HiveWatch

Your Guide to: Security Program Effectiveness

4 things to consider when building your program

At its most basic, a security program exists to protect its assets and personnel from numerous ever-evolving threats. But security leaders know that this over-simplified definition does little to provide overarching context into the pieces of the puzzle that need to be in place to truly meet the safety and security needs of the organization.

In this sense, security leaders not only become security experts, but must don their business hats to provide C-suite leadership with the full picture of how the security program effectively pushes the organization's goals forward and contributes in a meaningful way.

This eBook covers the basic tenets of a security program, along with tactical necessities used to build a security program for your organization. More importantly, it covers the four considerations that need to be made when assessing your security program for its effectiveness:

1. **Baseline creation**
2. **Benchmarking goals** (and whether your organization needs them)
3. **Determining return on investment (ROI)** (and communicating it to the C-suite)
4. **Investing in technology driven by business goals**

WHAT IS CONSIDERED A SECURITY PROGRAM?

A security program is the organization's security policies, procedures, tools, and controls that are in place to protect the organization. Oftentimes in physical security, security leaders are tasked with ensuring the security program is in place to protect the organization from risk; but it's more complex than that when it comes to communicating security's value.

A robust physical security program incorporates a variety of measures and practices to mitigate risks and ensure the safety and security of an organization's resources.

Some of the key tactical components of a security program might include these basics:

Risk assessment: Identifying potential physical threats and vulnerabilities, evaluating the likelihood and impact of various security incidents, and prioritizing risks to focus on the most critical.

Security policies and procedures: Establishing clear guidelines and protocols for maintaining security, defining roles and responsibilities for security personnel and other staff, and outlining procedures for responding to security incidents and emergencies.

Access control: Implementing systems to control who can enter and exit the premises, using various tools and technology to monitor access, and restricting access to sensitive areas.

Surveillance: Installing cameras and other monitoring equipment to observe and record activities, using security personnel to patrol and monitor the premises, and ensuring that surveillance systems are regularly maintained and monitored.

Physical barriers: In some cases, this means deploying barriers such as fences, gates, and bollards to prevent unauthorized entry, using security locks, reinforced doors, and windows to protect buildings, and designing the physical layout of a space to enhance security and visibility.

Lighting: Using adequate lighting and motion-detected lighting systems around the perimeter and within the premises to deter criminal activity.

Alarms and detection systems: Installing intrusion detection systems to alert in the event of unauthorized entry, using fire alarms and smoke detectors to protect against fire hazards, and investing in environmental monitoring systems for hazards like floods or chemical leaks.

Emergency response planning: Developing and practicing emergency response plans for various scenarios, training staff on how to proceed in the event of a security breach, fire, or other emergencies, and coordinating with local emergency services for efficient response.

Security personnel: Hiring and training security resources (whether it's staffing a global security operations center (GSOC), field resources, or guarding personnel) to monitor and protect the premises, equipping these staff members with the necessary tools and communication devices, and ensuring ongoing training is performed.

Ongoing maintenance and review: Regularly inspecting and maintaining all security systems and equipment, reviewing and updating security policies and procedures to address new threats and vulnerabilities, and conducting periodic security audits and assessments to ensure the effectiveness of the program.

While these are high-level components of a security program that, taken together, are supposed to offer increased protection from threats, it's always critical that security leaders continue to monitor trends, assess performance, and adjust accordingly.

This eBook aims to provide security leaders with four steps to take when assessing an existing security program (and what to do when there might be something lacking).

STEPS TO TAKE WHEN CREATING AN EFFECTIVE SECURITY PROGRAM

In a recent webinar from *Security Magazine*, 54% of attendees reported that the biggest challenge their security program faces is budget-related, followed by inefficiencies at 20%. While there are significant discussion points to be made about the state of physical security investments, it's critical to note that a lot of spending goes into maintaining the status quo around security programs without truly diving deeper into how a program contributes to overall business goals. In doing so, security leaders miss out on the chance to optimize resources for use in other departments, spreading out the ability to invest in new technology with data that is shared across teams.

