CARLTON FIELDS

Heal Thyself: Insider Threats to Heed, Especially for Industries with Large Amounts of Personal Information

August 22, 2016

A recent study by the Ponemon Institute found that insider threats due to malicious or negligent employees are the leading cause of private-sector cybersecurity incidents. Of the over 600 information security professionals surveyed, more than half reported that their organizations have suffered incidents or data breaches due to insiders' mishandling of data. Surprisingly, despite the prevalence of such insider mishandling, less than half of the companies require employees to undergo security training, and only about one-third of senior managers believe that employee awareness of data security risks is a priority for their senior executives. Reducing insider threats is even more important for organizations in industries where employees have access to vast amounts of highly sensitive personal information, such as the health care, financial services, insurance, and education industries. With that highly sensitive personal information comes greater customer expectations of privacy. In addition, organizations in these industries are subject to sector-specific privacy laws. Indeed, lackadaisical training and poor internal privacy and security programs can run afoul of laws such as the Health Insurance Portability and Accountability Act, the Gramm–Leach–Bliley Act, and the Family Educational Rights and Privacy Act, potentially leading to hefty financial penalties and sanctions, even in some cases in the absence of an actual breach. In addition to legal liabilities, insider breaches can cause reputational damage and compromise intellectual property. Another recent Ponemon study not only identified insiders as a significant cause of incidents, but also quantified the additional cost of data breaches to companies in higher-risk industries. In that regard, the study found that, while the overall average cost for every record lost or stolen in a breach was $158, it was $355 for health care organizations (more than double the overall average cost), $246 for educational organizations, and $221 for financial institutions. The same study also identified health care and financial services as the industries with the two highest customer churn rates, a factor that contributes significantly to incident response costs. Taken together, these studies make clear that insider threats should not be overlooked, especially within industries with large

amounts of sensitive data. The good news is that organizations can take steps to mitigate the risks posed by insiders. In fact, the first of these studies highlighted some best practices to improve security awareness and reduce insider threats, including:

- requiring mandatory security training for all employees, including C-suite executives;
- "gamifying" training (i.e., making it interactive and real-time) to encourage participation, knowledge retention, and good habits acquired during training;
- designing an enforcement system that combines rewards and punishments tied to data security; and
- establishing, from the top-down, an organizational culture of security.

Every organization must develop its own privacy program based on the nature of its business and the regulatory scheme in which it operates. Organizations, particularly those in higher-risk industries, would be well-served by reviewing these studies and implementing these best practices. After all, when it comes to cybersecurity, often the greatest risk comes from within.

Related Practices

Consumer Finance
Technology
Cybersecurity and Privacy
Labor & Employment

Related Industries

Technology