SECURITY FRAMEWORKS | ONTIC

REPORT

The State of Data Analytics in Physical Security:

Adoption, Challenges, and Opportunities

Table of Contents

Introduction

As physical security has become more digitized, organizations are now generating unprecedented volumes of data from cameras, access control systems, incident and case management platforms, risk intelligence feeds, and connected sensors. For chief security officers (CSOs) and senior security leaders, the central question is no longer whether data exist, but whether those data are being translated into timely insights that improve risk outcomes, optimize resources, and inform strategic decisions.

At the same time, advances in analytics, business intelligence, and artificial intelligence have raised expectations from executives that physical security should demonstrate the same level of analytic rigor as finance, operations, and cybersecurity. Yet, despite widespread investment in tools and technology, the maturity and impact of security metrics programs remain highly uneven across the industry.

This report presents findings from a cross-sectional survey of physical security professionals that examines "The State of Data Analytics in Physical Security: Adoption, Challenges, and Opportunities." Using the Clark and Estes KMO gap analysis framework, the research explores how knowledge, motivation, and organizational influences shape the adoption and maturity of security metrics and analytics programs. The results highlight a critical reality: simply deploying new tools does not guarantee better decisions. And neither does simply collecting data. Adoption and impact depend on whether practitioners have the skills and confidence to use analytics, whether they are motivated to incorporate data into daily work, and whether structures such as metrics programs, review cadences, and leadership expectations support or inhibit data-driven practice.

The remainder of this report moves from diagnosis to action. It begins with a summary of key findings, then explores in more detail the current state of analytics adoption, knowledge and skills gaps, motivational factors, and organizational barriers. Building on these insights, it introduces a four-level Security Analytics Maturity Model and a practical KMO-aligned roadmap that CSOs and security leaders can use to progress from ad-hoc, informal reporting toward an integrated, insight-driven security analytics capability.

Survey overview

The survey was conducted by Security Frameworks, a firm specializing in security metrics strategy and data analytics advisory, and Ontic, a security platform that centralizes intelligence, research, investigations, and program metrics for enterprise and government organizations. The results explore how security leaders measure performance and demonstrate impact.

Respondents were security professionals and corporate and enterprise security leaders from the United States and more than 35 other countries. Respondents spanned a range of roles, from analysts and managers to directors, CSOs, and deputy CSOs, and most brought more than a decade of experience to their responses, offering a seasoned perspective on the realities of analytics adoption. Their answers provide a multi-layered view of how security data is collected, analyzed, and used in practice today. See "Methodology" on page 19 for more survey details.

Key findings

The research shows an industry that values data analytics in physical security but struggles to apply it consistently and effectively. The core issue isn't a lack of data, it's a misalignment between what security teams know, what drives them, and how their organizations support analytics.

1 Knowledge gap remains a barrier to adoption.

Familiarity with security metrics, data analytics techniques, and analytics tools is at varying levels of knowledge amongst security professionals, with a substantial portion indicating only limited familiarity with key concepts and tools. This suggests an uneven foundation of core analytical competencies across the industry.

2 Analytics is valued, but confidence is limited.

Most security professionals rate the collection and analysis of security data as important or extremely important to their role and say they would attend analytics training if it were offered. At the same time, many report only moderate confidence in their ability to perform data analysis or use analytics to improve their programs.

3 Formal metrics programs are emerging, not yet embedded.

A majority of respondents indicate that their organization has, or is developing, a security metrics program, but many describe it as still "developing" rather than "established" or "optimized." In many organizations, metrics are collected and sometimes reported, but not always analyzed, and not consistently used to drive decisions.

4 Organizational barriers outweigh lack of interest.

When asked about the biggest obstacles to stronger analytics, respondents most often cite lack of leadership support, insufficient resources (budget, personnel, tools, training), and organizational resistance to change. This suggests that motivation is present, but structures and support have not kept pace.

5 Scope and integration of metrics remain limited.

Metrics commonly cover incidents and investigations, but fewer programs systematically measure performance across areas such as staffing, training, technology uptime and effectiveness, threat management, and protective intelligence. Dashboards and integrated views are emerging, but are not yet universal.

6 Maturity is clustered at the lower and middle levels.

Applying the KMO based Security Analytics Maturity Model, most organizations fall into the "Aspirational" or "Developing" levels, with fewer reaching "Proficient" and only a small minority operating at an "Optimized" level where analytics are deeply integrated into enterprise risk and business decision-making.

