"Preventing employee theft of company data is as much about changing culture as it is about adding technology... The key to a comprehensive insider threat program is to ensure that your technical capabilities and culture of security complement each other."

The Intersection of Human Resources and Cybersecurity: How to Mitigate Threats From Within

Q: AS DATA BREACHES PROLIFERATE, COMPANIES ARE RAMPING UP THEIR CYBERSECURITY PROGRAMS. IN ADDITION TO PROTECTING AGAINST CYBER CRIMINALS, WHERE ELSE SHOULD COMPANIES FOCUS THEIR EFFORTS?

SETH P. BERMAN: Since the threat of outside hackers is constantly in the news, there is a tendency for companies to overlook the fact that the most common causes of data breaches stem from within their organizations. According to the *IBM 2016 Cyber Security Intelligence Index*, 60 percent of all data breaches are caused by insiders. When devising data security plans companies need to remember that not all threats originate outside the company's firewalls. Employers must take steps to minimize the risk of rogue insiders misappropriating intellectual property, financial data, or customer contact lists.

Q: DO YOU HAVE ANY TIPS ON HOW TO PREVENT INSIDER THEFT OF DATA?

SB: Preventing employee theft of company data is as much about changing culture as it is about adding technology. Many employees who steal data justify it to themselves because it doesn't seem wrong. Indeed, there is a societal disconnect on what data belongs to whom on a corporate computer. Employees typically feel that any data they worked on or contacts they made belongs to them, and can therefore migrate with them to next employer. However, employers (and, in most instances, the courts) don't share this view. Thus, the first step in combatting insider threats is to address this disconnect. Companies should regularly remind employees that they do not own company data. Training should occur several times during an employees' tenure, including at their initial training, during annual compliance sessions, and, perhaps most critically, as part of the exit process. Of course, training alone won't solve this problem. Companies also need to institute security controls, consider using data loss prevention software and ensure that they have adequate logging and monitoring capabilities. The key to a comprehensive insider threat program is to ensure that your technical capabilities and culture of security complement each other.

Q: HOW CAN HR PROFESSIONALS HELP PROTECT AGAINST DATA BREACHES?

SB: Good data security training starts the moment a new employee is hired. When employees join, HR should inform them of the security policies and remind them that company data belongs to the company. Equally important, HR should ensure that employees know that the company does not allow data taken from a prior employer to be put onto its computer system. Employees should be required to acknowledge this policy in writing.

When employees leave, regardless of the reason, HR should notify them that they cannot take any company data. HR should specifically ask whether the employee believes that any data on the corporate network belongs to the employee (such as personal photos or documents) and find out if the employee intends to copy that data before leaving. If there is data that the employee is allowed to retain, HR should work with the departing employee to establish guidelines over what specific data is being retained and how that will be accomplished. For select employees, it might be prudent to conduct a digital forensic examination of their computers to ensure that they abided by these guidelines – it is far easier to address this kind of theft if it is discovered promptly.

Finally, HR and IT departments should coordinate to cut off access to corporate IT systems when an employee leaves. IT must also change the passwords for any administrator or shared accounts that the employee used. These seemingly obvious steps are missed all too often. A surprisingly large number of hacking incidents are caused by recently departed employees who log back into their former employer's network using either their own credentials or the credentials of someone else they know at the company.

Seth P. Berman

PARTNER
Privacy and Data Security
617.439.2338
sberman@nutter.com

Seth P. Berman leads Nutter's Privacy and Data Security practice group and is a partner in the firm's Litigation Department. Corporations and their boards engage Seth to address the legal, technical, and strategic aspects of data privacy and cybersecurity risk, and to prepare for and respond to data breaches, hacking and other cyberattacks. Seth teaches a Cyber Crime Law class at Harvard Law School.

PRESS CONTACT:
Heather Merton
Senior Communications Manager
617.439.2166
hmerton@nutter.com

Nutter is a top-tier, Boston-based law firm that provides legal counsel to industry-leading companies, early stage entrepreneurs, institutions, foundations, and families, across the country and around the world. The firm's lawyers are known for their client-centric approach and extensive experience in business and finance, intellectual property, litigation, real estate and land use, labor and employment, tax, and trusts and estates. Co-founded in 1879 by Louis D. Brandeis, who later became a renowned justice of the U.S. Supreme Court, Nutter is dedicated to helping companies prosper in today's fast-paced business environment.