What's in Your WISP?

By Joe Lazzarotti, CIPP

During the past year, large-scale data breaches have once again captured the public's attention. However, data breaches and legal obligations to safeguard data do not affect only the Fortune 500. In fact, small and mid-sized businesses may be more likely targets for a data breach than larger organizations, even if their breaches do not make national headlines.

> "*But for every high-profile case, there are dozens of threats to confidential data held by everyday enterprises*."

E. Scott Reckard and Tiffany Hsu, *Small businesses at high risk for data breach*, Los Angeles Times, July 4, 2014.

It is not hard to see why - these companies often have significant amounts of personal data, adopt similar technologies and practices (BYOD/devices, cloud, remote workers, reliance on vendors, etc.) but employ less sophisticated safeguards and have fewer resources to react to an attack. Browsing a well-known list of *reported* breaches tracked since 2005 by Privacy Rights Clearinghouse - one can see that many of the organizations are *not* household names. A small, solo health practitioner easily can maintain sensitive personal information on thousands of individuals. A neighborhood restaurant can process credit card data for hundreds of customers a week. Insurance brokers, accounting and law firms also maintain large amounts of client data.

Whether the personal information pertains to customers, patients, investors, or students, a business likely has specific regulatory or other obligation to safeguard that information. And, of course, all businesses maintain employee personal information – that too requires protection. So, what is a small business to do?

The "WISP" – Written Information Security Program.

What is a WISP?

Many of the challenges to safeguarding sensitive personal and other critical information can be addressed by developing and implementing a comprehensive "written information security program" (WISP). In short, a WISP goes well-beyond the one

paragraph handbook policy on privacy; a WISP is a written set of integrated policies and procedures that establishes administrative, physical, technical and organizational safeguards that apply across an organization. Maintaining one will better position a company to protect its business, defend claims and governmental inquiries related to a data breach and compliance, avoid whistleblower claims from employees who claim the company is not doing enough to safeguard data, and can even provide a competitive advantage in some cases. WISPs can and should be designed to better manage and safeguard critical company information (e.g., proprietary information and trade secrets), even if the large-scale data breaches in the news tend to involve individuals' personal information.

Often driven by IT departments, WISPs are most effective when developed through the collaboration and institutional knowledge of key persons across the enterprise. Importantly, WISPs should not be treated as static policies. WISPs need to change and adapt with the business and its information risks. So, for example, acquiring a new business may present new and different risks that were not anticipated during the original assessment, and which can create a security gap in an otherwise comprehensive WISP.

Is a WISP required?

As explained below, federal and state laws have requirements for businesses and other entities to maintain a WISP. In some cases, more than one of these laws can apply to a business generally or to certain segments of its data. Industry standards also have developed that mandate safeguards be developments in the nature of a WISP. The best example of this is the Payment Card Industry (PCI) standards that apply to card processors.

Increasingly, however, businesses are finding that their customers or clients – whether individuals or other businesses – are demanding that the businesses they work with have WISPs to safeguard the personal and other data they entrust to the businesses. As a result, greater attention is being given to data privacy and security provisions of master services agreements, and the corresponding indemnity requirements. Finally, many businesses impose a WISP requirement on themselves when they communicate to their customers, such as in a website privacy statement, that they protect and safeguard their customers' personal information. Failing to do so, may expose the company to claims of engaging in unfair or deceptive trade practices by the Federal Trade Commission or a state Attorney General.

In general, federal law has imposed data security obligations on certain industries. For example, health care providers and business associates have to comply with the privacy and security regulations under HIPAA. Many educational institutions are subject to the Federal Educational Rights and Privacy Act (FERPA). And, the Gramm-Leach-Bliley Act created wide-ranging notification and data protection requirements for

insurance companies and financial institutions. For businesses covered by these and similar laws, some form of a WISP is required by law.

In addition, many states have enacted laws intent on safeguarding personal information. Examples of these kinds of laws include: obligations to create reasonable safeguards, breach notification requirements, data destruction mandates, and requirements to have a written contract with a vendor to safeguard the personal data shared with that vendor. Generally, these statutes are similar state to state, with remedies for violations ranging from enforcement actions by state attorneys general to private actions by affected individuals seeking damages, in some cases including treble or punitive damages.

The state best known for mandating a WISP by law is perhaps Massachusetts. In 2010, Massachusetts regulations (201 CMR 17.00) became effective requiring companies that "own or license" personal information about Massachusetts residents to develop a WISP. According to the regulations, "own or license" refers to circumstances where a company *receives, stores, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment*. Notably, a business that maintains personal information on a Massachusetts resident arguably must comply with those data security regulations, even if the business does not have a location or do business in the Bay state. The WISP regulations in Massachusetts include a number of specific safeguards, such as a requirement to encrypt mobile devices that maintain personal information. For more information about these safeguards, you can access a checklist we prepared for this purpose.

A number of other states have similar requirements, but most without the same level of specificity as the rules in the Bay state. These include, without limitation, California, Connecticut, Delaware, Maryland, Nevada, Oregon, and Texas. Recently, Florida also added a requirement for businesses to safeguard personal information, effective July 1, 2014. In September 2014, a bill was introduced in New York, A.10190 (Dinowitz) that would amend New York's data breach notification law to include a WISP requirement very similar to the law in Massachusetts.

What should a WISP look like?

WISPs can take many forms, although they generally will include, as noted above, administrative, physical, technical and organizational safeguards that apply across an organization. WISPs mandated by law will need to apply those safeguards to personal information – Social Security numbers, financial account numbers, etc. However, the safeguards are often extended to apply to important business and client data either because of client demands, ethical mandates or perceived value.

Without limitation, below are examples of the kinds of policies one would expect to find in a WISP:

- Risk assessment and re-evaluation
- Data classification
- Access management
- Information systems usage requirements, including device management
- Electronic communications guidelines
- Emergency/disaster recovery
- Data breach response protocol
- Vendor management procedures
- Record retention and destruction

The process for developing a WISP generally involves four steps – risk assessment, policy development, implementation/training, re-evaluation. Key to this process, however, is executive-level support and appropriate coordination of all departments within the organization. Only after understanding all of the organization's data privacy and security risks, and developing and implementing a coordinated and reasonable plan to address present and future risks can the organization have a compliant WISP best able to address those risks.

* * *

Clearly, information is akin to "plant and equipment," a critical business asset that drives revenues and future growth, and that warrants appropriate safeguards. As organizations strive to harness the business potential of the digital age, information risk is on the rise. Business owners, executives and their counsel are prudent to recognize the potential exposures as well as how to protect against them. Having a WISP is a necessary component of those efforts.

About ADP

ADP has developed and enacted a global set of security policies and procedures for our locations, associates, and vendors, all which form part of ADP's comprehensive WISP. See more regarding our policies at ADP's Trust Center: About Jackson Lewis.

Jackson Lewis PC, a national law firm, offers a team of dedicated privacy attorneys that counsels companies of all sizes through the key steps for safeguarding personal information, including risk assessment, policy drafting, training, vendor agreement negotiation and data breach response, and whether the information relates to customers, employees, patients, students, or other individuals.