$1.50 VOL. 39 NO. 25 www.ocbj.com JUNE 20-26, 2016

ORANGE COUNTY BUSINESS JOURNAL

TROUTMAN SANDERS

Lessons in Commercially Reasonable Data Security

by Ronald I. Raether, Partner, and Megan Nicholls, Associate, Troutman Sanders LLP

Information security presents a real problem for many companies and the issue is increasing in importance and complexity. Many businesses are in denial that they could ever suffer a breach; unwilling to address security for fear that doing so will impede profitability. What is the net value to the bottom line if criminals are permitted to steal the identity of your valued customers, your intellectual property and diminish your goodwill?

Ronald L. Raether

So, how do you prevent your company name from headlining the next data breach notification story? The simple answer: Maintain a robust information security program by understanding how information is received, used, stored and transmitted both inside and outside the organization. At the core of many information security laws is a layered approach to data security involving sound technology, administrative controls and a well-thought out data governance plan.

Creative use of Technology

Companies should employ a layered security approach in accordance with industry standards that addresses any issues unique to its business. This can include perimeter security, intrusion detection systems, egression device monitoring, oversight and surveillance technologies and the like. With this layered approach, when one security element fails, there are several others in place to mitigate, if not prevent, the resulting harm. Mobile devices, wireless networks, and remote company server access all play a key part in the ever-expanding virtual 'office' space increasing efficiency and flexibility, but they may also increase a company's risk of breach. Companies must balance the benefits of technology with appropriate enterprise risk management to isolate and minimize security threats, as well as mitigate resulting harms. Centralized control is essential.

Administrative Controls and Data Governance

Information should be managed according to sensitivity of the information and the risks posed if the information is stolen. A company must look at how each category of information is accessed or transmitted, by whom and for what purpose. Employees and third-party contractors have access to data and systems that can impact security well beyond their office space or assigned job responsibility. Ultimately, more sensitive, or high-risk/high-injury, information should be segregated from and guarded more securely than less sensitive, or lower-risk/lower-injury, information.

Megan Nicholls

A company's written policies and procedures should set forth clear, comprehensive and repeatable controls to restrict and audit access to and use of sensitive information. Regulators and law enforcement will have an easier time understanding a company's efforts if written policy and procedures are in place. But that is not enough. Employees must be trained regularly on their information security role and companies must audit for compliance with these policies and procedures.

Companies can ultimately limit the risk posed by creating a culture where every employee is empowered to take an active role in information security, regardless of hierarchy, through education and accountability. The most effective information security regimes have some relation with general counsel or another individual that can take concerns to the board and help achieve the proper balance between business functionality, privacy and information security.

For more information, contact Ronald I. Raether at 949.622.2722 or ronald.raether@troutmansanders.com. Contact Megan C. Nicholls at 949.622.2789 or megan.nicholls@troutmansanders.com.