SAFETY AND SECURITY

Cybersection

Third-Party Risk Management

Data breaches like those involving Target and Equifax underscore the critically important nature of third-party vendor management to any company's overall risk profile and reputation – not to mention bottom line.

Data Protection:

It is critical that your vendors properly secure any confidential information they collect and store on your behalf and ensure that they comply with the latest cybersecurity protocols and frameworks. A review and understanding of your vendor's information technology and data protection policies and procedures should be a part of any vender management program. In addition, in the event of a data breach by your vendor, you need to understand before such an occurrence what laws and regulations apply and who is responsible to act. This is particularly important when your vendor or business is in multiple jurisdictions which may have different requirements.

For cybersecurity resources, be sure to check out our cybersecurity resources online: **www.dobs.pa.gov/Businesses/cybersecurity**

Marketing and Advertising Laws

A review of you and your vendor's communication and marketing protocols – when others reach out on your behalf or refer leads to you – should also be a part of your vendor management procedures. As marketing to your customers has become more complex and consumers are targeted using ever-increasing personal information, it is important to make sure your vendors – especially those who perform marketing, referral, and communications duties -- are complying with the applicable federal and state rules and requirements, including do not call and solicitation laws such as the:

- TCPA – or the **Telephone Consumer Protection Act of 1991**. Among other things, this limits the use of automatic dialing systems, limits solicitation hours, and requires compliance with the **National Do Not Call Registry**.
- **Pennsylvania Do Not Call List** – Since 2002, Pennsylvanians could opt-out of many solicitations. Any vendor you use to communicate on your behalf should be familiar with not only the national requirements, but state requirements as well.

Cyber Insurance: Right for Your Company?

Cyber attacks are increasing in volume and sophistication, but traditional general liability insurance policies may not provide effective coverage for all potential exposures caused by cyber events.

Cyber insurance could offset financial losses from a variety of exposures—including data breaches resulting in the loss of confidential information—that may not be covered by more traditional insurance policies. You should assess the scope of coverage of current insurance and consider how cyber insurance may fit into your company's overall risk management framework.

As with any insurance coverage, cyber insurance does not diminish the importance of a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure.

You can find additional information on risk management and cybersecurity risk management from the Federal Financial Institutions Examination Council (FFIEC) at **www.ffiec.gov**.

A Well-Informed *Marketplace*

Investor Education & Consumer Protection

"We work to help consumers understand how they can navigate modern financial services to deposit, spend, borrow, send, and invest money with confidence."

– Robin L. Wiessmann, Secretary of Banking and Securities