Ashley Madison – That Electronic Communications Policy Was a Good Idea After All

Insights
9.01.15

When does an employee's extramarital activity become his or her employer's concern?Before the Ashley Madison breach, the answer might as well have been "[almost] never."

Since the Ashley Madison breach has a sufficient tinge of prurient naughtiness and scandal, the media has given the general public an unusual gift for a cybersecurity breach—ongoing coverage, revealing in unusual detail the repercussions of a data breach. Onlookers can perceive, or at least imagine, the worst-case scenario of a data breach, hopefully from dry land high above the storm below.Many are not so lucky to breathe such rarefied air.

One surprising statistic is the number of government e-mails used to create accounts on Ashley Madison, which has spurred a number of investigations for employee misconduct, citing inappropriate use of public resources and time.The data dump revealed as many as 15,000 accounts linked to federal government e-mail addresses or computer systems—that number does not include access from state and local government employees.

The statistic raises a concerning question for employers in general; when an employee misuses company resources and compromises their own privacy, what do you do?In a case like the Ashley Madison case, where misuse was apparently rampant, it may lead to unwanted negative attention from the public.For employees who deal with sensitive information, such as U.S. Attorneys, military personnel, or representatives within Homeland Security, a breach such as Ashley Madison presents an opportunity for outsiders to test the loyalty of employees.Furthermore, such public attention compels an employer to consider their own policies to determine whether and how they must discipline their employees.Moving forward, how closely should employers monitor employee usage of company resources?A good policy, tailored to a company's model practices will place employees on notice of the ramifications of misconduct, allowing managers to investigate misconduct and take action that can protect the company from damage.A well drafted policy will also outline the appropriate and legal boundaries of conduct for a manager during such an investigation.

Private employers observing how government agencies handle the breach should take note that private and public employers are subject to different privacy standards, since public employers, as extensions of the government, are subject to unreasonable search and seizure restrictions under the 4th Amendment of the U.S. Constitution.Investigations of federal employees will be subject to the standard set forth in *O'Connor v. Ortega* [1987] 480 U.S. 709: that the search must be (1) justified at

standard set forth in *O'Connor v. Ortega* (1987) 480 U.S. 709, that the search must be (1) justified at its inception, (2) limited to measures reasonably related to the objectives of the search, and (3)not excessively intrusive in light of the circumstances.Furthermore, government agencies have varied degrees of interest based on security clearance and area of work; for example, Homeland Security and branches of the military will undoubtedly treat misconduct differently than municipal governments will.Private employers will be subject to standards established by laws that vary from state to state.

Employers who do choose to examine the Ashley Madison data dump to determine whether employees have misused company resources in violation of a specific policy should exercise caution.ALM did not verify e-mail addresses, therefore, the mere appearance of an employee's e-mail address in the data dump does not provide conclusive evidence of misuse.Additionally, the appearance of a company IP address in the data dump could be a result from guest use of the company network.