Maintaining an effective security program, therefore, becomes an essential piece of the puzzle, driven by the need for security departments to justify additional investments in technology that keep people, customers, and assets safe from threats.

Here are four steps to take when evaluating your security program and determining whether it's working for the organization:

1. CREATE A BASELINE

Creating a baseline for reporting the effectiveness of a security program begins with establishing data and KPIs that will be assessed. Security leaders must also understand how the performance of the security organization works in tandem with the needs of the business. A lot of times, security operates in a vacuum. But security leaders need to understand the strategy of the business.

One piece of advice is to spend some time with senior leaders in the organization and ask them questions, such as, "Where do you see the company going?" and, "Are we scaling globally, or staying domestic?" The answers – using data – can better inform the actions of the security program as it relates to risk. For example, if security is focused domestically and the business is looking to expand globally, those goals are misaligned. Being able to match what the security team is trying to achieve with what the business needs is critical.

It's important to look at what the risk is to the business if you go offline because of a security incident. Make sure as a security leader, you're gathering data and information about the impact to the business, response time, and how that mitigates risk to the C-suite.
Creating a baseline should start with the following:

- Gain a holistic view of what data points are collected today
- Align the business strategy, prioritize based on what's known
- Develop goals that are measurable
- Be flexible

The bottom line is: Put these steps into practice in a blame-free environment that focuses on continuous improvement.

2. RECONSIDER BENCHMARKING GOALS

A lot of organizations seek understanding about their business and security programs by benchmarking themselves against their peers. This means looking at your competitors to figure out what they're spending on security programs, how they're performing, and how you measure up. But this might not be the best approach.

Benchmarking can be a useful tool, but like any tool or process, it's important to identify the desired outcome from the comparison at the beginning of the exercise.

It might be prudent to ask questions of your security leadership, such as, "Are you seeking to understand the program's maturity? Do you want to understand if the coverage allocation for an executive is appropriate based on their unique profile? Do you want to leverage the comparison to craft an effective business case for more resources?" This will help define if this is the best approach.

The bottom line is: Organizations are unique in terms of priorities, risk exposures, and risk appetites, so it's important to think about these things before you rely too heavily on peer benchmarking.

3. FOCUS ON MEASURING ROI

In addition to the baseline and benchmarks, security leaders need to be able to measure ROI on the tools and resources they use in their programs. This is one of the most critical steps toward ensuring the C-suite understands the value that security brings to the organization.

In short: It's difficult to conceptualize how a security program is performing without first knowing the metrics that you're competing against. Measurement cannot happen without the data.
For example, in a GSOC, there is a rich subset of data that can be used. Using this data to approach

other stakeholders, you can paint a picture for them. For example, we've realized operators spent XX minutes triaging a call in our GSOC, and we need to shoot for XX minutes. Framing the improvements in ways that leaders can understand makes it more likely that you can ensure buy-in and investment.

As another example, leveraging existing incident frequency data, you determine that static posts (where guards are in a fixed location) are inefficient at 50% of facilities. You deploy a new guard tour technology and decrease ineffective guard spend by 30%. This proves ROI to leadership by providing real-time analysis. Data remains a critical piece of the puzzle.

