

Just What the Data Ordered

FOR SPLUNK, SWIFT GROWTH LED TO NEW POLICY AND PROCEDURAL REQUIREMENTS—AND NEW LEGAL CONSIDERATIONS BY ERIN BRERETON

San Francisco-based software provider Splunk's data collection and analysis product, Splunk Enterprise, was an almost instant hit upon its debut in 2006. The software, which collects and analyzes machine data generated by websites, applications, networks, and RFID assets, can identify traits like user transaction patterns and performance issues, making it useful for everyone from pizza companies to disaster relief agencies.

Companies can use Splunk Enterprise to identify fraudulent wire transfers while they're happening, route telecommunication carrier calls more efficiently, understand order delivery delays, and improve dozens of other operations.

In its first five years, Splunk's customer base swelled from 150 clients to more than 3,000. But it still relied exclusively on outside counsel to handle legal needs—until Splunk CEO Godfrey Sullivan met Lenny Stein. The former chief legal officer at winemaker Jackson Family Enterprises was introduced to Sullivan by mutual friends. Sullivan wasn't looking for a GC, Stein says. But the two got along well, and within three weeks, Stein had joined Splunk.

"The company was at an early stage and still growing rapidly," Stein says. "Its legal needs were finally getting some much-needed focus."

Stein—who has worked as GC for both start-ups and multibillion-dollar corporations—began to institute the procedures required for Splunk to eventually go public. "I did a systematic assessment of the legal needs across all functions and aspects of the business," he says. "From that, I knew what was in good shape and what required more attention."

For example, the company needed to ensure it had the proper export control policies in place. Splunk's software was

able to help because it is able to detect users' geographic location by IP address when they attempt to download the product. By correlating user data with a third-party database, Splunk has been able to reject access for U.S. trade- and transaction-prohibited countries and persons and also to document its compliance with export controls.

Splunk's federal government contract work also necessitated internal compliance checks. In recent years, the customer base has expanded to include security operational centers within companies, universities, and government agencies.

While the government can be a good customer, federal contractor agreements can present concerns involving intellectual property development and pricing and billing terms, notes Rick Vacura, who co-chairs Morrison & Foerster's Government Contracts Practice and who has worked with Splunk on government compliance matters. "You have to have certain compliance policies and procedures—Lenny understood that message loud and clear. When Splunk's government market started to grow, he wanted to put into place what compliance,

infrastructure, and experienced personnel were needed so he could sleep better at night and the business could grow with minimum compliance risk."

Requirements vary based on the type of contract, but contractors are generally subject to audits requiring them to substantiate any charges billed to the government. Splunk had to ensure it was carefully tracking expenses, expenditures, and other project details. "It's not unusual to have government auditors request access to a contractor's books and records regarding invoices that were submitted to—and paid by—the government three or more years prior to the audit," Vacura says. Having those records available is important because companies that can't prove compliance face stiff penalties. "If the company doesn't deliver what it promised and lacks adequate books and records, it can quickly turn into a civil or criminal false claims case," he says.

As Splunk's compliance needs grew, its legal department expanded from one person—Stein—to 17 in-house professionals. The company's client base has also increased to more than 7,000. Splunk hosts a robust online community where customers share tips for implementing Splunk products. Splunk's developers generate new offerings, but many of Splunk's new use cases actually come from its customers, Stein says.

"Organizations have come to recognize the tremendous value within their machine-generated data, now that Splunk has provided a platform to gain insight from that data in real time," Stein says. "Our customers have really led the way for our product's growth."

"The company was at an early stage and still growing rapidly. Its legal needs were finally getting some much-needed focus." LENNY STEIN



COMPANY: SPLUNK
LOCATION: SAN FRANCISCO
REVENUE: US \$302.6 MILLION (FY2014)
EMPLOYEES: 1000 (2014)
WHAT THEY DO: PRODUCE SOFTWARE FOR SEARCHING, MONITORING, AND ANALYZING MACHINE-GENERATED BIG DATA, VIA A WEB-STYLE INTERFACE.