The rising importance of analytics in physical security

Over the last decade, physical security has become increasingly data-rich as organizations deploy AI-enabled video surveillance, access control systems, incident management platforms, risk intelligence sources, and a wide range of IoT devices. These technologies generate large volumes of events, logs, alarms, and operational data that can be analyzed to improve incident response, asset and brand protection, and organizational resilience. Non-incident driven data, such as security tasks, guard tours, calls for services, and many other routine security tasks can have a significant impact on data-driven insights. However, research and practitioner experience suggest that physical security has historically lagged behind domains such as IT security and finance in its systematic use of analytics, often relying on anecdote and experience instead of structured metrics.

Incident management systems are a critical data backbone for any serious security metrics program because they centralize and structure the full lifecycle of events, alerts, incidents, investigations, operational tasks, and outcomes in a way that can be analyzed over time to inform risk decisions. Additionally, link analysis across various data points can be significantly enhanced when a centralized incident management system is used to collect and analyze security data enterprise-wide. When incident, case, and guard activity data are consistently captured with locations, classifications, and resolution details, they create the longitudinal dataset needed for predictive analysis, allowing teams to identify recurring hotspots, precursors to serious events, and workload trends that signal emerging risks. A well-maintained persons of interest (POI) database further amplifies this value by linking incidents, behaviors, and watchlist subjects, enabling analytics to surface connections between repeat actors, locations, and modus operandi that would be difficult to see in siloed reports.

> **Physical security has historically lagged behind domains such as IT security and finance in its systematic use of analytics, often relying on anecdote and experience instead of structured metrics.**

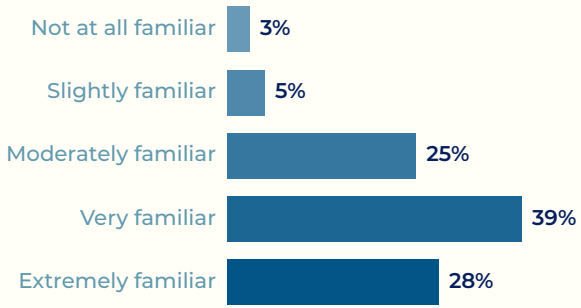
Despite this potential, the survey suggests that many security teams underuse the data available from their incident management, security tasks, access control, and related systems. While data are collected, consistent metrics, analytical methods, and decision-oriented visualizations are not yet standard practice across the industry.

Knowledge and skills:
Analytics capability is uneven

Familiarity with security-related data

Across the sample, physical security professionals report widely varying levels of knowledge and skill in data analytics. Some respondents, often in larger organizations or more technical roles, describe themselves as very or extremely familiar with collecting and analyzing security-related data, working with security metrics, and using tools such as dispatch, incident management, and case management platforms. Others, particularly in smaller teams or non-technical roles, report that they are only slightly familiar or not at all familiar with these practices.

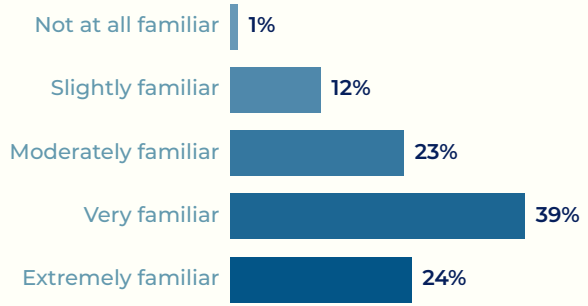
How familiar are you with the collection and analysis of security-related data?



Familiarity with the use of security metrics

Self-reported confidence in performing data analysis and using analytics to measure and improve security programs is generally lower than familiarity ratings, highlighting a critical gap between conceptual understanding and practical capability. Even among respondents who indicate moderate familiarity with analytics concepts, many rate their ability to conduct analyses and generate useful insights as only slightly adequate or moderately adequate. Visual analytics and data storytelling skills appear especially underdeveloped: respondents report lower familiarity with creating analytical graphs, dashboards, and visual reports than with basic data collection, suggesting that even where data are captured, they are not always translated into clear, decision-ready formats.

