THE SONY PICTURES ENTERTAINMENT, INC. SCANDAL SERVES AS A WARNING TO EMPLOYERS ABOUT COMPUTER SECURITY

Employers' Advisor Blog Archives
December 23, 2014

Attorneys

Elizabeth McPhail

In recent days, the scandal with Sony Pictures Entertainment, Inc. went from an embarrassing tabloid scandal to a possible terrorist threat. The breach also has impacted thousands of current and former employees. On December 15, 2014, a federal class action lawsuit was filed in California on behalf of current and former employees. The complaint asserts that Sony has not taken adequate steps to prevent the massive breach and protect the personal information of over 15,000 past and present employees whose data was compromised.

The exposed personal identifying information, the complaint asserts, includes "current and former employee names, home addresses, telephone numbers, birthdate, social security numbers, email addresses, salaries and bonus plans, healthcare records, performance evaluations, scans of passports and visas, reasons for termination, details of severance packages, and other sensitive employment and personal information." The suit claims that Sony made a business decision to risk a breach of this personal identifying information despite knowing for years that there were weaknesses in their computer network.

The alleged causes of action in the Sony case include negligence, violation of a California statute related to the confidentiality of medical information, violation of California Civil Code Section 1798.82 related to computerize data, and violation of the code of Virginia Section 18.2-186.6 related to personal information. The complaint seeks both monetary and injunctive relief, as well as costs and experts'/attorneys' fees.

Apparently, this is not an isolated issue. Michael McCartney is a computer forensics expert and the president/CEO of DIGITS LLC. He advises that "in addition to direct costs associated with responding to a data breach such as this, there are also a tremendous amount of soft costs associated with the liability of reporting, litigation, fines and possibly penalties." Mr. McCartney's words should be of great concern to employers considering that "it is estimated that 60% of companies that suffer a data breach will be out of business within 6 months of that breach." Mr. McCartney counsels that "companies need to take an aggressive proactive role in protecting their data and planning for a data breach. Security assessments, vulnerability assessments, network monitoring, security policy review, and incident response

planning are just a few things companies can do to better prepare their security posture."

Companies often spend much of their efforts regarding computer security focused on regulatory requirements and ensuring that customer information is not breached. All of this in mind, employers should also be focused on protection of employee information that is electronically stored.