ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Legal Ops Brief: Why Security Matters

Law Department Management

How does legal operations protect the vital information it possesses? No doubt all parties of the law business triad — legal departments, law firms, and business units — have asked this question. How do law departments feel when their information leaves the nest? How do lawyers and law firms protect and guard their client's most important digital assets when it shows up on their doorstep? How do the business providers who rent space in the clouds word the lease agreement and hold the keys? All these questions are on the minds of legal ops professionals.

Legal ops professionals as well as organizations managing information for legal purposes are working to ensure information is managed in a secure manner through process development, protection development, risk analysis, and enforcing policies to protect the greatest asset of their organizations.

Legal ops hold a unique portion of an organization's commitment to securing information, especially when it engages to develop secure processes for protection and risk analysis for guarding its organizations greatest assets. Let's start with the legal ops role in protecting information and why it is such an important task. But first some definitions associated with security and information protection:

- **Information security** is a concept of securing information through process and in any form.
- **Information governance and knowledge management** are key terms that law firms and law departments use when managing information.
- **Cybersecurity** is a term used to describe the specific measures of securing digital

information within a network or cyber-based platform from threats such as breach, theft, and/or corruption.
- **Threats** exist where external parties or internal bad actors can breach, steal, or corrupt such data assets, compromising the position or integrity of the client or the law firm.

Find a partner

The role of the legal ops function is to ensure security risk assessment. Alongside information security or information technology (IT) groups, they provide leadership and collaboration among the triad of the legal partnership ecosystem.

Here is a basic example of how this works: Law departments engage with law firms and business partners to work on a specific legal matter. Current best practice is for master service agreements (MSAs) to include provisions for cybersecurity. MSAs should specify a cyber audit of the external party’s data hosting facilities, lines of data transfer, qualifications to manage data (e.g., personnel certifications or ISO certifications), and processes involved with protections such as breach of firewall, catastrophic failure of servers, and monitoring entry to secure locations.

Law departments usually work with their IT or information security teams prior to engagement to ensure that data leaving the organization will be protected and secure with their dedicated partner. By evaluating the security parameters, the company can withhold engagement due to insufficient security measures or inability to address such concerns or proceed if it meets security standards.

In turn, the recipients of the engagements (law firms/business partners) perform the necessary actions within the criteria of evaluation and meet expectations or address issues or deficiencies. While the process is both business and technology focused, the result is to ensure client and provider can assure information is managed safely and securely, promoting strong working relationships, and reducing the risk of threats.

Legal ops leads in this space because it occupies the intersection between law departments, law firms, and business partners at the operational level. Only legal professionals understand other legal professionals — so leave it to the professionals. Legal ops groups typically work with information security and IT teams to promote transparency in process. By establishing what is necessary within the law triad, legal ops professionals and their partners set the parameters.

> Legal ops groups typically work with information security and IT teams to promote transparency in process.

It is important to remember there is no one size fits all solution. For example, financial organizations, such as banks and security brokerage firms, require compliance standards that are mandated by the local or national governments. Depending on the industry, companies will need to utilize different approaches to reduce the threats that may damage the reputation or revenue of the client.

These formal compliance procedures and actions must be implemented, sustained, and monitored by personnel in each law firm, law department, or business provider — or else security is compromised.

Cybersecurity insurance

A cybersecurity insurance provision is now a common part of an MSA. Legal operations groups have been engaging cloud service providers with stringent provisions for cybersecurity insurance to protect from damages in the event of significant loss or reputable damage.

Cloud service providers have purchased cybersecurity insurance policies to meet client demands. By choosing a cloud provider with proper cybersecurity insurance, legal ops professionals align internal technology practices to ensure client needs are met for storage, processing, and transmission.

Audit, audit, audit

Legal ops should also lead a continual audit to evaluate both internal and external security measures. Perform an annual security check when law firms or business partners begin an engagement. The annual security audit is a part of the preferred status arrangement, which the engaged firm must complete to maintain status.

Law departments share accountability in maintaining secure information. There is always the risk of infected files, ransomware inadvertently downloaded, or bad actors causing issues — but it’s critical to manage that risk.

Legal ops is the binding element that protects information between the legal business triad, keeping everything moving in the safest and most protected way possible.

Jack Thompson

Assistant Director - Global eDiscovery & Legal Operations

Sanofi

Jack Thompson is assistant director of global eDiscovery and legal operations for Sanofi, a global biopharmaceutical company.