THE DANGER OF A WISP

For businesses that maintain data on customers or, increasingly, their own employees, the term "WISP" should be familiar. A WISP, or Written Information Security Program, is the document by which an entity spells out the administrative, technical and physical safeguards by which it protects the privacy of the personally identifiable information it stores. Health care entities subject to HIPAA have long-since become accustomed to not merely developing their own WISPs, but requiring the same of any business associate with which they share patient information. Similarly, banking, insurance and financial institutions have for years developed WISPs in response to their industries' privacy requirements.

Increasingly, however, state laws are expanding privacy requirements beyond the worlds of health care and finance to require the safeguarding of personal information about any resident of the state. (See e.g., the Rhode Island Identity Theft Protection Law or the Illinois Personal Information Protection Act.) By covering all residents of the state, this latest generation of privacy laws typically applies to a business' employees. Effectively, this means that every business in that state that maintains information on its employees must have a WISP in place to protect that information.

Businesses that have not implemented a WISP are playing a risky game. Security incidents happen every day. Furthermore, they don't only happen to the careless: in hacker culture, the harder the target, the greater the challenge and potential notoriety. For the business whose security is breached, when regulators or prosecutors come knocking, the worst possible posture is to not have a WISP in place. The second-worst posture, however, is to have a really nice WISP tucked in a drawer somewhere, with no indication it was ever implemented. The danger of a WISP is in thinking that it is enough on its own.

A "paper program" is always better than no security program at all, but a business seeking to protect itself – both from a potential security breach and from the severity of sanctions and publicity that can accompany such a breach – should be able to demonstrate that it has actively undertaken the key elements of a well-written and tailored WISP. One of the key elements of an effective WISP, one that every business of every size would be expected to undertake, is a security risk assessment. If the business has not endeavored to assess its risk areas and identify means to mitigate those risks, it can expect to be shown no quarter by any regulator, prosecutor, or journalist. For businesses above the mom-and-pop level, that risk assessment should be conducted by a qualified and certified third-party. The same holds true for auditing and monitoring. For even the largest of businesses with the most sophisticated IT departments, an internally-conducted audit will never have the credibility of an objective third-party audit.

The value of having risk assessments and regular audits performed by a third party cannot be overstated. First, the wider exposure of third-party auditors makes them more adept at identifying vulnerabilities. Also, for those wondering whether it's better to forgo a risk assessment so they can say "but we didn't know" if something goes wrong, the law defines knowledge to include willful disregard. Those hoping to find safe harbor in blissful ignorance will be sorely disappointed. If you could have known, you should have known; and if you should have known, you knew.

Moreover, the willingness to use a third-party for risk assessment and audit establishes a mind-set that leads to a more effective security program in practical application. A business that hires a law firm to write its WISP and oversee a risk assessment and audit program done by a skilled IT compliance firm does more than establish an effective security structure: the signaling function of that top-level commitment establishes a "culture of compliance" throughout the organization. A culture of compliance minimizes the primary source of vulnerability for any business: lax security practices by its own employees. Lastly, if your business is ever hit by a hack or other unfortunate breach, the use of a certified third-party transmits your utmost commitment to compliance to the regulators, prosecutors and journalists who may hold the financial and reputational well-being of your business in their hands. If you would like to learn more about information privacy protection regulations and best practices or need help with your organization's WISP, please contact PLDO Attorney Joel K. Goloskie at 401-824-5100 or email jgoloskie@pldolaw.com.

Joel K. Goloskie

Senior Counsel

Joel K. Goloskie is Senior Counsel with Pannone Lopes Devereaux & O'Gara LLC and a member of the Health Care, Litigation, and Corporate & Business Teams. His experience ranges from compliance and HIPAA privacy matters to regulatory filings and approvals, contract drafting and management, and mergers and acquisitions. He has assisted health care clients as they dealt with compliance orders and deferred prosecution agreements, and has represented clients in both civil and criminal matters in federal court.

PANNONE LOPES DEVEREAUX & O'GARA LLC

counselors at law

Pannone Lopes Devereaux & O'Gara LLC is a full service law firm that provides legal services in multiple practice areas including administrative law, business and corporate law, health care law, municipal law, nonprofit law, employment law, estate planning, probate and trust litigation, criminal defense, civil litigation, government relations and strategies, real estate development and commercial lending and special masterships. Our attorneys are cross-trained in several disciplines and work in collaborative teams to quickly identify the core issues in any legal matter and prescribe the right strategy from concept through resolution in the most responsive and cost-effective manner. For more information about our firm and our attorneys, please visit www.pldolaw.com or contact our firm.