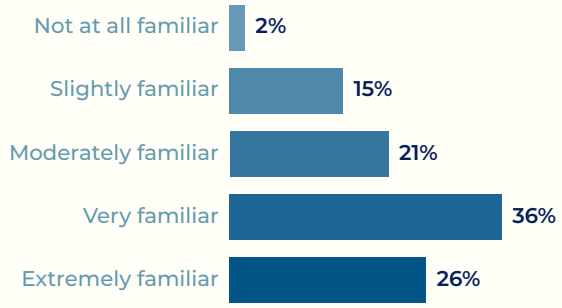
How familiar are you with the use of security metrics? (Security metrics are measurable indicators used to assess the effectiveness, efficiency, and risk management of security operations and programs, e.g., incident response times, access control violations, or security system uptime, guard tour completion rate).



Familiarity with data analytics

When it comes to familiarity with data analytics, 38% of security professionals reported not at all familiar to moderately familiar, highlighting gaps in knowledge and general understanding of data analytics, such as collecting, processing, and analyzing security-related data to identify patterns and insights.

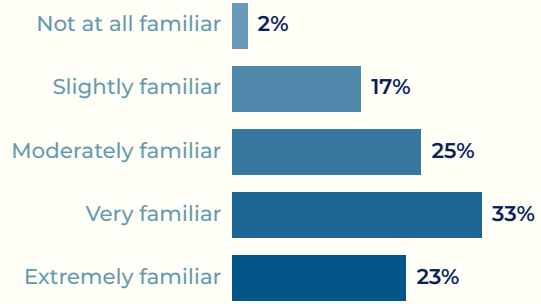
How familiar are you with data analytics in the context of physical security? (Data analytics involves collecting, processing, and analyzing security-related data, such as incidents, access logs, investigations, alerts, and risk assessments, to identify patterns, trends, and insights that support decision-making and improve security operations).



Familiarity with tools and applications

Familiarity with tools and technology to aid data collection and analysis is another area of opportunity for security professionals. While 56% of survey respondents indicated they are very familiar to extremely familiar with tools and applications, 44% of respondents reported they are not at all familiar to moderately familiar in this area. Procedural knowledge in incident management systems and various tools generally used for data collection and analysis is a prerequisite in establishing the confidence and motivation for such tasks.

How familiar are you with utilizing tools and applications used to collect security-related data (e.g, dispatch systems, incident management systems, case management systems)?

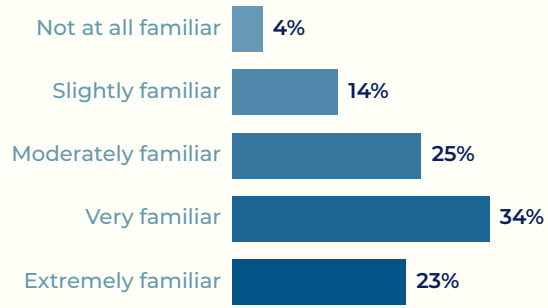


> **Without sufficient hands-on skills and confidence, security professionals are less likely to integrate analytics into day-to-day decision-making, regardless of their interest or access to tools.**

Familiarity with creating analytical graphs

Similarly, data presentation and ability to showcase collected and analyzed data is a significant step forward in a developed and optimized security metrics program. While 57% of respondents reported they are very familiar to extremely familiar with creating analytical graphs, 43% of security professionals reported they are not at all familiar to moderately familiar in this area.

How familiar are you with creating analytical graphs and reports to visualize security data (e.g., bar graphs, line graphs, pie charts, heat maps, scatter plots)?



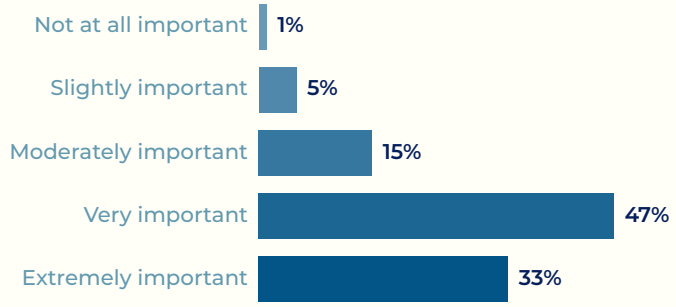
Within the Clark and Estes gap analysis framework, these patterns reflect a significant **knowledge gap**. Without sufficient hands-on skills and confidence, security professionals are less likely to integrate analytics into day-to-day decision-making, regardless of their interest or access to tools. For CSOs, this points to a specific development opportunity: targeted training in metrics selection, basic analysis techniques, and visualization practices that equip security teams to move beyond raw data and ad-hoc reports toward consistent, insight-driven management.

