Ethikos Volume 38, Number 1. January 01, 2024
Cultivating cybersecurity culture: Ethics, compliance, and the SEC's new disclosure rule

by Emily Miner

Emily Miner (emily.miner@lrn.com) is Vice President, Advisory Services for LRN in Jacksonville, Florida, USA.

No organization today can afford to underestimate the threat posed by cybersecurity attacks. Recognizing the potential impact of such risks on investor decision-making, in July the U.S. Security and Exchanges Commission (SEC) ramped up its regulatory approach. Its new rules require public companies to report material cybersecurity incidents fast (within four days) and disclose their risk management processes every year in a standardized form.

Yet, it's not enough for companies simply to meet the letter of these rules. If their cybersecurity compliance programs are to be truly robust, organizations must have a strong ethical culture that pervades all levels. Having the right ethos, values, and environment—as well as appropriate policies, procedures, and controls—ensures that employees not only know what the rules are but, crucially, that they also understand the underlying reasons behind compliance requirements.[1] It may sound obvious, but it's often overlooked: an ethical culture helps people make appropriate decisions and take effective actions, making it a cornerstone of data security resilience in today's challenging climate.

The integration of cybersecurity rules and organizational culture

The SEC's disclosure rules impose an incredibly important obligation on public companies; however, this obligation goes far deeper than merely what they are required to report in the aftermath of an incident. Leaders must renew their focus on prevention and risk management processes for cybersecurity and data privacy with vigor.

Since this regulatory framework is relatively new, it's impractical to have a playbook in place for every possible situation companies may face. What organizations can do, however, is develop guidelines based on value-driven principles, which can be adapted as necessary and honed over time as policies and standards evolve in response to the dynamic cybersecurity landscape.

But what is equally crucial is communicating the "why" behind these measures to embed these guardrails and processes into an organization's very fabric. This approach ensures that employees not only follow cybersecurity rules but see the need for them. When cybersecurity becomes ingrained, it becomes more than compliance—it becomes a shared commitment to safeguarding the organization's data, reputation, and, by extension, its future.