jackson lewis

Employee Privacy and Data Security Training

A Legal Requirement and Prudent Business Practice

By Joseph J. Lazzarotti, Esq., CIPP

Jackson Lewis PC

Many executives may be surprised to learn that one of the most frequent causes of data breaches is employee error, and not just employees in the IT department. The types of information involved in breaches go beyond payment cards, Social Security numbers and patient medical information, and can include valuable proprietary or trade secret information; privileged or financial data belonging to employees, clients and customers; and sensitive internal email communications. Every day mishaps like failing to lock a door, using the wrong email address, forgetting a device on a plane, forwarding the wrong attachment, or not knowing who is authorized to access data can have catastrophic consequences for a business.

It is true that a number of safeguards can be employed to minimize instances of these and other kinds of employee error. However, training is critical. For one, training may be required by law to protect certain information. But even if not expressly required by a statute, it is likely data security training would be considered a reasonable safeguard for businesses required to protect certain data. Additionally, businesses in various industries increasingly are being required by contract, including government contracts, to conduct training to protect information entrusted to them. Finally, with vast amounts of data so easily at our fingertips, it is simply a prudent business practice to train employees about the company's policies and best practices concerning information confidentiality, privacy and security.

Is employee error really a problem?

Yes. Looking back at our own experience as a practice group, having handled hundreds of data incidents and breaches, employee error is easily the most frequent cause. A number of reports and surveys suggest similar findings, namely that employee error is a key reason why companies are experiencing damaging losses of data.

Late last year, the Wall Street Journal reported on a survey by the Association for Corporate Counsel that found "employee error" is the most common reason for a data breach. CSOOnline reported on Experian's 2015 Second Annual Data Breach Industry Forecast, stating, "employees and negligence are the leading cause of security incidents but remain the least reported issue." According to Kroll, in 31% of the data breach cases it reviewed in 2014, the cause of the breach was due to simple, non-malicious mistake. These incidents were not limited to electronic data – about one in four involved paper or other non-electronic data.

When people think about data breaches, they tend think more about the illegal hacking into computer networks by individuals, criminal enterprises or even nation states, than they do about simple employee error. This makes some sense as hacking incidents seem more likely to draw intense media focus and capture the public's attention. Unfortunately, having this impression about the causes of data breaches leads many to conclude that because they believe their

organization is less likely to be the target of a hack, the organization is less likely to have a data breach. Too often, these individuals miss altogether the potential for employee error and as a result significantly underestimate the risk of a data breach. An example of employee error mentioned in the ACC survey – "accidently sending an email with sensitive information to someone outside the company" – is something most business either have heard about or experienced in their own organizations.

Even if that is true, do we have a legal requirement to train employees?

For many businesses, the answer is yes, but it will depend on the kind of business, where it is located and the type of data the business maintains. Here are some examples:

- ***Healthcare providers, health plans and business associates***. Certain health care providers and health plans, and their business associates are subject to the privacy and security regulations under the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA privacy regulations require that

  > ***"covered entities must train all members of its workforce…as necessary and appropriate for the members of the workforce to carry out their functions." HIPAA Privacy Rule § 164.530(b).***

  The HIPAA security regulations require covered entities to

  > ***"[i]mplement a security awareness and training program for all members of its workforce [including management]. Security Rule § 164.308(a)(5).***

  So, all covered healthcare providers – such as hospitals, physician practices, dental offices, nursing homes, and home healthcare providers – have a regulatory requirement to train their workforce members. These requirements also apply to business associates of these covered entities – including accounting firms, consultants, law firms, and medical billing companies.

  The training requirement also extends to certain employer-sponsored group health plans. Many employers sponsor some form of a self-funded health plan, such as a self-funded plan that meets the minimum value requirements for purposes of the Affordable Care Act, or a health flexible spending arrangement. For employees that handle protected health information in the course of administering these plans, training is required.

- ***Financial Institutions*****.** As one of the most heavily regulated industries in the United States and globally, financial services organizations are subject to a wide range of data privacy and security requirements given the critical nature of the data they use, receive, maintain and disclose. These requirements include employee training:

  Safeguards Rule. Under the Gramm-Leach-Bliley Act ("GLBA") and pursuant to regulations issued by the Federal Trade Commission ("FTC"), certain financial institutions are required to develop administrative, technical, and physical safeguards to

protect customer information (known as the “Safeguards Rule). For this purpose, financial institutions generally include organizations such as lenders, financial advisors, loan brokers and servicers, collection agencies, tax preparers, and real estate settlement services that have customer information, whether collected from their own customers, or received from other financial institutions.