Motivation and perceived value:
Interest is not the problem

Importance of collecting and analyzing security data

Despite the knowledge and skills gaps described above, motivation to use data analytics appears relatively strong among physical security professionals. Most respondents rate the collection and analysis of security data as important or extremely important to their role, indicating broad recognition that analytics should be central to modern security management rather than a peripheral reporting task. This aligns with the rising emphasis on data-driven decision-making in adjacent domains such as IT, risk management, and operations, and suggests that many security practitioners want to move in the same direction.

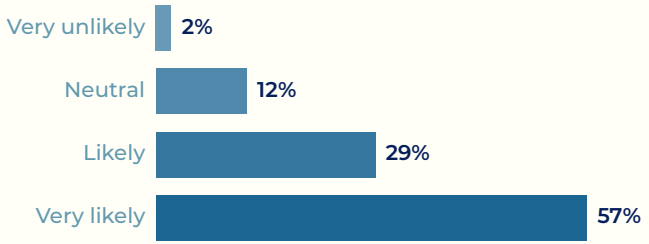
How important is collecting and analyzing security data to you in your role as a security professional?



Willingness to attend training programs

Interest in developing analytics capabilities is also evident in attitudes toward training. A large share of respondents (86%) indicate that they would attend a data analytics training program if their organization offered one, and many explicitly cite lack of knowledge or training as a key constraint. Within the Clark and Estes framework, this combination of high perceived importance and strong training interest suggests that the "M" in KMO (motivation) is relatively strong in many organizations.

If your organization offered a data analytics training program, would you attend?

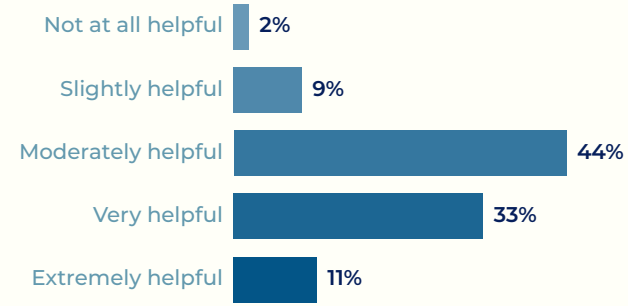


> **A large share of respondents (86%) indicate that they would attend a data analytics training program if their organization offered one.**

Perceived effectiveness of security programs

Perceptions of the usefulness of existing metrics programs, however, are more mixed. Among respondents whose organizations have a formal metrics program, some describe it as very or extremely helpful in informing risk mitigation and program improvements, while others view it as only slightly helpful or neutral. Where metrics are seen as loosely connected to real decisions, motivation can erode over time, as practitioners perceive analytics as a reporting obligation rather than a source of actionable insight.

How effective is your security metrics program in measuring and improving your security program?



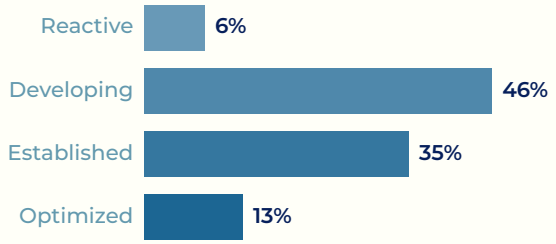
> **For CSOs, ensuring that metrics reviewed in dashboards and meetings are clearly linked to meaningful outcomes, such as incident reduction, response performance, and business continuity, is essential to sustain positive attitudes and engagement.**

Organizational factors:
Structure, leadership, and resources

Security metrics program maturity

Organizational conditions, leadership practices, structures, and resources play a decisive role in shaping analytics adoption and maturity. The survey indicates that a significant number of respondents work in organizations that either lack a formal security metrics program or are in the early stages of developing one. Even among organizations that do have a program, self-reported maturity levels frequently fall into “developing” rather than “established” or “optimized,” suggesting that systematic, recurring use of analytics to guide program decisions is still emerging rather than standard practice across the industry.

How would you describe the maturity of your organization's security metric program?



Reactive - Minimal use of data analytics; decisions are primarily based on intuition.

