Basic Data Privacy / Security "Good Practices"

A complete checklist for improving data privacy and security practices would vary from industry to industry and from state to state, but certain data privacy and security good practices apply to all organizations. For example, covered entities and business associates in the healthcare industry must comply with HIPAA and related Privacy and Security Rules. Outside healthcare, organizations often have other federal or state laws with which to comply. The good practices outlined below were selected because they can often be implemented without a large budget but provide significant benefits.[1]

1. **Assign ultimate data privacy and security responsibility to one person.**

   As with any other project of significance in your organization, there needs to be someone with ultimate responsibility. This person needs to have sufficient authority to get things done.

2. **Beef up your contracts with vendors and business associates.**

   A significant percentage of all data breaches are caused by third-party vendors and business associates.

   a. Make sure that your contracts with service providers and others with whom you share confidential, personal information require those companies to protect confidential, personal information with reasonable security measures or more stringent measures as required by law.
   b. Healthcare organizations should require their associates to comply with HIPAA's Security Rule.
   c. Require your third-party vendors and others with whom you share confidential, personal information agree to defend and indemnify you for data privacy/security incidents that relate to or arise out of the work performed by such third-party vendors.
   d. Consider insisting that your vendors purchase data privacy and security insurance so that they have the money to indemnify you if the vendor or service provider is involved in a data security incident.

3. **Implement a continuous workforce training and awareness program.**

   Organizations should implement an ongoing training and awareness program. Some training and awareness materials can be general in nature and still make a difference in your organization. It is important, however, to include training related to the specific information

[1] Of course, there is no assurance that implementing these good practices will prevent or lessen the severity of a data breach. Organizations are advised to engage legal counsel with significant experience in the data privacy / data security practice area to develop a comprehensive compliance plan that will also minimize the likelihood or severity of a data breach.

Updated 1/12/2012
© 2012 ePlace Solutions, Inc.

security risks and vulnerabilities in your organization. These risks and vulnerabilities will be identified in the course of the risk assessment described below.

4. **Prepare for data security incidents:**

    a. Identify the team of people (Incident Response Team, or IRT) that should be involved if you have a data security incident. Depending on the size of your organization, this team could be as few as one or two people, or as many as 12 or 13 people.
    b. Keep a list of the IRT members complete with contact information so others in your organization know who to call if they suspect there has been a data security incident
    c. Prepare an incident response plan

5. **Understand who/what/when/where & why, related to the confidential and/or personal information you collect and/or store.**

    Organizations manage data that they do not know exists. Meet with key players in your organization that touch confidential and/or personal information, including your HR director, your network administrator, IT director, and others. You want to identify the individuals who know about information such as Social Security Numbers, financial account numbers, usernames and passwords, health information, and any other information that could be used to identify individuals. This group of individuals should be able to provide a complete picture of: (1) **what** type of information is collected; (2) **why** such information is collected; (3) **when** the information is collected; (4) **where** the information is located or stored; and (5) **how** it is used, shared, and protected.

6. **Evaluate the security for each location where confidential, personal information is stored.**

    Write down each storage location. These may include areas within a building, file cabinets, smart phones, or office equipment like servers, copiers, and PCs. Next, discuss whether you collect information that you don't really need. If so, consider changing company procedures to eliminate collecting this information in the future. For information you do need, think through scenarios whereby an unauthorized individual may gain access to the information. Examples might include backup tapes that get forgotten in the backseat of the car, smart phones that get lost, servers that get hacked, or disgruntled employees who access customer information. Write down these risks and attack scenarios. Don’t forget to account for those catastrophic events that no one thinks will really happen, like floods, hurricanes, earthquakes, or fires (because these events really do happen).

7. **Consider the ways to avoid or mitigate the risks that you just identified.**

    Federal and state laws often refer to administrative, physical, and technical safeguards to protect confidential, personal information. Let's look at a few examples of each of these

© 2012 ePlace Solutions, Inc.

safeguards to get you thinking about how easy it might be to better protect the confidential, personal information that you collect and/or store.

Administrative safeguards could include: (1) limiting access to confidential, personal information relating to customers, employees or others so that the only employees who have access to this information are those who need to use this information to perform their job duties; (2) adopting a “clean desk policy” that requires employees to properly secure records containing confidential, personal information; (3) creating or updating a record retention policy that would help ensure that your organization does not keep records for longer than necessary; and (4) creating or updating policies and procedures in your organization to address privacy and security issues (e.g. acceptable use policies).

Physical safeguards could include: (1) storing paper records containing confidential, personal information in locked file cabinets; (2) shredding records that contain confidential, personal information; and (3) storing servers, laptops, and backup tapes in secure, locked areas.

Technical safeguards may include: (1) encrypting laptops, flash drives, and data stored on servers; (2) updating software regularly; and (3) installing and updating firewalls, antivirus and anti-spyware software.

8. **Review and update your existing data security policies, plans and procedures.**

If you have already developed your incident response plan and your organization's policies and procedures, review them every 6 months, and after every data security incident, to make sure that they still make sense. The same is true for your risk assessment and analysis of mitigation measures. This is not only a best practice but, under some laws and for certain industries, it's a legal requirement. Train your workforce on the content of your new or updated policies and procedures. Without adequate training, your policies and procedures may be useless or even hurt your organization. Training does not always require elaborate measures or expense. Training employees on your policies and procedures is often best performed by managers and supervisors.

© 2012 ePlace Solutions, Inc.