

Keeping Confidential Information Confidential: It's Time for HR, Legal, and IT to Work Together

By **Jennifer Baldocchi** and **Heather Morgan**

On November 24, 2014, Sony Pictures Entertainment employees logged onto their computers to find waiting for them a threatening message from hackers. Over the next several weeks, detailed, confidential data about the company and its workforce was publicly released to Internet users everywhere. As reported by the media and alleged in the multiple class action lawsuits against Sony that followed in the wake of the breach, the leaked information ranged from:

- personal data of tens of thousands of employees, including their Social Security numbers, medical files, passports, and visas; to
- valuable company secrets, such as unreleased movies, film budgets, and contracts; to
- sensitive data and email communications.

Sony will vigorously defend claims that it negligently failed to secure its employees' most private and sensitive personal information, and the viability of the lawsuits remains to be seen. However, the surrounding publicity has served as a grim reminder of the very real and ongoing threat that all employers face in today's global, mobile, and digital world.

A growing list of large companies have suffered the unlawful disclosure of personal, proprietary, and sensitive data from their computer systems and its devastating repercussions. Cybersecurity experts warn that it is not a matter of if a company will experience a data breach, but when. These same experts agree that the biggest threat may not come from external hackers, but from intentional or accidental internal cyber breaches. Insufficient procedures, the lack of consistent monitoring, and poor policy enforcement contribute heavily to data breaches.

Of course, safeguarding data has grown *far* more complex since the days of filing cabinets and locked drawers. The sheer volume of information exploded over the last decade. It migrated to shared drives, laptops and PCs, smart phones, email, the cloud, thumb drives, and external hard drives. Most companies keep *huge* amounts of confidential data — intimate private details about the workforce, trade secrets, privileged, sensitive email communications, and more. At the same time, a diverse body of law developed. A long list of cryptic acronyms now governs the information revolution: UTSA, EEA, HIPAA, CMIA, FACTA, CFAA, and NSPA to name a few. Not surprisingly, case law flourished and splintered as it followed the twists and turns of information governance.

Protecting information is hard. Traditionally, IT professionals shouldered the bulk of this responsibility, constantly striving to stay one step ahead of cybercriminals and rogue employees. But digital solutions are only part of the equation. Lawyers and human resources professionals must join the defense.

Simply stated, IT must provide the tools, while lawyers provide the rules, and HR implements and monitors. Without these three groups working seamlessly together, a company will leave chinks in its armor. So too, employers who persist in treating data management and security as just an IT issue — or who are too overwhelmed to take control of their workforce data — are the most likely to be featured in the next headline-grabbing scandal.

Whether the confidential data are the company's most valuable "crown jewels," or instead, private personnel records and sensitive email communications, safeguarding the data requires a clear understanding of the duties and the interests at play, and a commitment from IT, lawyers, and HR to work together. As a united front, these groups can create the culture of compliance necessary to keep confidential information confidential.

Where and How to Begin?

As employment lawyers, we have deep experience advising companies who seek to implement and sustain enterprise-wide personnel processes to better achieve legal compliance and reduce legal risk. We know how to help employers proactively diagnose and remedy high stakes risk issues. Building a robust data protection program requires a well-thought plan, streamlined investigation to prioritize risk, and the creation of baseline standards and best practices. It requires knowing when to draw upon the targeted expertise of attorneys in our **Privacy and Data Security** practice and collaborate with outside consulting firms. It requires knowing how to tailor legal advice and the program contours to meet the unique needs of each company's workforce organization, HR infrastructure, and culture. It requires leveraging information that we have learned through years of helping employers build state-of-the-art personnel processes and defending against employment lawsuits and agency audits.

Our approach to helping employers better manage and protect their data recognizes that companies need help prioritizing the chaos spawned by years of uncontrolled data proliferation. We also know that employees can be either the strongest or weakest link in any company's data protection program. The fundamental steps to building such a program include:

- **Data Prioritization:** Understanding what the company has, such as personal employee data, regulated data, third party provider data (and access to data), trade secrets, privileged information, sensitive communications, and other reputational data.
- **Evaluating Current Storage, Retention, and Tech Use Policies:** Documenting what practices and protections already exist.
- **Creating Best Practices and Baseline Standards:** Recommending additional steps to ensure legal compliance and safekeeping.
- **Implementation:** Operationalizing and monitoring the data protection regime.
- **Incident Response:** Developing a detailed plan to respond when a data breach occurs.

Please contact us if you are interested in learning more about some or all of the steps outlined above. We are committed to helping employers make their data work for and not against them.

We look forward to helping you better protect your data and navigate the future of employment law.

#1 in *The American Lawyer's A-List of the Most Successful Law Firms in America*

Top 5 for the past 3 years in the *Financial Times' North America Innovative Lawyers Report*