Developing - Metics are routinety collected and analyzed, with periodic reporting to

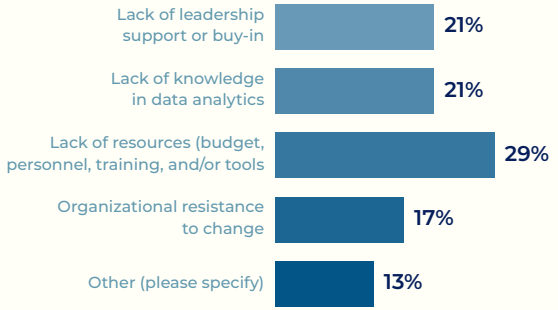
Established - Metrics are systematically collected, analyzed, and reported, with results actively used to guide program improvements

Optimized - Security metrics program is fully integrated, regularly updated, and drives continuous improvement across the organization

Barriers to implementing security metrics programs

When asked to identify the single most significant barrier to implementing or strengthening a security metrics program, respondents most often select options such as lack of leadership support or buy-in, lack of knowledge in data analytics, lack of resources (budget, personnel, training, tools), and organizational resistance to change. These responses highlight that many security teams are attempting to advance analytics in environments where strategic direction, staffing, and funding may not yet align with data-driven ambitions. From a Clark and Estes perspective, even highly motivated and knowledgeable practitioners will struggle to close performance gaps if organizational structures do not support the desired behaviors.

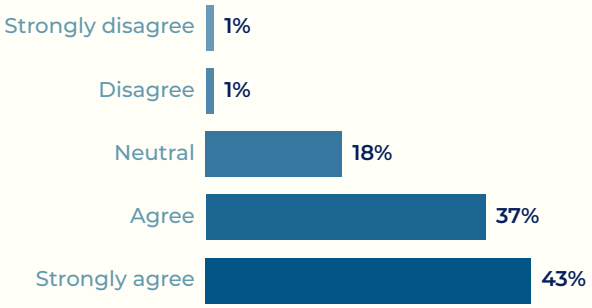
What do you consider the primary barrier to implementing a security metrics program in your organization?



CSO support

Leadership behaviors around metrics and reviews are particularly influential. In some organizations, respondents report that their CSO or head of security actively supports the use of data analytics, requires team members to incorporate analytics into their programs, and mandates recurring metrics review meetings at both the security-team and executive levels. These organizations are also more likely to describe their metrics programs as established or optimized and to report that metrics insights are very or extremely likely to inform risk mitigation decisions. In contrast, respondents who report infrequent or ad-hoc metrics reviews and limited executive-level engagement with security data, tend to describe lower program maturity and more pronounced barriers.

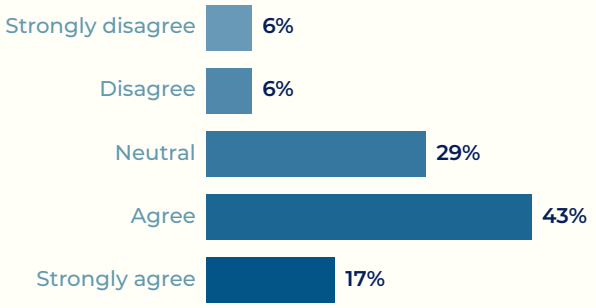
My CSO/Head of Security is supportive of utilizing data analytics in our security program.



Analytics and review requirements

Structural practices around what is measured and how data are managed further differentiate more mature programs from less mature ones. Organizations at higher maturity levels typically measure a broader set of domains, physical security performance, incidents and investigations, staffing and resource utilization, training and personnel performance, technology and system performance, threat management, and protective intelligence and are more likely to use dashboards and integrated platforms to visualize and centralize data.

My CSO/Head of Security requires each member of our security team to utilize data analytics in their respective security programs.



My CSO/Head of Security requires a recurring security metrics review meeting to review and discuss our program's security metrics.

For CSOs, these patterns suggest that organizational investment in formal metrics programs, recurring review cadences, and analytics infrastructure is a critical lever for advancing from isolated data points toward a coherent, enterprise-level view of risk and performance.

The KMO performance gap:
Why tools alone are not enough

Viewed through the Clark and Estes KMO lens, the findings suggest that physical security's analytics performance gap is driven less by a lack of data and more by misalignment across knowledge, motivation, and organizational conditions.

On the **knowledge** side, many practitioners have at least moderate conceptual familiarity with metrics and tools but lack confidence in their ability to perform analysis and translate findings into decisions, particularly in the areas of visualization and data storytelling.

