Key Findings from

THE STATE OF SECURITY MANAGEMENT

A Baseline Phenomenological and Empirical Study

Funded by

ASIS FOUNDATION™

MODULE 3:

Embrace Change

Leaders must be prepared to deal with changes—sometimes radical, always dynamic—in the risk environment. Executives face changes in management principles, practices, and tools as well as social factors in organizational, national, and global governance.

The years 2019 and 2020 represented a sea change in security management, and the changes are still developing. For the past several years, change has been a popular theme in security professional development courses, books, papers, and articles. In addition, the CSO Standard lists "change agent" as a required skill for a senior security executive. The next sections examine a few categories of change.

COVID-19

The COVID-19 pandemic, and its associated uncertainty, changed in the global risk environment. As a result, corporate security chiefs and cybersecurity leaders are gaining prominence in many corporate settings. Torsten Wolf, Director of Forensics at Control Risks-Germany, notes that the pandemic, "in combination with the pressure of an economic downturn, lasting uncertainty, and, in many cases, a fight for daily survival, … may prove to be a perfect storm" for fraud and other risks. A report by the Association of Certified Fraud Examiners notes:

- Businesses continue to grapple with the economic fluctuations, supply chain disruptions, remote operations, and the toll this year has taken on the health, safety, and well-being of the workforce.

- Organizations are much affected by cyber-fraud (including hacking, ransomware, and malware), payment fraud, identity theft, and unemployment fraud.

- It has become more difficult to prevent, detect, and investigate fraud, in part because of travel restrictions, the need to conduct interviews remotely, and lack of access to evidence.

- Many businesses are investing in anti-fraud technology, consultants, and training.

In addition, the pandemic has eroded trust in companies and institutions, potentially increasing security risks.

CIVIL UNREST

In the United States, in spring 2021, several incidents seen as racially motivated police brutality sparked a rampage of vandalism, arson, looting, and killing in major cities across the United States. The destruction

will result in at least $1 billion to $2 billion of paid insurance claims, costing the insurance industry more than any other violent demonstrations in recent history. As reported in *Security Infowatch,* the violence "left a devastating trail of damage amongst businesses of all sizes in the communities where they occurred and have led many organizations to rethink risk mitigation strategies in confronting these types of events. Historically, incidents of civil unrest were isolated to individual cities and were infrequent occurrences, but the proliferation of social media and the speed with which information flows today has resulted in a paradigm shift in how these types of events unfold."

Civil unrest has been expanding globally in recent years. According to *Political Risk Outlook 2020,* the number of countries rated extreme risk in its Civil Unrest Index has...jumped by 66.7 percent.

Today's challenges include the movement to defund the police and efforts to reduce security personnel's authority and increase their liability. Such changes may affect security service providers' structure, strategies, and tactics. This, in turn, will affect corporate security professionals' risk management strategies and internal and external relationships. These changes may also affect the skills and competencies important for security officers and managers.

CYBER RISKS

Ransomware attacks on businesses, municipalities, law enforcement agencies, and critical energy infrastructure affect many geographic areas, industry sectors, and millions of people. In a 2020 cyberattack, malicious code was planted surreptitiously in software used by U.S. government agencies, major corporations, universities, and hospitals. Such incidents create widespread cyber-uncertainty—another aspect of the developing changes in security management priorities, thinking, and practices.

SECURITY THOUGHT LEADER PERSPECTIVE:

Reacting to Change

"Disruption is the rule, not the exception. The global landscape is rapidly changing, and this demands business acuity, technical know-how, and a curious mindset from senior security executives and risk analysts."

–Michael Padilla-Pagan Payano
CEO and Chairman
Al Thuraya Holdings, Nicosia, Cyprus

MORE ON CHANGE

Security executives are increasingly likely to face multiple, stacked risk events, straining resources, diffusing strategic focus, and confounding traditional risk mitigation strategies. This has tremendous implications for the security management profession.

The third 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*.