COSMOS
Navigate the Compliance Universe

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.

Cybercompliance risk assessment

There is no one-size-fits-all CRA that will address the needs of every organization. Conducting a comprehensive CRA is the catalyst for developing a risk-based plan to address the requirements of new or amended laws and

regulations. Building the risk assessment begins by identifying a universe of applicable cybercompliance risks that pertain to your industry within your regulatory environment. Some legal and regulatory requirements pertain to most organizations (e.g., GDPR[1], GLBA[2]), while many other requirements will be distinctly tied to your industry (i.e., NAIC Insurance Data Security Model Law[3]) and geography (i.e., California Consumer Privacy Act of 2018[4]).

The objective to populating the cyber-risk universe is to be as inclusive as feasible, versus eliminating risks deemed to be remote. Once the inherent risk universe has been identified, it's time to apply quantitative and qualitative analysis. The quality of risk management measures the effect that the implemented mitigating factors have to reduce cybercompliance risk exposure for the organization. These might include board and senior management oversight; policies, procedures, and limits; risk monitoring and management information system (MIS) reporting; and internal controls and training. The resulting residual cyber-risk is the exposure that remains once the quality of risk management has been applied to the quantity of risk inherently present for each risk factor.

Although variances might exist, the objective of this analysis is to identify any gaps that may exist between the minimum requirements of the law or regulation and the current state of cybersecurity preparedness. Together, the CISO and CCO will develop plans to close the gaps in a manner that both safeguards consumer and company data, as well as satisfies regulators.

Predictive tools and regulatory resources

Reducing uncertainty in the regulatory process is a key step to improving regulated entities' compliance with laws and regulations. There has long been a widely held perception that regulatory agencies' approach to supervision lags the private sector in cybersecurity maturity. But in the past few years, this perception has been shattered as federal and international legislators and regulators have sought to stem the onslaught of cybercrime and cyberespionage perpetrated globally by organized crime, rogue states, and stateless actors.

Standardized frameworks, such as the National Institute of Standards and Technology (NIST) *Cybersecurity Framework*,[5] as well as predictive tools and regulatory resources, including the Federal Financial Institutions Examination Council *Cybersecurity Assessment Tool*,[6] can decrease examiner subjectivity and misalignment between the private sector cyber-risk assessment and regulatory expectations.

Incorporating an accurate interpretation of regulatory expectations to evidence satisfactory cyber-risk management is critical. Ranking residual cyber-risks according to the highest severity will then allow the CCO to identify the improvement opportunities that may necessitate the CISO's attention to demonstrate satisfactory compliance with the legal and regulatory requirements. Assigning skilled resources to monitor, examine, and test higher risks will ensure that the cybercompliance function has the most impact possible to reduce regulatory risk to the organization.

Meeting regulatory expectations

Good enough may be good enough in some instances. Although it is important to meet minimum regulatory expectations by stipulated due dates for filings and certifications, an organization is cautioned against trying to achieve best-in-class compliance. The laws and regulations that have been enacted generally reflect an approach to cybersecurity that seeks to balance the interests of consumer protection, prudent business practices, financial constraints, and regulatory agency oversight capacity. Therefore, your organization isn't going to earn "extra credit" from the regulator by investing disproportionately oversized resources to achieve comparatively incremental improvements beyond the required standards.

Fulfilling the ethical intent of the regulations to safeguard critical infrastructure and consumer data must take precedence over a static, check-the-box approach. Regulators should strive to draft regulations and engage in supervision that provides transparency and predictability to CISOs and CCOs. Heightened trust between the regulators and regulated entities will drive meaningful investments in flexible, tailored solutions that truly mitigate risk.

Regardless of what investment choices your leadership team makes to develop the organization's cybersecurity compliance framework, the outcomes of the activities should clearly demonstrate to the regulator that appropriate controls are in place (or require remediation). Regulators will seek documentation of good governance and transparent MIS reporting.

Toward that end, the CISO will be able to report periodic results of plan activities to senior management and the board to provide further assurance that cybercompliance risk is being managed within the approved risk appetite. Regulators will often review reports made to boards of directors and the associated meeting minutes to validate that the cybersecurity compliance framework has been reviewed and approved by the board.

Conclusion

Across the globe, multijurisdictional cyber-regulation has been imposed upon organizations in a well-intentioned attempt by governments to protect sensitive regulated consumer and employee data. Accurately identifying, quantifying, and ranking the cybercompliance risks applicable to an organization can validate compliance with these new regulatory requirements, while identifying shortcomings that deserve prompt attention to achieve full compliance. In the second part of this series, we will explore the evolutionary relationship between cybersecurity and compliance and how that promises greater risk management and innovation in the years ahead.

Takeaways

- Cyber-regulatory risk management is a multijurisdictional alphabet soup.
- Deploying predictive and adaptive solutions, while reducing active defense resource allocation, better positions regulated entities to detect and deflect global cyberthreats.
- Heightened trust between the regulators and regulated entities will drive meaningful investments in flexible, tailored solutions that truly mitigate risk.
- Reducing residual cyber-regulatory compliance risk can reduce your organization's exposure to significant financial penalties and reputational damage.
- The role of a modern chief information security officer is changing, and they should be seen as enablers in a world that is becoming exponentially powered by digital and digital technologies.

1 Directive 95/46/EC (General Data Protection Regulation), Regulation (EU) 2016/679 of the European Parliament and of the Council, enacted April 27, 2016.
2 Gramm-Leach-Bliley Act, Public Law 106–102, United States Congress, enacted November 12, 1999.
3 Insurance Data Security Model Law, National Association of Insurance Commissioners (NAIC), passed October 24, 2017.
4 California Consumer Privacy Act of 2018, Assembly Bill No. 375, State of California, enacted June 28, 2018.
5 Cybersecurity Framework Version 1.1, National Institute of Standards and Technology, April 2018.
6 Cybersecurity Assessment Tool, Federal Financial Institutions Examination Council, May 2017.