On the **motivation** side, professionals across roles consistently rate data analytics as important to their work and express willingness to attend training, indicating that interest is not the primary bottleneck. Active choice, persistence, and effort are all decisive factors in forming the motivation required to master skills.

The most pronounced constraints fall under **organizational** factors: uneven presence and maturity of formal metrics programs, inconsistent leadership expectations, and barriers such as insufficient resources, limited buy-in, and resistance to change.

Three areas of focus

Moving from Gap to Mastery

What is security analytics maturity?

In this report, security analytics maturity refers to the extent to which a physical security program systematically collects, analyzes, and uses data and metrics to inform decisions about risk, operations, and strategy. It is not simply a measure of how many tools are deployed or how many dashboards exist, but of how consistently data is used to guide action and drive improvement across the program.

> **Mature programs go beyond describing what happened to diagnosing why it happened and, increasingly, to anticipating what is likely to happen next.**

At higher maturity levels, security analytics is characterized by standardized metrics across multiple domains, reliable data pipelines, regular review cadences at both operational and executive levels, and clear linkages between metrics and decisions. Mature programs go beyond describing what happened to diagnosing why it happened and, increasingly, to anticipating what is likely to happen next. They integrate physical security data into broader enterprise risk and business intelligence discussions, ensuring that security insights contribute directly to organizational resilience and performance.

A KMO-based Security Analytics Maturity Model (SAMM)

Building on the survey findings and the KMO framework, this research proposes a four-level Security Analytics Maturity Model tailored to physical security programs. Each level reflects characteristic patterns in knowledge, motivation, and organizational conditions, as well as the scope and impact of metrics use.

Most organizations in the study cluster in the Aspirational and Developing levels, with fewer reaching Proficient and only a small minority operating at an Optimized level where analytics consistently shapes strategic decisions. The model is designed not as a scorecard but as a roadmap to help CSOs understand where they are today and what it will take to move to the next level.

LEVEL 1

Aspirational

Analytics is informal and fragmented, driven by individual effort rather than a defined program. Metrics, if present, live in personal spreadsheets or ad-hoc reports, and regular reviews are rare. Familiarity with data, tools, and visualization is low, as is confidence in using analytics to improve programs. Leadership seldom requests data for decisions, and barriers such as limited knowledge, resources, or priority are common.

LEVEL 2

Developing

The organization sees the value of metrics and has begun a basic program, typically focused on incidents and a few operational indicators. Many practitioners are moderately familiar with analytics, but confidence and capability remain limited. Reviews occur quarterly or ad hoc, and executive discussions are often descriptive. Motivation and training interest are high, but organizational support is still developing.

LEVEL 3

Proficient

Metrics are systematically collected and used to improve performance across incidents, investigations, staffing, training, technology, and threat management. Many respondents are highly familiar with analytics, and core leaders are confident in their abilities. Regular reviews are standard, supported by dashboards or BI tools. Barriers shift toward scaling, integration, and change management rather than basic knowledge gaps.

LEVEL 4

Optimized

The metrics program is fully integrated and drives continuous improvement. Security analytics is embedded in enterprise risk and BI processes, with data reflected in executive dashboards. Skills, leadership commitment, and governance are aligned to strategic objectives. Barriers focus on advanced capabilities like predictive analytics, AI governance, data ethics, and automation rather than foundational adoption.

Security Analytics Maturity Model for Physical Security

This table summarizes a four-level Security Analytics Maturity Model that classifies programs based on their survey responses and KMO profile.

Level	Label	Core Description	Typical Survey Pattern (Examples)	KMO Profile Focus
1	Aspirational	Analytics activity is informal, fragmented, and largely driven by individuals rather than a defined program.	No or unclear metrics program; few or no defined security KPIs; low familiarity and confidence with analytics; rare or no metrics review meetings.	**Significant K and O gaps;** motivation often latent but under-leveraged.
2	Developing	Organization recognizes the value of metrics and has started a basic program, but practices are inconsistent and narrow.	Metrics program exists but rated "Developing"; focus mainly on incidents and a few operational metrics; quarterly or ad-hoc reviews; training interest high.	Motivation relatively strong; knowledge partial; **organizational supports emerging but fragile.**
3	Established	Metrics are systematically collected, analyzed, and used to guide program improvements across multiple domains.	Program rated "Established"; broad metric set (incidents, performance, staffing, training, technology, threat); monthly/ quarterly reviews; dashboards in use.	Solid knowledge base and motivation; **organizational structures largely in place, still maturing.**
4	Optimized (Insight Driven)	Analytics is integrated into strategy and enterprise risk; data continuously drives optimization and innovation.	Program rated "Optimized"; frequent internal and executive reviews; integrated dashboards and platforms; high familiarity, confidence, and perceived impact of metrics.	**High alignment across K, M, and O;** focus on advanced issues (predictive, AI, governance).

