COSMOS
Navigate the Compliance Universe

CEP Magazine - August 2019
Stronger bonds: The evolution of the CISO-CCO regulatory partnership

By Gopal 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 second of a two-part series dealing with cybersecurity risk management, regulations, and solutions.

In the first part of this two-part series, "Great expectations: The shifting cyber-regulatory landscape," we addressed the heightened risk management expectations that regulatory agencies have expressed for the entities that they supervise.[1] This part will address the evolution of cybersecurity risk management and the increasing convergence between private sector solutions and regulatory expectations.

Chief information security officers (CISO) and chief compliance officers (CCO) are facing mounting questions from boards of directors, CEOs, shareholders, customers, and the media, who are seeking reassurance that their organizations' digital infrastructure and data remain secure against tomorrow's threats not yet even imagined. Leveraging cyber compliance risk assessments (CRAs) and other predictive tools and resources, CISOs and CCOs have also sought to integrate their efforts with the strategic objectives of the business lines while addressing regulatory agency efforts to supervise risk management effectiveness. Partnerships with governmental agencies that invite and reward innovation enhance trust and foster more effective risk management and strategic outcomes.

Evolution of cybersecurity and compliance

At the dawn of the computer age, the era of mainframe computing necessitated an information security approach that employed physical security measures focused on protecting access to hardware and printed output. As knowledge of computing increased, access to terminals began to be subject to passwords, and mainframes and printers were secured behind locked doors and required entrants to sign in on paper logs.

Even before the public internet came into existence, sensitive information was being transmitted by governments and large corporations across telephone lines. When the World Wide Web invited the public to access the internet in the later 1980s and early 1990s, an immature comprehension of the inherent risks of sharing personal details allowed criminals widespread access to lucrative data. Law enforcement agencies became involved as government and financial institution systems were subjected to thefts of data. Information technology leaders sought to harden infrastructure.

Even as the infrastructure was being strengthened to prevent external attacks and thefts of sensitive data, the accounting scandals of the late 1990s and early 2000s—most notably Enron and MCI—revealed the risks associated with financial data manipulation. Perpetrated from within these corporations by seasoned professionals, these scandals revealed the lengths to which greed could drive individuals to misuse information systems. Government regulation sought to increase transparency to mitigate the risk of future financial crimes and corruption, resulting in greater focus upon internal audit and compliance controls. With the passage of the

Sarbanes-Oxley Act of 2002 (SOX), the marriage between information technology, financial accounting, and regulatory compliance had been truly cemented.

The transition from the regulatory compliance cost center enshrined by federal regulation since the early 2000s to the strategic partner of the future is in its infancy. In McGraw, Migues, and Chess's well-known description of the four tribes of CISOs (i.e., Enabler, Technology, Compliance, and Cost Center), firms in the Enabler tribe "have long since evolved the security mission from compliance to commitment [where e]ven the Board of Directors has moved past compliance and uses a risk management approach to provide oversight. What regulators truly appreciate about this post-2008 financial crisis approach to risk management is that CISOs in this tribe proactively get in front of the problem both internally and externally by intentionally influencing the standards by which they will be judged."[2]