CEP Magazine - July 2019

# Great expectations: The shifting cyber-regulatory landscape

By Gopal K. Padinjaruveetil, CISA, CISM, CGEIT, CRISC, TOGAF 9, and Cris Mattoon, JD, CCEP, CAMS, MCM

**Gopal K. Padinjaruveetil** (gpadinjaruveetil@aaamichigan.com) is Vice President, Chief Information Security Officer, and **Cris Mattoon** (cqmattoon@aaamichigan.com) is Assistant Vice President, Compliance & Ethics, at The Auto Club Group in Dearborn, Michigan, USA.

***This is the first of a two-part series dealing with cybersecurity risk management, regulations, and solutions.***

Chief information security officers (CISO) and chief compliance officers (CCO) are facing mounting questions from boards of directors, CEOs, shareholders, customers, and the media, seeking reassurance that their organizations' digital infrastructure and data remain secure against tomorrow's threats, some not yet even imagined. The continual onslaught of high-profile cybersecurity incidents wrought upon corporations and government agencies by illicit state actors and organized crime syndicates has culminated in a burgeoning cacophony of multijurisdictional cyber-regulation. International, federal, state, and model laws have begun to converge with increasing frequency and intensity to assign explicit accountabilities to organizations and executives with the objective of protecting sensitive regulated consumer and employee data.

In the first part of this two-part series, we address the heightened risk management expectations that regulatory agencies have expressed for the entities that they supervise. The second part of the series will address the evolution of cybersecurity risk management and the increasing convergence between private sector solutions and regulatory expectations.

## Heightened regulatory expectations

Spurred largely by well-intentioned legislators and regulators responding to a complex criminal trend that has attracted continual media attention, the alphabet soup of EU GDPR, NYS DFS, NAIC, etc. continues to be served up piping hot until all cups runneth over. Despite the increasing burden of laws, regulations, and industry standards, cyberstaff and software solutions are finite resources that must be efficiently deployed to detect and mitigate foreseeable risks. CISOs are increasingly partnering with second-line-of-defense compliance counterparts to develop enterprise-wide cybercompliance risk assessments (CRA) to target key regulatory requirements.

In addition to providing your cybercompliance team with a blueprint for monitoring and testing higher-risk digital distribution channels, information systems, and data management processes within your organization, a CRA demonstrates to auditors and regulators that your cyber-risk management program is objective, documented, and repeatable. Having a well-defined plan supported by a comprehensive CRA can go a long way toward demonstrating appropriate due diligence, even when an organization experiences the inevitable, reportable cybersecurity incident.