Section 314.4 of the Safeguards Rule requires financial institutions to assess and address the risks to customer information in all areas of their operations, *including employee management and training*. FTC guidance for compliance with the Safeguards Rule lists a number of steps financial institutions should take, including **“[t]raining employees to take basic steps to maintain the security, confidentiality, and integrity of customer information.”**

Red Flags Rule. The Fair and Accurate Credit Transactions Act (“FACT Act”) requires certain federal agencies to direct financial institutions and creditors to do more to detect, prevent, and mitigate identity theft. These rules apply to a broad list of businesses - "financial institutions" and "creditors" with "covered accounts". For example, a "creditor" is defined non-exhaustively to include "lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies and telecommunications companies". And, covered accounts include any account for which there is a foreseeable risk of identity theft.

The set of rules that followed became known as the “Red Flags” rule, which requires these covered entities to adopt programs designed to detect, prevent, and mitigate identity theft. To administer the program in compliance with the regulation, the organization must “**[t]rain staff, as necessary, to effectively implement the Program**.” See, e.g., 16 CFR § 681.2(e)(3).

FDIC Guidelines. The Federal Deposit Insurance Corporation (FDIC) applies the Interagency Guidelines Establishing Information Security Standards (Guidelines) that provide standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The Guidelines apply to depository institutions insured by the FDIC, such as banks, state savings associations, insured state branches of foreign banks, and any subsidiaries of such entities (other than brokers, dealers, persons providing insurance, investment companies, and investment advisers). Under these Guidelines, each institution shall, **“[t]rain staff to implement the bank's information security program.”**

Regulation S-P. GLBA also directed the Securities and Exchange Commission to establish appropriate standards to protect customer information. These rules, known as Regulation S-P, apply to investment advisers registered with the Commission, brokers, dealers, and investment companies subject to the Commission's jurisdiction. Under these rules, these entities “must adopt policies and procedures that address

administrative, technical, and physical safeguards for the protection of customer records and information...reasonably designed to:

> (a) Insure the security and confidentiality of customer records and information;
>
> (b) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
>
> (c) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

In Notice 05-49, the National Association of Securities Dealers ("NASD") (now known as the Financial Industry Regulatory Authority, or FINRA) reminded its members about the need to comply with Regulation S-P. It stated in part that although there is no "one-size-fits-all" policy or procedure to comply, members' policies and procedures should "at a minimum" include: "***providing adequate training to employees regarding the use of available technology and the steps employees should take to ensure that customer records and information are kept confidential***."

- ***Federal Contractors*****.** Under the Federal Information Security Management Act (FISMA) certain federal agencies are required to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, *including those provided or managed by another agency, contractor, or other source*. Specifically, under 44 U.S.C. § 3544(b)(4):

  > *Each agency shall develop, document, and implement an agency-wide information security program…to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes…**security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency**.*

- ***State Law Mandates*****.** Although there is not yet a universally applicable federal data security statute in the United States, a number of states have required business and other entities operating in the state or maintaining personal information about state residents to have safeguards in place to protect that information. In some cases, training is an express requirement, in others states it is expected as a "reasonable safeguard."

  Massachusetts. Under comprehensive data security regulations that apply to businesses that maintained personal information of Massachusetts residents, the business must maintain a written information security program (WISP). **A WISP must include ongoing employee (including temporary and contract employee).** Data Security Reg. 201 CMR § 17.03(2)(b).

Oregon. Oregon also requires certain businesses to maintain a WISP. The WISP must include administrative safeguards under which the business: **"[t]rains and manages employees in the security program practices and procedures."** ORS § 646A.622(d)(A)(iv).

Texas. In Texas, certain entities that engage in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information are subject to a set of HIPAA-like rules to protect that protected health information. Under that law, "***[e]ach covered entity shall provide training to employees…necessary and appropriate for the employees to carry out the employees' duties for the covered entity***." Texas Health and Safety Code § 181.101.

General Safeguard Requirements. A number of other states impose more general requirements on businesses to safeguard the personal information they maintain. In general, those states require businesses to maintain "reasonable safeguards" to protect personal information of state residents. These states include, without limitation, California, Connecticut, Florida, and Maryland.

