Insights: News Releases

2016 Data Theft Survey

JULY 20, 2016

New Study Reveals that Companies Are Unprepared to Protect What Matters Most to Them

ATLANTA (July 20) – Responding to the increasing cyber threat to organizations' most vital confidential information – their "knowledge assets" – Kilpatrick Townsend & Stockton and Ponemon Institute released today their findings from *The Cybersecurity Risk to Knowledge Assets* study. This inaugural study kicks off an initiative to provide organizations with the tools they need to protect their most important assets in the information age.

Knowledge assets are confidential information critical to a company's core business -- other than personal information that would trigger notice requirements under law -- including trade secrets and corporate confidential information such as product design, development or pricing; other non-public information about the organization, its plans or relationships; or other crucial customer information.

The survey was conducted to determine the extent of the risk and organizational effectiveness in safeguarding such data, to assess whether the widespread publicity accorded data breaches subject to notification laws and related regulatory requirements have skewed organizations away from a focus on theft or loss of their most critical information, and to compile and provide helpful practices.

More than 600 individuals familiar with their companies' approach to managing knowledge assets and involved in the management process were surveyed.

How serious is the threat and how prepared are corporate entities?

Theft is rampant. Seventy-four percent of respondents say it is likely that their company failed to detect a data breach involving the loss or theft of knowledge assets, and 60 percent state it is likely one or more pieces of their company's knowledge assets are now in the hands of a competitor.

Companies don't know what they need to protect, or how to protect it . Only 31 percent of respondents say their company has a classification system that segments information assets based on value or priority to the organization. Merely 28 percent rate the ability of their companies to mitigate the loss or theft of knowledge assets by insiders and external attackers as effective. The great majority who rate their programs as not effective cite as the primary reasons a lack of in-house expertise (67 percent), lack of clear leadership (59 percent), and lack of collaboration between different job functions (56 percent).

Executives and boards aren't focused on the issue and its resolution. A data breach involving knowledge assets would impact a company's ability to continue as a going concern according to 59 percent of respondents, but 53 percent replied that senior management is more concerned about a data breach involving credit card information or Social Security numbers than the leakage of knowledge assets. Only 32 percent of respondents say their companies' senior management understands the risk caused by unprotected knowledge assets, and 69 percent believe that

senior management does not make the protection of knowledge assets a priority. The board of directors is often even more in the dark. Merely 23 percent of respondents say the board is made aware of all breaches involving the loss or theft of knowledge assets, and only 37 percent state that the board requires assurances that knowledge assets are managed and safeguarded appropriately.

The cost is high, and it may not be covered. The average cost to remediate attacks against knowledge assets in the past 12 months was $5.4 million, with nearly 7 out of 10 respondents saying that the maximum cost estimates for such attacks would top more than $100 million and almost 5 out of 10 assessing the cost at more than $250 million. On average, only 35 percent of the losses resulting from the theft of knowledge assets are believed by respondents to be covered by their company's current insurance.

Careless employees and unchecked cloud providers are key risk areas. The most likely root cause of a data breach involving knowledge assets is the careless employee, but employee access to knowledge assets is not often adequately controlled. Fifty percent of respondents replied that both privileged and ordinary users have access to the company's knowledge assets. Likewise, 63 percent of respondents state that their company stores knowledge assets in the cloud, but only 33 percent say their companies carefully vet the cloud providers storing those assets.

"In the data classification schemes we have helped create over the years, we have often seen companies identify their most essential knowledge assets, and then face the fact that -- until that moment -- they have provided no special cyber or any other protection for those assets commensurate with their importance," said Jon Neiditz, Co-Leader, Kilpatrick Townsend Cybersecurity, Privacy & Data Governance Practice. "For our clients who invent, we encourage them not to 'leave knowledge assets on the table' -- to choose between, for example, patent, copyright, trade secret and/or contractual protections (including in open source) and then arrange for cybersecurity and insurance protection accordingly."

Mr. Neiditz continued, "By focusing on the application of good cybersecurity risk management principles to prioritized knowledge assets, this research breaks new ground for boards of directors and organizational leaders in fields such as information security, legal, audit, risk management, compliance, IT, intellectual property, privacy, human resources and procurement. The importance to chief privacy officers, for example, is evident from non-notice-triggering customer information being respondents' highest-valued knowledge asset across all industries. To all organizational leaders, the study offers a call to action and a set of arguments justifying action while also providing an ongoing chronicle of successful and unsuccessful practices and programs."

"Companies face a serious challenge in the protection of their knowledge assets. The good news is there are steps to take to reduce the risk," said Dr. Larry Ponemon, Chairman and Founder, Ponemon Institute. "First of all, understand the knowledge assets critical to your company and ensure they are secured. Make sure the protection of knowledge assets, especially when sharing with third parties, is an integral part of your security strategy, including incident response plans. To address the employee negligence problem, ensure training programs specifically address employee negligence when handling sensitive and high value data."

For a copy of the executive summary and full report, please click here.

About Kilpatrick Townsend

To help safeguard our clients' information, business operations, intellectual property, and corporate reputations, Kilpatrick Townsend's Cybersecurity, Privacy & Data Governance Practice offers the full spectrum of cyber legal

services across the U.S., Canada, Europe, Asia, and Latin America. Our integrated team of multidisciplinary attorneys uses its in-depth experience and legal acumen to help clients identify and protect their knowledge assets and prepare for and effectively respond to data breaches and incidents. For more information, please click here.

About Ponemon Institute

The Ponemon Institute© is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors and verifies the privacy and data protection practices of organizations in a variety of industries. For more information, please click here.

###

Related People



Jon Neiditz

Atlanta, GA
t 404.815.6004
jneiditz@ktslaw.com