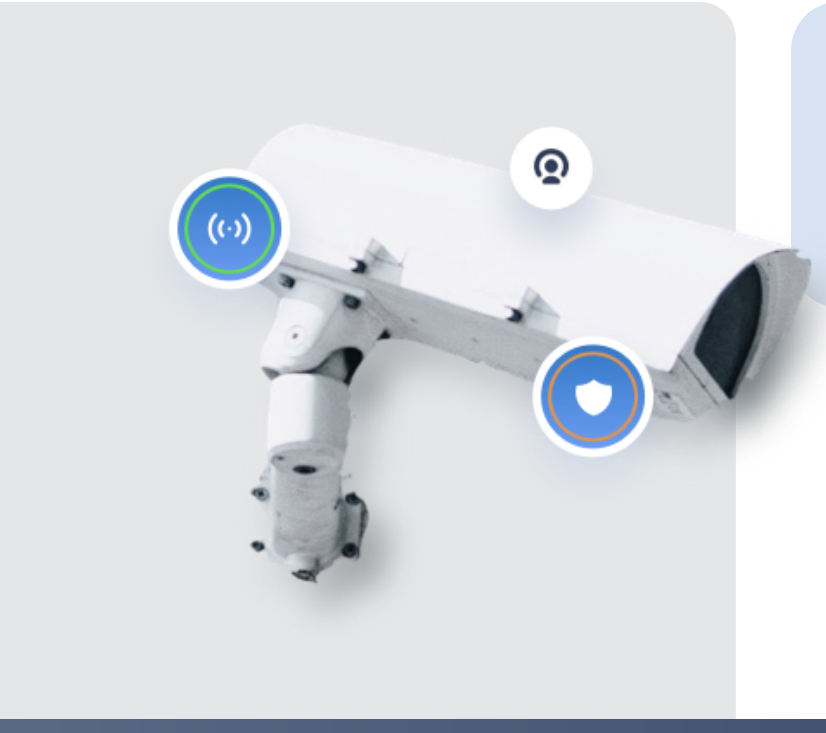
The bottom line is: Organizations that have a security program with a strong internal brand that is able to continuously communicate its value add into the C-suite, with data to back it up, are the most effective.

4. CONSIDER TECHNOLOGY INVESTMENTS THAT MEET PROGRAM GOALS

When considering technology investments to reduce risk, it's important for buyers to take a risk-based approach to acquisition. Before investing in a specific solution, do the following:

- Audit internally to avoid redundant tools
- Consider point versus complementary solutions
- Assess data ownership and access
- Ensure flexibility and future-proofing related to strategic roadmaps

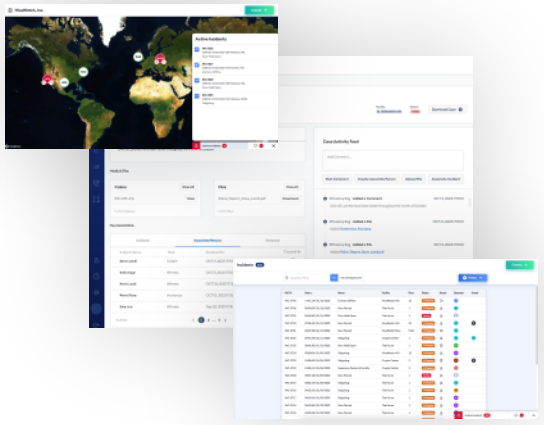
The best technology investments highlight security program metrics that can be used to showcase the benefit of security to the broader business (see our first point above).



The bottom line is: Without the data-driven insights to support technology investments and the outcome it can have on your program, security can often get lost in the discussion as a "cost center" rather than a business enabler.

HOW HIVEWATCH CAN HELP DRIVE SECURITY PROGRAM EFFECTIVENESS

HiveWatch provides security leaders with one of the most critical components of security program effectiveness: data.



The **HiveWatch® GSOC Operating System** allows security teams to bring together information and data from multiple technologies and disparate systems into a single platform that improves their overall security posture, reduces noise and complexity, and delivers more intelligence across the organization. Security leaders can then take this data to ensure security is aligning its goals and objectives to those of the organization.

The **HiveWatch® Command Center** is perfect for security teams looking to better manage their operations and facilitate more effective communication without device connectivity. Centralizing security resources, such as standard operating procedures, guard/field resource communication, emergency response, case and incident management capabilities, device health, and much more can lead to more efficient response and streamlined management of operations. Taken together, this can mean better resource alignment and cost savings.

To support security program effectiveness, HiveWatch captures baseline systems data ahead of implementation, then we help customers design their ROI models to capture things like:

- Operator and guard response time
- Device health and impact to integrator contracts
- Guard compliance with SLAs
- Incident trends to drive resource allocation

Learn more at www.hivewatch.com

HiveWatch