Bloomberg Law

bloombergbna.com

Data Security

INSIGHT: Boundaries Between IT and Security Functions – and How IG Teams Can Work with Each

BY DEANA UHL, FTI TECHNOLOGY

One of the most difficult challenges in any business setting is managing change and its effects on corporate culture and the boundaries of various roles and responsibilities. Many people are inherently resistant to or fearful of change and prefer to retain as much control as possible over shifting policies. In information governance (IG), one area where this challenge often arises is in the blurring of lines between the functions of the CIO/IT department, the CISO/information security team, and the in-house legal team.

Earlier this year, an FTI *Advice from Counsel* study, which evaluated the state of IG and information security at large corporations, found that many organizations too often view IT and information security roles as interchangeable. Study respondents stressed the danger of blurring lines between these groups and were clear that it is critical to understand the difference between the skill sets. Similarly, the role of the general counsel or in-house legal team plays in relation to information security is also often confused, which can create problems when it comes to obtaining buy-in for projects and ensuring approval across all departments. IG stakeholders—compliance, legal, IT, information security, records management, etc.—must all understand the differences and counter dependencies of critical roles and know which team to go to with various needs, as each group will have its own set of priorities and approach issues differently.

IT, under the CIO, is a service organization within a company, with the purpose of giving the business the technology it needs to function. IT keeps things running, initiates new systems, and troubleshoots when problems within the network arise. Conversely, the CISO and information security serve a compliance utility, focused on protecting the company's data and critical digital assets. The Compliance, Governance and Oversight Council (CGOC) provides guidance on this, and makes a clear distinction between IT and information security. Together with the EDRM standards group, the CGOC developed the Information Governance Reference Model (IGRM), which categorizes IT as an efficiency organization, and privacy and security as risk organizations. While both groups share some overlap in the assets, or 'containers of information' they provide to the business, their responsibilities and the value they deliver are unmistakably separate. The general counsel provides oversight of these and other functions, ensuring that legal risk of all projects and activities is understood and mitigated according to the company's existing obligations and risk tolerance.

Further, the National Association of Corporate Directors (NACD) offers literature urging boards to approach security as a risk management issue, not an IT issue. In a handbook, the NACD emphasized the challenge of "detecting the presence of attackers in an organization's systems and networks, [and that] on average, it takes 146 days before an organization realizes it has been breached." The NACD also mentioned the "severe consequences of cyberattacks, specifically noting that companies and directors can find themselves exposed to legal risks following an attack."

When IG teams are able to successfully separate these functions and work with each on the appropriate projects, an organization can achieve reduced risk and streamlined processes. One way of looking at it is by viewing IT as the gas pedal, and information security as the brakes. Both are equally important to keeping the organization moving in the right direction. Information security is sometimes seen as an impediment, but without reliable brakes, things can't move quickly and are more likely to spin out of control. Below are some approaches that can help draw lines between IT and information security, and ensure all stakeholders are collectively working together to reduce risk and optimize processes.

- **Check egos at the door:** Human nature is what it is, and often projects are hindered by egos or leaders that feel territorial over certain activities. Everyone involved in IG needs to be open to collaboration and understand that the work they do can be complementary. Each team has unique perspectives and expertise that bring value.
- **Playbooks:** The most successful teams address blurred lines at the outset of an IG initiative. This includes setting expectations early on and putting plans, workflows, and policies into a playbook that has buy-in across stakeholders.
- **Recognize pitfalls:** In many cases, security should not fall under the CIO's purview, and there can be conflicts of interest when it does (for example, a data breach caused by improper installation or management of certain technology). We're seeing a similar expectation on the privacy front, with the General Data Protection Regulation's guideline that corporations appoint data privacy officers and give them complete independence.
- **Proactively manage differences:** Working styles vary greatly, and oftentimes, people are simply not on the same page. Various people and teams will approach the same problem very differently. Teams can manage differences and get people on the same page by 1) defining agreed-upon verbiage; 2) taking time to think through different perspectives; and 3) keeping people looped in and abreast of changing processes throughout a project.

When the GC, CISO, and CIO are locked into their independent expectations and working well together, the benefits are significant. The risk assessment process is a prime example. When a new cloud system is being onboarded, IT will focus on delivering what the business users are asking for and handle the logistics of implementation. Alongside that, information security should be vetting the vendor's cybersecurity fortitude and asking, ''How are we protecting this new information store?'' Meanwhile, the legal department evaluates potential legal and compliance risks related to using the system. In a compliance or data breach situation or investigation, the CIO should only be involved as requested, allowing the legal and security teams full autonomy to conduct their work. In any case, when all three groups are on the same page, business needs can be addressed as quickly and efficiently as possible without compromising security or introducing more risk.

Deana Uhl is a Senior Director in the FTI Technology practice and is based in Houston. Ms. Uhl provides consulting to corporate clients, with a focus on designing, implementing and enabling change management for information governance, data privacy, data security and e-discovery programs. Ms. Uhl has particular expertise in advising oil and gas companies on the processes and technology to effectively address legal and regulatory matters and improve information quality and life cycle management to support operational excellence.

The views expressed in this article are those of the author and not necessarily those of FTI Technology or of Bloomberg Law.