ROETZEL
FOCUSED ON WHAT MATTERS TO YOU

CORPORATE COMPLIANCE ALERT

3/5/15

Cyber Preparedness: Corporate Boards and Officers Need to Manage the Risk of Cyber Attacks

In the now infamous hack of Sony's computer systems in the fall of 2014, investigators estimated that nearly 100 terabytes of data were stolen. Sony joined a crowd of other well-known cyber attack victims like JPMorgan Chase and Home Depot, both of which suffered large-scale assaults on their information systems in the past year. The steady increase in cyber attacks on U.S. businesses has drawn the attention of a number of regulatory agencies, including the Securities and Exchange Commission, Federal Trade Commission and The Financial Industry Regulatory Authority. These agencies, in the words of Securities and Exchange Commission Commissioner Luis Aguilar, are making it "abundantly clear" that boards and company management must work harder to prepare for cyber attacks and have plans in place to deal with attacks that do occur, or face exposure to both legal and regulatory sanctions.

All companies, and in particular their boards and officers, must assess their level of cyber attack preparedness with the same level of scrutiny with which they assess their readiness for other potentially critical risks to their company's data, infrastructure, finances, corporate reputation and shareholder confidence. To this end, boards of directors must educate themselves on the potential cyber threats to their business and their potential impacts. Conscientious and comprehensive oversight at the board level is essential in cyber risk preparedness and would necessarily include, among other safeguards:

- An assessment of the type of controls in place over company information systems
- Evaluation of those controls through testing, up to, and possibly including, a simulated attack
- Implementation of a plan for employee training in cyber security
- A formalized reporting process for suspected breach
- A thorough response plan in the event of breach

Cyber security, like other corporate compliance areas, is best served when board, officers and employees are fully engaged in a "culture of compliance" and proactive assessment of risk. Please contact any of Roetzel's Corporate Compliance team for further information on the implementation or assessment of a cyber security plan.

Brian E. Dickerson
Practice Group Manager
White Collar Litigation & Corporate Compliance
202.570.0248 | bdickerson@ralaw.com

Anthony J. Calamunci
419.254.5247 | acalamunci@ralaw.com

James L. Ervin, Jr.
614.723.2081 | jervin@ralaw.com

Amanda M. Knapp
216.615.7416 | aknapp@ralaw.com

Thomas M. Larned
202.697.4892 | tlarned@ralaw.com

Nicole Hughes Waid
202.906.9572 | nwaid@ralaw.com