COSMOS
Navigate the Compliance Universe

Report on Supply Chain Compliance Volume 2, Number 18. September 26, 2019
Supply chain compliance at SCCE's 2019 Compliance and Ethics Institute: Your key takeaways

By Sascha Matuszak

SCCE's 2019 Compliance and Ethics Institute took place in National Harbor, Maryland, bringing together more than 1,400 compliance and ethics professionals for five days of informative sessions, networking and exhibits. The sessions covered a variety of important topics, including third-party due diligence, trade compliance, automation and risk assessment, the ins and outs of government contracting, establishing ethical compliance programs, and data privacy and cybersecurity.

Dr. Kurt Michels, chief compliance officer at Volkswagen Group, spoke on the cultural transformation underway at Volkswagen, following years of litigation and recrimination over the emissions scandal. Michael Horowitz, Inspector General at the U.S. Department of Justice, spoke about maintaining independence and integrity while investigating both high- and low-profile cases. Gerry Zack, CEO of SCCE, interviewed Olga Pontes, chief compliance officer at Odebrecht S.A. on the company's recovery from scandal.

Based upon the many conversations that took place, we gathered some of the most important takeaways for our readers.

Data management will become everyone's responsibility

The global push to revamp how technology companies collect, process and store personal data has compliance officers across sectors seeking tools and guidance for how to protect their companies' data and comply with the ever-growing list of regulations, and attendance at the data privacy-focused sessions seemed to reflect this.

Charles Shugg, partner and chief operating officer at Sylint Group, Inc., stated that C-suite level employees will be held accountable "in ways not seen before" (quoted from U.S. Senator Elizabeth Warren) for massive data breaches. Shugg pointed to the Data Breach Prevention and Compensation Act of 2019 (S. 1336, 116th Congress) as proof. The law would impose jail time on executives of large companies that "negligently permit or fail to prevent" a "violation of the law" that "affects the health, safety, finances, or personal data" of 1% of the population of any state. Legislation introduced by U.S. Senator Ron Wyden would go much further.

Over the next few days, speakers discussed government cybersecurity standards and regulations, the concept and implementation of "reasonable" cybersecurity due diligence, and the complex web of international data privacy laws that companies must understand and comply with.

David Kessler, public sector counsel for Verizon, provided a helpful list of some of the cybersecurity standards and regulations that government contractors must be aware of:

- ISO 27001, 27017, & 27018; Information Security Management : Information security for cloud computing, and controls applicable to personally identifiable information (PII).
- The Payment Card Industry Data Security Standard : Applies to payment card processors and the storage,

processing or transmittal of cardholder or sensitive authentication data.

- Federal Acquisition Regulation (FAR) 52.204-21 : Basic 15 controls that apply to the first layer of government cybersecurity.
- NIST SP 800-171 & SP800-53

  Federal Information Security Management Act of 2014 (44 U.S.C. § 3551) : National Institute of Standards and Technology controls for information security, which contains 110 controls on the low end and up to 385 controls on the high end.
- CNSSI 1253/NSS : Committee on National Security Systems Instructions for Information Security, a top level security framework for computing and IT, including up to 862 separate controls.

Speakers also discussed responses to data subject requests, software compliance and security, and the interplay between GDPR, U.S. federal regulations and the many data privacy regulations popping up in Brazil, India, China and across the U.S. (e.g., California, New York and Nevada).

RSCC will cover these topics over the next few weeks and months, including exclusive interviews with experts and speakers from this year's Institute.