Jaeckle FLEISCHMANN & MUGEL, LLP

Securing Your Technology and Preventing Cyber Risks in the Workplace: *The "Top Ten" List*

Attorney Advertising

Jaeckle Fleischmann & Mugel, LLP was pleased to serve as one of the presenting companies at a Business Leadership Forum entitled: ***The Invisible War: Securing Your Technology & Preventing Cyber Risks.*** *Kevin Burke, a Partner in the firm's litigation practice group outlined the ten steps that companies can take to avoid data and information breaches in the course of their business operations.*

1. **Address Organizational Issues:** Know your organization. What do you do and how do you do it? What do you need to protect? What are the inherent organizational factors that increase your risk (e.g., remote offices, suppliers, or subcontractors with differences in culture, politics or language)?

2. **Pre-screen Potential Employees:** The information collected during this process will help hiring managers make informed decisions and mitigate the risk of hiring a "problem" employee.

3. **Form a Multidisciplinary Team** at your organization dedicated to protecting your information. Include human resources staff, security, IT and legal professionals. The team should create policies, drive training, and monitor problem employees.

4. **Establish Policies and Practices:** Policies should delineate appropriate use of intellectual property, clearly disclose the organization's right to monitor and audit employee activity on proprietary systems and describe the company grievance/whistle-blowing procedures. Policies should also outline what are considered "risk" behaviors when handling and providing company information.

5. **Implement technical solutions to protect company data:** Preempt IP theft by flagging high-risk insider behavior with security technology. Implement a data protection policy that monitors inappropriate use of IP and notifies employees of violations, which increases security awareness and deters insider theft. Alert managers, HR, and security staff when exiting or terminated employees access and download IP in unusual patterns.

Continued on page 2

Continued from page 1

Jaeckle Fleischmann & Mugel, LLP

Avant Building - Suite 900
200 Delaware Avenue
Buffalo, New York 14202-2107
T: 716.856.0600
www.jaeckle.com

6. **Conduct Training and Education:** Policies and practices that are not recognized, understood and adhered to are of limited effectiveness. For instance, most IP thieves have signed IP agreements. Organizations should have more direct discussions with employees about what data is and is not transferable upon their departure and the consequences for violating these contracts.

7. **Evaluate continuously:** Without effective monitoring and enforcement, compliance will lapse and insider risk will escalate.

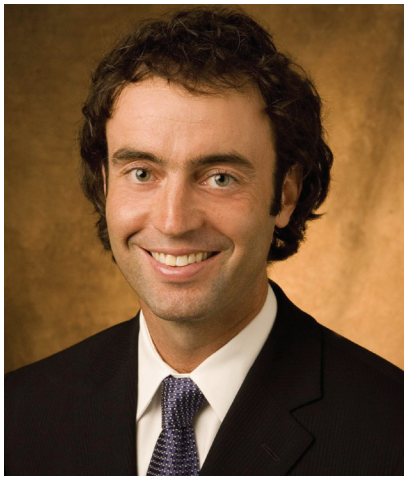
8. **Review Insurance Policies:** Your organization probably has a policy or policies for CGL, D&O, business interruption, and maybe even trade secret coverage. Many carriers now offer cyber liability policies. Review your coverage with an agent.

9. **Conduct Exit Interviews:** Interview employees on their way out the door to identify problems. Is he/she disgruntled, angry or jilted? Is he/she taking a new position with a direct competitor? Review any restrictive covenants and the handbook or policies covering confidential information. Most importantly: collect all hardware capable of storing information electronically, or at a minimum audit contents before releasing hardware to the departing employee.

10. **Act Immediately:** In the event of a suspected breach - ACT. Contact security professionals and involve skilled counsel as soon as possible to ensure compliance with all state and federal regulations and otherwise minimize your organization's exposure.

Costs & Effects of Security Breach

- ✓ Employee downtime
- ✓ Decreased morale
- ✓ Legal fees and costs
- ✓ Forensic Experts fees and costs
- ✓ Company Leaders are forced to manage litigation vs. the business
- ✓ Potential direct lawsuits by third-parties
- ✓ Loss of customer goodwill
- ✓ Possible criminal repercussions



For more information regarding best practices for reducing the risks associated with data and information breaches in the workplace, please contact Kevin Burke at 716.843.3854 or kburke@jaeckle.com.

The Business Leadership Forum brings together company leaders to discuss critical challenges and topics of interest. Visit the forum website at ***businessleadershipforum.com*** *for additional resources recommended by a panel of experts on technology and data security.*