **dispatch notifications** directly to the relevant field personnel. It also integrates with video surveillance and access control systems to pull any relevant footage or data, streamlining the response process and ensuring the delivery of actionable information in real-time.

Use HiveWatch to not only monitor and manage your field resources more effectively but also continuously refine your security processes for improved operational efficiency and better security outcomes.

Contact HiveWatch today to speak to one of our security specialists about your organization's needs.

Hive**Watch**