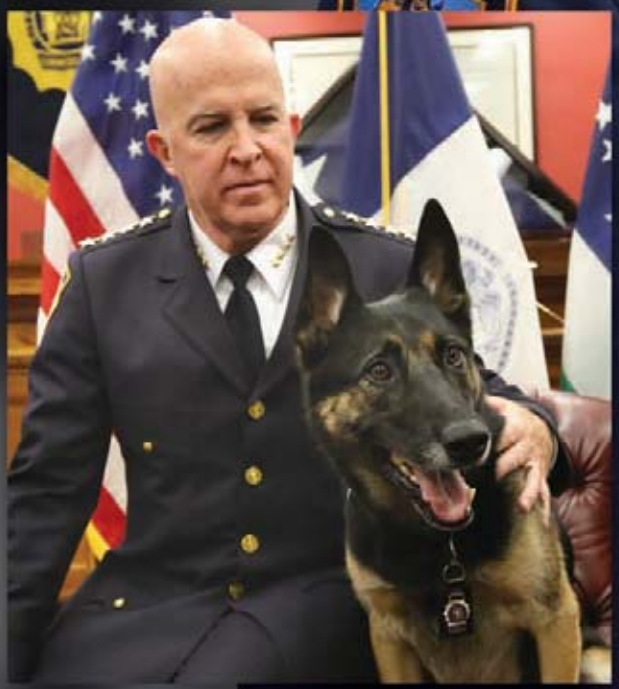
Spring 2017

# SECURITY DIRECTOR

ASIS International/New York City Chapter



## PERSON OF THE YEAR

JAMES P. O'NEILL

POLICE COMMISSIONER

CITY OF NEW YORK

The ASIS NYC Chapter thanks the following companies, organizations and institutions for their support to the chapter through advertising in this issue of *Security Director*.



SECURITY DIRECTOR

ASIS International/New York City Chapter

# CONTENTS



**Contributors:**

mitigations, the RNA can provide a snapshot of where potential peril currently resides.

An RNA establishes the requisite level of information, allows the organization to maximize limited resources and provides a foundation to build, restructure or update security and risk management capabilities. It informs all levels of management of the relative risk environment by focusing on the degrees of impact, the disruptive scenarios posing risk and the overall effectiveness of risk-related programs.

**The effectiveness of mitigation and controls can change rapidly due to operational circumstances and organizational priorities that are altered by new methods and technologies.**

The RNA provides a timelier and less resource intensive option to identify the risk profile and select preplanned mitigation when compared to the time and materials required for organization-wide risk assessments. These risk management competencies are further refined by focusing on feedback loops to identify internal best practices, overcome lessons learned and reinforce the trust and confidence of stakeholders.

**Conclusion**

Maintaining organized situational awareness provides the operational agility necessary to pursue opportunities based on stakeholder demands and the evolutionary pace of the industry. However, attempting to maintain an unvalidated risk profile taken from others is certain to bring unwelcome surprise. Using a medical analogy, in spurious risk management, a medical practice treats patients based on similar treatments at other facilities. Assuming their patients require similar treatment, and since no one has suffered adverse effects (yet), the practice deems their strategy acceptable. Conversely, in performing an RNA, a practice analyzes the representative data specific to patient needs, discerns the risk between ailments that are chronic versus acute, implements a treatment and then evaluates the strategy for effectiveness.

Risk is a continuum with trade-offs in all decision-making. Given the escalating pace and shrinking resources available on today's front lines, the RNA provides the agility needed for this paradigm as threats continue to morph and evolve. The effectiveness of mitigation and controls can change rapidly due to operational circumstances and organizational priorities that are altered by new methods and technologies. The means to assess risk must be adaptable to strategic design. Otherwise, the organization will assume its place in the growing modern antiquity.