Roadmap for advancing security analytics maturity

To move from aspiration to sustained, insight-driven practice, CSOs must orchestrate parallel progress in all three KMO domains. The following recommendations provide a practical roadmap.

1 Strengthen knowledge: Build baseline analytics capability

- **Define the core analytics skill set.** Specify what every leader and practitioner should be able to do (interpret core metrics, read dashboards, ask analytical questions) and what advanced skills are required for analyst roles.
- **Offer targeted, practical training.** Focus on metric design, basic analysis, and visualization using existing tools rather than abstract statistics courses.
- **Leverage mentors and internal partners.** Use mentoring, "analytics office hours," or joint projects with data teams to help practitioners turn raw security data into meaningful insights.

2 Harness motivation: Make analytics meaningful and visible

- **Connect metrics to outcomes that matter.** Frame analytics around incident reduction, response performance, guard utilization, and executive visibility, not just "reporting requirements."
- **Position training as a career opportunity.** Emphasize that analytics skills increase influence and advancement, reinforcing professionals' willingness to invest effort.
- **Celebrate early wins.** Share examples where data changed a decision or improved performance to reinforce the perceived value of analytics.

3 Re-engineer organizational supports: Institutionalize metrics and reviews

- **Formalize a metrics program.** Create a charter that defines purpose, governance, core metrics, data sources, owners, and cadence.
- **Standardize review cycles.** Establish regular internal and executive metrics reviews with a consistent dashboard and documented action items.
- **Address structural barriers directly.** Respond to identified barriers with visible executive sponsorship, resourced training, and, where appropriate, additional headcount or tooling.

4 Expand measurement scope and integrate data

- **Broaden what you measure.** Include response performance, staffing and resource utilization, training effectiveness, technology and system performance, threat management, and protective intelligence.
- **Integrate key data sources.** Centralize incident, case, access control, and technology performance data in a unified reporting environment.
- **Standardize definitions and data quality.** Agree on common definitions and basic data quality checks so leaders can trust and consistently interpret metrics.

5 Align leadership behaviors with analytics ambitions

- **Model data-driven decisions.** Leaders should routinely ask for data, use dashboards in meetings, and expect major decisions to be supported by metrics and trends.
- **Set clear expectations for managers.** Require each program owner to maintain a focused metric set with targets and report on them at defined intervals.
- **Integrate analytics into enterprise risk.** Ensure physical security metrics appear alongside cyber, operational, and financial indicators in enterprise risk reporting.

6 Use KMO as an ongoing diagnostic tool

- **Reassess regularly.** Conduct periodic KMO-based assessments to identify where knowledge, motivation, or organizational supports are improving or lagging.
- **Tailor interventions.** Focus training where knowledge is weak, culture and governance where organizational barriers dominate, and incentives and communication where motivation is at risk.
- **Plan KMO interventions for new initiatives.** When introducing new technologies or platforms, deliberately plan how you will support K, M, and O so adoption is not left to chance.

Methodology

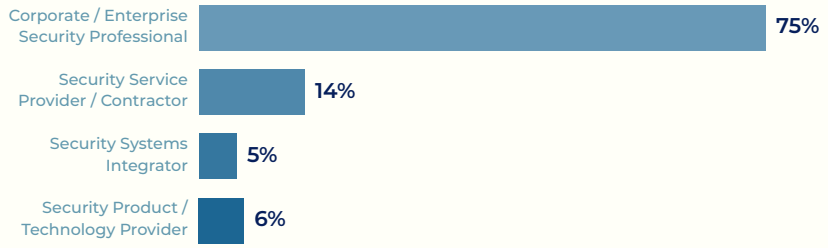
This report is based on a quantitative, cross-sectional survey of practicing physical security professionals. The study used a non-experimental, descriptive design to capture a snapshot of how security analytics is currently understood, implemented, and experienced across a range of organizations. The survey instrument was explicitly structured around the Clark and Estes gap analysis framework, with items designed to measure knowledge and skills, motivation and attitudes, and organizational conditions.