- ***Payment Card Industry Data Security Standards (PCI DSS).*** Businesses that accept credit or debit cards as payment for goods and services will have certain obligations under PCI DSS standards. The major card brands (e.g., Visa, MasterCard, American Express, Discover) maintain the standards, which are administered by the Payment Card Industry Security Standards Council. In October 2014, the Council published "Best Practices for Implementing a Security Awareness Program Concerning PCI DSS Requirement 12.6" which states:

> ***[A] formal security awareness program must be in place****…Security awareness should be conducted as an on-going program to ensure that training and knowledge is not just delivered as an annual activity, rather it is used to maintain a high level of security awareness on a daily basis.*

Good to know, but our company does not maintain that much personal information, only employee data and that is locked down in HR.

There are least two things wrong with this statement.

First, personal information is not the only information that a business might want to protect. Many companies maintain proprietary and confidential business information that if shared outside the organization (or with the wrong people inside the organization) could cause it substantial harm. A company's business partners and customers might obligate it to maintain safeguards to protect the information the business partner or customer shares with the company. Training might be expected to be included in these safeguards, and it may even be expressly stated in the services agreement.

Second, certain employee information is personal information any may be subject to some of the requirements outlined above. For example, the Massachusetts data security regulations apply to customer *and* employee personal information. With the growing number of data breaches affecting employees and increasing concerns about privacy, federal and state

agencies regulating employment practices seem to be moving in a direction of requiring greater security over employee data, which includes training. Consider the following statement from recent EEOC proposed regulations under the Americans with Disabilities Act concerning wellness programs:

> *Employers and wellness program providers must take steps to protect the confidentiality of employee medical information provided as part of an employee health program. Some of the following steps may be required by law; others may be best practices.* ***Proper training of individuals who handle medical information in the requirements of the HIPAA Rules, the ADA, and any other applicable privacy laws is critical****.*

What should a privacy and data security training program look like?

There is a myriad of ways to design a training program to create awareness and build a culture of privacy and security in an organization. But, there are some key issues organizations should consider when setting out to design such a program. Some of these include:

- ***Who should design and implement the program?*** If the organization has a privacy officer, this might be a good choice, but certainly not the only one. However, there should be an individual or department responsible to maintaining the program.

- ***Who should be trained?*** In general, this should include workforce members with access to the information the organization desires to safeguard. However, even unauthorized employees may get access to that information, inadvertently perhaps, and may need to be made aware of certain company protocols, such as how to report a data breach.

- ***Who should conduct the training?*** Organizations may do training in-house, outsource it, or a combination of both. When performed in-house, the person to deliver the training might depend on the information or safeguards being covered. For example, if the safeguards at issue relate to information obtained by call center representatives, the call center manager might be a good choice to deliver the training. It is not necessary, however, that a member of the IT, HR or Legal departments deliver the training, or that it be a person with technical IT knowledge. But, the ability to convey specific information about company requirements, legal mandates and use of technology to maximize security is certainly helpful.

- ***What should the training cover?*** Again, the substance of the training will depend on the organization, the data at issue, the audience and other factors. In general, training should cover some basic issues, such as what is confidential or personal information, or what is a data breach. However, training programs can be significantly enhanced when they use real situations that participants in the program can relate to and apply in their jobs.

- ***When and How Often?*** Basic privacy and security training should be provided before an individual obtains access to confidential or personal information. At a minimum, the principles should be conveyed at least annually thereafter. Training also may be needed after changes in policies; following increases in levels of access or sensitivity of information; to react to changes in technology; following a security incident and other situations.

- ***How should training be delivered?*** There are many ways to deliver a consistent message about data security throughout an organization. These include policies, notices, newsletters, intranet dashboard, in-person sessions, online courses, videos, testing, tabletop exercises, employee resource group (ERGs), or a combination of these. We worked with First Watch Data Breach Solutions to develop a 9-segment video training series made up of 3-4 minute sessions that cover some very basic information about privacy and data security that all employees should know.

- ***Should training be documented?*** Yes. In some cases, such as under HIPAA, documentation is required. However, an organization will be in a much better position to defend its data privacy and security practices if it can show that it maintains a comprehensive training program. This generally means that the organization tracks the materials covered in the training and those who attended or received the information.

We did training and employees still send the emails to wrong addresses and make other mistakes!

No system of safeguards is perfect, and that includes privacy and data security safeguards. As one component of a set of such safeguards, training will not achieve perfection in any organization. The effort is more about awareness, risk management, litigation avoidance and mitigating exposure.

ATTORNEY ADVERTISING

For additional information, please contact:

Joe Lazzarotti, Esq., CIPP
Principal | Morristown, NJ Office
973-451-6363 | lazzarottij@jacksonlewis.com

4828-4121-0669, v. 1