DAVIS MALM & D'AGOSTINE P.C.

ATTORNEYS AT LAW

REGULATORY LAW ALERT
JANUARY 2018

IT'S A NEW YEAR: TIME FOR A DATA SECURITY CHECKUP

The start of a new year is a great time to check your company's overall cybersecurity and privacy health and fix any problems early in the budget cycle. Below are some key questions to ask your information technology, human relations, and legal personnel to ensure your company's data security and privacy policies will keep you safe throughout 2018.

1. Does your company have a written information security plan (WISP) that includes all of the following:
   - an identified manager responsible for maintaining the WISP;
   - training in WISP requirements for new and temporary employees;
   - protections limiting the access of terminated employees to sensitive personal information (PI);
   - review of third party vendor access to sensitive PI and confirming applicable security requirements in vendor contracts;
   - robust employee authentication and access controls to PI located on company networks;
   - encryption of PI on laptops and transmitted via email; and
   - annual review of WISP provisions (and more frequently following a breach or major change in the company's business)?

   The detailed Massachusetts data security rules in 201 CMR 17.00 are the most rigorous in the United States and have been in place since 2010 for all businesses with Massachusetts employees, and virtually all businesses with Massachusetts customers. If these requirements are not already in place, commissioning a new or expanded WISP should be a priority in 2018.
2. If your company has a WISP, have you reviewed and updated it over the past 1-2 years? As noted above, Massachusetts law requires businesses to review their WISPs not less than annually, with particular attention to companies with materially changing businesses or which have experienced a breach. If your company has not performed a review, including an updated risk assessment, you should do so on a priority basis. Security threats are proliferating rapidly, as are best practices for avoiding or minimizing them. WISPs should be evolving documents that address the changing security environment, rather than being placed in a drawer and forgotten.

3. Have you developed written contingency plans for addressing a security breach or emergency conditions at your workplace? At the same time you work on your WISP, you should also give thought to preparing an incident response plan and an emergency response plan. These plans will protect you in the event of a security breach, natural disaster, act of terrorism, or extended computer system disruptions, and will enable your company to continue to operate effectively in difficult circumstances. If you do not have these contingency plans in place already, it is wise to do so as early as possible.

CONTACT

If you have questions, please contact Robert J. Munnelly, Jr., in our Regulatory and Administrative Law Practice.

One Boston Place, Boston, Massachusetts 02108 | phone 617.367.2500 | fax 617.523.6215 | info@davismalm.com.