OK, I Get It, Data Security is Important for My Small Business … So What Do I Do?

During the past year, large-scale data breaches once again captured the public's attention. But 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 they don't make national headlines.

Your business could be at risk

Small- and mid-sized companies often have significant amounts of personal data and adopt similar technologies and practices (BYOD/devices, cloud, remote workers, reliance on vendors, etc.) as larger companies.

At the same time, they generally employ less sophisticated safeguards and have fewer resources to react to an attack. For example:

- A small, solo health practitioner can easily maintain sensitive personal information on thousands of individuals.
- A neighborhood restaurant can process credit card data for hundreds of customers a week.
- Insurance brokers and accounting and law firms 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. So, what's a small business to do?

Consider a written information security program

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, or WISP. A WISP is set of integrated policies and procedures that establishes administrative, physical, and technical safeguards that apply across an organization. Maintaining a WISP can 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 even provide a competitive advantage in some cases.

Often driven by IT departments, WISPs are most effective when developed through the collaboration and institutional knowledge of key persons across an organization.

WISP: A set of integrated policies and procedures that establishes administrative, physical, and technical and safeguards that apply across an organization.

Importantly, WISPs should not be treated as static policies. Rather, they need to change and adapt with the business and its information risks.

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 certain safeguards in a WISP. The best example of this is the Payment Card Industry (PCI) standards that apply to card processors.

Increasingly, customers or clients are demanding that the businesses they work with have WISPs to safeguard the data they entrust to the organization. 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 proclaims they protect and safeguard their customers' personal information. Failing to do so may expose the company to Federal Trade Commission, or a state attorney general's claims of engaging in unfair or deceptive trade practices.

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 to safeguard personal information. Examples include obligations to create reasonable safeguards, breach notification requirements, data destruction mandates, and written contracts to safeguard the personal data shared with a 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.

Types of Policies Often Found 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**

What should your WISP look like?

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

A Step-by-Step process to create a WISP

The process for developing a WISP generally involves four steps: risk assessment, policy development, implementation/training, and 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 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.

ADP® has developed and enacted a global set of security policies and procedures for our locations, associates, and vendors, all of which form part of ADP's comprehensive WISP. See more regarding our policies at ADP's Trust Center (**adp.com/adptrustcenter**).