In 2018, Resolve to Keep Employment Records Secure

Labor & Employment Law Update

on February 8, 2018

Though hacked systems are alarming, too often, data breaches come from much more obvious sources, such as computers without passwords (or weak ones), files left sitting out on desks, and even briefcases left on airplanes (like Department of Homeland Security analysis of terrorist threats at the Super Bowl). An employer's exposure for data breaches can be significant. At minimum fines, civil suits (including class actions), lost trust and bad publicity, and remediation costs.

In 2017 alone, some of the major headline data breaches include the *Paradise Papers* and *Panama Papers* scandals (two data breaches totaling 3.9TB of data and 24.5M documents), a credit reporting agency, a telecom provider and a wholly owned web service provider. As we previously discussed, employers are obligated through various statues and regulations to keep and maintain many types of employment records containing significant personal, confidential, and highly sensitive information. Such records range from job applications and resumes, to tax forms and benefits applications, to medical records stemming from workers' compensation, disability, and FMLA claims. These records contain employees' (and their dependents') addresses, phone numbers, social security numbers, dates of birth, banking and financial information, and highly sensitive medical information. Other internal files may contain client information, usernames, and even passwords that employees keep the same across work and personal accounts. **In short, employers maintain all of the information necessary to completely hack sensitive information exposing all employees to possible identity theft, or other adverse use of their private information.**

Data Security in the 21st Century

The significant data breach risks require companies to practice good record maintenance hygiene. Some important and simple steps to follow in 2018 include:

- Secure electronic systems: restrict access to necessary programs, folders, and files, with employees using unique, memorable passwords/passphrases. Perform a physical "audit" to ensure employees are not storing passwords beneath keyboards (yes, it still happens!).

- Utilize protection: lock offices, install privacy screen filters, keep files secured. Remember, a data breach can be as simple as one prying employee looking in another's file left on a desk – or the cleaning service pocketing an entire file.
- Keep communications confidential: avoid unintentional disclosure through speakerphone and group printers.
- Enable remote wipe capabilities in case portable devices are lost, stolen, or otherwise compromised.
- Plan for the unexpected: establish protocols to secure systems and maintain data integrity should it be necessary to terminate an employee, including the chief technology officer, and how to handle a data breach should it occur.
- Engage legal counsel as necessary to perform audits of policy and practice, address high risk situations to ensure legal compliance, and shepherd remediation and handle concise communications if and when a breach occurs.

Through strategic planning and implementation of security policies and protocols, companies can be prepared to efficiently address situations in a fluid and dynamic manner without impeding operations.

In 2018, Resolve to Keep Employment Records Secure