COSMOS
Navigate the Compliance Universe

CEP Magazine - June 2018
Technology risk assessment for compliance: Data privacy and security risks

By Lauren Connell

Lauren Connell (connell.lauren@gmail.com) is Managing Associate at The Volkov Law Group in New York, NY.

Compliance officers operate where the rubber meets the road, where regulatory requirements are translated into specific controls over business conduct. We are experts at operationalizing policies and procedures. As technology has transformed the way business is done, it is no surprise that Compliance departments have had to make adjustments to align operations with compliance requirements. Now, Compliance departments are perfectly situated to address new challenges posed by the new risks technology creates, including data security and privacy.

The financial industry has been a compliance leader in this area because of Financial Industry Regulatory Authority regulations that apply to electronic communications and social media and, more recently, requirements imposed by the New York Department of Financial Services.[1] Other industries are behind the curve but, faced with quickly growing risks and regulatory demands, are working hard to catch up.

Risk sources and regulatory demands

Companies are facing risks from criminals and hackers as well as increasing regulatory expectations. Compliance is a natural partner for the Information Technology (IT) department to address these very real dangers.

Criminal risks

In this age of technology driving business operations, hackers are getting increasingly creative, creating serious risks and potentially devastating harm to large and small businesses alike. From basic ransomware attacks to full-out assaults designed to collect sensitive personal and financial information, businesses must embrace compliance and defensive solutions to prevent devastating attacks. Last year, businesses such as HBO, Anthem, Experian, and many others suffered harm that was widely reported in the news media. In the case of HBO, hackers gained illegal access to unreleased shows, including an episode of HBO's *Game of Thrones*, embarrassing internal emails, and private employee records. In another case, North Korea launched a global ransomware attack and took advantage of infrastructure weaknesses to spread mass chaos, locking people out of their information systems around the globe. Most worrisome, the attack severely affected the UK's healthcare industry, causing very real risks to people seeking healthcare.

In addition, traditional risk sources, such as physical security or employee access to confidential information, now pose a greater threat when technology can amplify the impact. For example, whereas a door left open may have resulted in petty theft in the past, now a door left open can result in the theft of technology that holds valuable confidential information. Even the theft of a single external hard drive can cause hundreds of thousands of dollars in remediation costs if it, for example, contained payment information from customers or personal information of employees.

Regulatory demands

Meanwhile, government regulators are addressing the impact technology has had on business by requiring businesses to improve technology and security capabilities. The U.S. Department ofJustice recently released a new Foreign Corrupt Practices Act Corporate Enforcement Policy[2] that requires companies seeking leniency benefits to maintain business record retention policies to prevent the destruction of electronic records, and to prohibit "employees from using software that generates but does not appropriately retain business records or communications." For example, if your employees are regularly communicating on a chat feature, does your business retain those records? What about communications made on the company's behalf over social media?

Most businesses are also aware that the EU's General Data Protection Regulation came into effect in May 2018, along with its very severe penalties, up to 4% of a company's annual revenue. Businesses covered under this regime must focus on their data privacy regimes and protect any personal data about any EU citizen that the business may collect.[3]

Compliance is a natural partner

These are not just problems for the company's IT department. Corporate functions across the board now face very real and significant risks concerning data management and privacy. Compliance departments are natural partners—even leaders—when it comes to identifying risks and developing strategies to mitigate such risks. Well-designed policies and procedures, training, cross-functional coordination, and auditing and monitoring to ensure compliance—these are all risk mitigation steps that Compliance departments are best suited and experienced to take on.