COSMOS
Navigate the Compliance Universe

ethikos Volume 33, Number 7. July 01, 2019
Protecting client data and assets against internal and external threats

By Christine Julien, Esq.

Christine Julien (Julchristine@gmail.com) is a regulatory healthcare and workers' compensation attorney in New York.

In recent years, a big concern of financial institutions has been the threat of client data and personally identifiable information (PII) reaching the wrong hands and how best to protect that data against serious security breaches. Financial institutions are corporations that provide services as intermediaries of financial markets and include but are not limited to banks, credit unions, insurance companies, lending companies, and investment and brokerage firms.

With advancements in technology and the rise of e-commerce, electronic payment methods, and mobile banking/investing, there is no shortage of PII and confidential client data floating in the "clouds." According to Wikipedia, *cloud storage* is defined as "a model of computer data storage in which the digital data is stored in logical pools. The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company."

The threat that confidential client data, including but not limited to account numbers, passwords and emails, could be compromised and land in the hands of cyber criminals is a serious enough concern that companies have invested in the latest technology and hired the best security and IT professionals and legal compliance experts to mitigate those risks. Hackers, scammers, and thieves have likewise become more sophisticated and aggressive in their attacks using malware, spyware, and other schemes to look for the slightest weaknesses in security to compromise data and launch phishing attacks and other fraudulent activities. One bad mistake or loophole can leave a company vulnerable to cyberthreats resulting in an incident or breach that may or may not require notification to the client(s) whose data has been compromised. However, the incident and/or breach and the response are all critical issues that must be handled appropriately, and if not, can ultimately cost an organization everything—its goodwill, reputation and client trust. The organization may also find itself in serious legal troubles with the regulators. However, with the focus on combatting external threats, have companies become too lax and, in some instances, negligent in protecting clients and consumers against *insider* threats?