**Michael Payne, CPP, Senior Advisor, Organizational Resilience, iJET International**

# HOMELAND SECURITY CELLPHONE SEARCHES: EFFECTIVE INVESTIGATIVE TOOL OR EXTREME INVASION OF PRIVACY?

**By Chelsea Binns, Ph.D., CFE**

The Department of Homeland Security (DHS) Customs and Border Protection (CPB) has conducted cellphone investigations at the United States border since 2009. According to recent reports, this controversial practice is happening more frequently. Opinions are divided as to the utility of these searches. Proponents find these investigations effective. Cellphone investigations have uncovered drug smuggling, child pornography and terrorism. However, critics say such searches invade citizens' privacy and "subvert American's constitutional protections against unreasonable search and seizure." This article will examine the use of this divisive investigative tool.

Electronic devices searches are legal. DHS has the legal authority to investigate electronic devices, which may include a complete forensic examination of cellphone contents. CBP directive No. 3340-049 outlines the legal authority of CPB to search electronic devices at the border. Applicable statutes include 8 U.S.C. 1225 and 19 U.S.C. 482.

The average investigation is minimal. What does an average

Continued on page 66

electronic device search entail? According to CPB, "browsing through a smartphone's photos or looking through a laptop's contents."

They are not conducted very often. According to CPB, electronic device searches affect "less than one hundredth of one percent of all travelers." In fiscal year 2016,

DHS conducted 23,877 electronic device searches. This sounds like a big number; however, it is only about 2% of cases. Over 1 million people enter the U.S. daily. Today, CPB is searching about 65 devices per day. Devices seizures are even more rare, done in a "very small number of cases."

The number of electronic device searches are increasing. In 2015, DHS Customs and Border Patrol (CPB) conducted 4,764 electronic device searches. 2016's figure, 23,877, represents a 401% increase. In contrast, between October 2008 and June 2010, 6,600 people were subject to electronic searches by the CPB. Overall, CPB went from searching about 13 per day in 2015 to 65 per day in 2016. According to CPB, "the increase is driven by our mission to protect the American people and enforce the nation's laws in this digital age."

The searches have uncovered evidence of crime. DHS has detected crimes via cellphone examinations. DHS has reported finding evidence of terrorism and child pornography, during such investigations.

The number of "successful" investigations is unknown. DHS reports the increase in cellphone examinations mirrors the growing volume of terroristic threats and "shifting world conditions." However, senior officials do not provide specifics regarding the number of searches which yielded actionable information.

Cases have raised serious privacy dilemmas. The media have reported numerous anecdotes of law-abiding travelers who have been unfortunate subjects of DHS cell phone searches. However, one recent case demonstrates the type of ethical challenge that may arise in the course of these investigations. In February 2017, DHS asked a NASA employee for his passcode and PIN, to examine his phone. He complied with their request. While legal, DHS's examination of the owner's phone, a work device, raised issues of privacy with respect to his NASA emails. This is a valid concern for many smartphone users, who often use a single device for both personal and business communications.

Courts tend to side with the government. In cases challenging device searches, the courts have largely supported the government. In a 2013 case, the courts found the 4th Amendment didn't protect electronic devices at an international border. There, the traveler was a 28-year-old doctoral student at McGill University in Montreal. His computer contained material related to his doctoral research in Islamic studies. Upon review, this material was deemed suspicious by investigators. They seized his laptop to conduct a forensic search, which the student believed to be unconstitutional. Ultimately, the court asserted the right of the government to search a traveler's electronic devices at the border, without cause.

Cellphones can be seized from travelers to conduct advanced investigations. In rare cases, a cellphone can be seized by CPB for further examination. CPB provides a document to travelers whose device is being confiscated. This document titled "Inspection of Electronic Devices" explains the process. Travelers are advised that their device will be "detained for further examination, which may include copying." Written receipts are provided to travelers with a point of contact at CPB. Following their inspection, CPB notifies the owner in order to make pickup arrangements. If pickup is not practical, CPB offers to mail the device at their expense. However, if evidence of a crime is uncovered on the device, CPB asserts their legal right to seize the device. In that case, the owner is notified and has an opportunity to contest the seizure through CPB.

