Key Findings from

THE STATE OF SECURITY MANAGEMENT

A Baseline Phenomenological and Empirical Study

Funded by

ASIS FOUNDATION™

MODULE 9:

Harness the Power of Security Metrics

Metrics and advanced decision-making tools have many benefits in the practice of security management. They add value, however they must be properly planned, designed, and employed. Security executives who understand and make the best use of these tools will be the most successful trusted advisors within their organizations.

Three quotes eloquently summarize the role of metrics and decision-making tools in security management today:

"Security operations managers who demonstrate the ongoing worth of their pro-grams, through efficient operations, measurable benefits, and reliable services, will thrive." (McCrie, 2016)

"Introducing risk management into the field of security and assets protection also presents an opportunity to apply metrics." (Mahoney and Peterson, 2016)

"To manage today's risks and anticipate tomorrow's challenges, organizations need to harness the power of data and analytics…[to] create meaningful and actionable insights [to address enterprise-wide risks.]" (Aon, 2019)

The notion of metrics as an essential tool for influencing executive/organizational decisions was prominently featured in our survey results. Answers to the question asking "what changes do you see in the security management field?" included these:

- Changes toward artificial Intelligence and machine learning
- Growing interest in intelligence-led security programs
- Starting to see intelligence collection and analysis for security professionals
- Intelligence and technology now drive security delivery and innovation
- Technology advancement in terms of artificial intelligence (AI)
- More focus on intelligence models and tools for more proactive response to security threats

The survey also explored the current use of metrics, data collection, and technology tools such as AI in the security management function. Some relevant points:

- Almost half of respondents indicated they use security-specific, formal metrics and analysis tools. Only 44 percent use more generic organization-wide metrics.
- About 40 percent of respondents use security-specific international or national standards as a measurement tool, whereas 52 percent indicated they use more general standards such as the ISO 9000 series.
- When asked to what degree respondents use metrics or statistical analysis, 72 percent stated they use these tools to "a moderate degree" or "a great deal."
- The final question in this series asked about the use of advanced technologies such as to aid executive decision making or program management. Almost 11 percent of respondents use artificial intelligence, machine learning, or data analytics "a great deal," 21 percent to "a moderate degree," and 36 percent "somewhat."

In the future, advanced tools will also help cut through the fog of high-stress or crisis situations, such as by sorting, prioritizing, evaluating, and consolidating emergency calls and calls for ser-vice.

SECURITY THOUGHT LEADER PERSPECTIVE:

Time to Embrace AI

"Chief Security Officers must embrace artificial intelligence now and begin integrating it into the profession or face losing their relevance and [perhaps be-ing] replaced by AI.... Bringing AI into the team, training themselves to focus on doing what only humans can do, training AI properly and letting it loose to help secure people [and organizational assets] is imperative to the business."

-Justin Crysler
Graduate Student

ENCOURAGING METRICS AND AI AS SECURITY MANAGEMENT TOOLS

In 2014 the ASIS Foundation sponsored a research project to study security metrics. The introduction states, "Security metrics are vital, but in the field and in the literature one finds few tested metrics and little guidance on using metrics effectively" (Ohlhausen et al., 2014). The project resulted in the development of a Security Metrics Evaluation Tool, a library of metric descriptions, and guidance on putting metrics into practice. It also established a recommended protocol consisting of technical, operational, and strategic criteria for security metrics.

Further advice was provided in 2016 to assist in developing a security metrics program geared toward larger enterprises. In an article titled "Some unconventional security metrics," Roger Johnston, PhD, CPP, articulated some important attributes of any good security metric. The important things should get measured, not just the things that are easy to measure. Quality must be emphasized over quantity. Recognize that compliance and security are not the same thing.

Process improvement is another valuable benefit of a metrics program (Taylor, 2013):

> *Measuring the value of programs which are designed to prevent events form occurring has been a difficult challenge for security professionals. A well-defined security metrics program allows security professionals to examine specific processes and*

components of their program and identify weaknesses, performance trends, and [potential] process improvements.

Security metrics are becoming more and more of a necessity, and advanced technology to support security risk management and security program decision making will become increasingly the norm.

The ninth in a series of nine modules, this paper explores the findings of an ASIS Foundation study conducted by Kevin E. Peterson, CPP, CIPM II and Joe Roberts, Ph.D. in 2020 and 2021. To download the full ***State of Security Management*** report, visit *asisfoundation.org*.

The ASIS Foundation, an affiliate of ASIS International, helps security professionals achieve their career goals with certification scholarships, practical research, member hardship grants, and more. The Foundation is supported by generous donations from ASIS members, chapters, and organizations. Online at *www.asisfoundation.org*.