Respondents included corporate and enterprise security professionals, security service providers, system integrators, and security technology vendors. They represented a variety of roles, from security analysts and operators to managers, directors, deputy CSOs, and CSOs and came from organizations of different sizes, with many working in teams of 21 or more security professionals. The sample was global in scope, with participation from the United States and more than 35 other countries.

The instrument collected demographic and role information as well as detailed responses on familiarity with analytics concepts and tools, confidence and perceived ability, perceived importance of analytics, training interest, existence and maturity of metrics programs, barriers to implementation, review frequency, scope of measurement, and dashboard use. Most items used Likert-type scales, enabling the calculation of descriptive statistics that summarize the distribution of responses within each KMO domain. Data were cleaned and grouped by K, M, and O domains, and descriptive analyses were used to interpret patterns and inform the maturity model and recommendations.

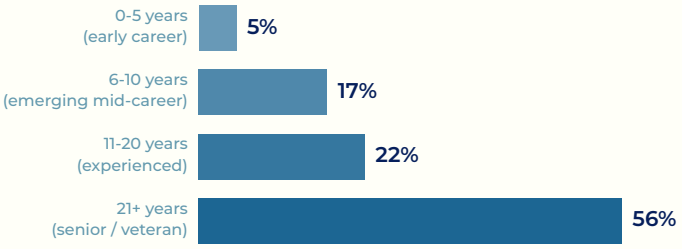
Survey participants' role in the security industry

Which of the following best describes your primary role in the security industry?



Survey participants' tenure as security professionals

How many years of experience do you have working as a security protessional?



Note: The survey participants reported having 11 or more years of experience (78%) in the security industry while 56% of respondents reported 21 or more years of experience, indicating participants who participated in this research had a vast knowledge of the security profession.

Caveats to the study

As with any survey-based research, there are important limitations to consider when interpreting these findings. Participation was voluntary, and while the sample includes a broad cross-section of physical security professionals, it is possible that those who chose to respond differ in meaningful ways from those who did not, for example, in their interest in analytics or their level of engagement with industry research. This introduces the possibility of non-response bias.

The accuracy of the results also depends on the representativeness of the sampling frame and the quality of contact information used to reach potential respondents. Because data were collected via an online survey, organizations or individuals with limited access to or comfort with digital platforms may be under-represented. In addition, all findings are based on self-reported perceptions and practices, which are subject to recall errors, interpretation differences, and social desirability biases.

Finally, the study's cross-sectional design provides a snapshot in time rather than a longitudinal view. While the proposed maturity model and KMO-based roadmap are grounded in current data and prior research, further work, particularly longitudinal and mixed-methods studies, will be needed to track how analytics maturity evolves over time and to establish stronger causal links between specific interventions and outcomes. Readers should therefore view the results as a robust starting point for action and dialogue, rather than as a definitive or exhaustive account of all organizations' experiences.

About the author

Dr. Farhad Tajali is a senior security leader and researcher specializing in the design and optimization of data-driven physical security programs. He has extensive experience leading enterprise security programs, including security systems, technology, and analytics functions, with a particular focus on leveraging metrics and maturity models to improve organizational performance and align physical security with enterprise risk and business objectives. He earned his Doctorate in Education (Organizational Change and Leadership) from the University of Southern California, and holds a bachelor's degree in Computer Information Systems from California State University, Northridge.

About Ontic

Ontic provides software that helps corporate and government security teams identify threats, assess risk, and respond faster to keep people and organizations safe. Its Connected Intelligence Platform unifies security operations and data into a centralized system of record, enabling organizations to conduct risk assessments, protect against workplace violence, and manage threats and incidents more efficiently. Fortune 500 companies and federal agencies rely on Ontic to support security programs such as executive protection, threat intelligence, and corporate investigations. Learn more at ontic.co or follow us on LinkedIn.

Ready to elevate your security metrics?

Turn insight into impact with proven frameworks and purpose-built technology. Visit securityframeworks.com to explore practical models for advancing your analytics maturity, and discover how Ontic helps security teams operationalize data at scale at ontic.co.

SECURITY FRAMEWORKS | ONTIC