As discussed, cellphone searches are an investigative tool used by DHS to protect national security. Privacy advocates lament DHS's legally supported cellphone searches as an infringement of privacy rights. DHS reports the increased searches are relatively small and mirror the growing volume of terroristic threats. DHS has the legal authority to conduct these searches, in the interest of border security. Yet privacy rights advocates argue that these searches violate 4th Amendment rights, and warrants should be required. Regardless of one's personal belief,

these searches have been deemed legal by the courts and have been used with positive results as an investigative tool in the fight against terror.

**Chelsea Binns, Ph.D., CFE,**
**Assistant Professor, Dept. of Criminal Justice, Legal Studies & Homeland Security,**
**St. John's University**

# THE EVOLVING ROLE OF THE CHIEF SECURITY OFFICER: RETHINKING EFFECTIVE RISK MANAGEMENT FOR 2017

**Jonathan Wackrow**

It wasn't so long ago that a Chief Security Officer's (CSO) job was relatively straightforward: secure the premises by focusing on facility access, guard services and camera surveillance. Today, CSOs are charged with mitigating an array of interdisciplinary and intersecting risks across the enterprise.

Remote access to buildings, interconnected air-handling units and remotely monitored vending machines all provide potential new entry points for threat actors. Emerging regulations, such as SEC rules that affect business continuity and transition plans, also compound the pressure on CSOs to address the complexity of this risk landscape and integrate new mitigation strategies and tactics into traditional physical security processes.

Consequently, the CSO's role is evolving into a mission-critical service that spans risk areas ranging from data protection and vendor due diligence to regulatory requirements for business continuity and compliance management.

**Addressing the Changing Threat Landscape**

Today's CSOs must manage risks spanning five multidisciplinary areas that have not traditionally intersected with the narrow scope of safety and security, covering policy development, resource procurement and execution to mitigate threats, vulnerabilities and risks in the following spheres:

**1. Cyber and Information:**
Data protection, intrusion testing, data breach and recovery, economic espionage, and internal threat assessment and privacy.

**2. Legal and Regulatory:**
Litigation support, regulatory liaison and investigation, and remediation efforts related to financial crimes, fraud and corruption, and whistleblower litigation.

**3. Diligence, Business and Geopolitical Intel:** Transactional diligence, commercial diligence and intelligence, employment screening, internal investigations, and geopolitical risk assessment.

**4. Governance, Risk and Compliance**: Audit expertise, risk, insurance, and reputation management

**5. Medical and Psychological:**
Employee counseling, crisis intervention, employee productivity, and workplace violence.

**Three Pillars of Protection**

In order to manage the responsibilities associated with these risks, CSOs can prioritize their strategic objectives and tactical actions using the following framework:

**1. People**:
Identify and acquire key personnel to support development and growth of the organization's corporate security department. All relevant employees must be trained in security and safety initiatives and be able to implement communications plans. Further, all employees must be trained and encouraged to identify safety and security concerns and provide feedback. CSOs must also identify preferred vendors and partners to support in-house efforts to respond to changing risk environments.

**2. Process:**
Prioritize utilization of vulnerability assessments to ascertain potential impact threats have on the organization. This, combined with benchmarking levels of security awareness, emergency preparedness and compliance with established policies and procedures, will inform specific initiatives for holistically understanding the entity's security ecosystem.

**At the organization level, companies should empower CSOs to play a more strategic part in overall enterprise risk management plans.**

**3. Technology:** Employ technology solutions and security systems to assist decision-makers in better utilizing the critical information and resources at their disposal. /

**Three Steps for Better Leveraging the CSO**

At the organizational level, the CSO is an integral stakeholder. Too often, however, the CSO is overlooked, under-resourced, and underutilized. Below are three steps that companies can take to

Continued on page 68