



RCW
Report Content Writer
www.reportcontentwriter.com.

AUTHOR: Rachel Agheyisi

EMAIL: rachel@reportcontentwriter.com.

TWITTER: www.twitter.com/rachel_rcw

7 Tips To Make Your Company's Information Security Plan More Manageable

If you operate a financial services business, which falls under the jurisdiction of the Federal Trade Commission (FTC), you may be subject to the FTC's Safeguard Rule (the Rule).

Compliance with the Rule requires you to have an information security plan that stipulates how your business protects the sensitive customer information you handle. The Rule defines sensitive customer information to include personal information such as social security number, ethnicity, and date of birth. It also includes financial information such as credit card number and bank account number.

For many businesses, writing a compliant information security plan is relatively easy. The challenge lies in implementing the policy and avoiding the consequences of non-compliance.

There are many approaches to handling data security compliance. The following are seven low-tech, simple tips to help make the task of implementing your information security plan more manageable:

1. **Don't be a data hog.** Clutter used to be a problem that people worried about at home. Unfortunately, domestic clutter has made its way past our pantries, garages, public storage facilities, and into our workspaces. Business clutter does not only occupy undue amounts of space; it complicates the task of tracking and protecting information. Eliminating clutter will help you organize to protect sensitive information.
2. **Collect only what you need.** Clearly, data collection and storage go together. Becoming purposeful in your request for customer's personal information will go a long way in streamlining your data storage needs. You will also have less information to protect. In short, if you have no business use for the personal information, don't collect it.
3. **Dispose of sensitive information properly.** Proper disposal means that the way you dispose of information must preserve the confidentiality and privacy of customers. The FTC's Disposal Rule requires companies to adopt disposal practices that prevent the unauthorized access to or use of information in credit reports. Simply dumping paperwork containing sensitive personal information is not an option. Shred, burn, or pulverize papers to keep them from prying eyes. If you plan to donate old computers, laptops, and other data storage devices, use

appropriate wipe utility programs to clean them out to prevent subsequent retrieval by unauthorized persons.

4. **Involve your employees.** This falls under the heading of creating a culture of security in your company. We see it on the television. A guy walks into the office, distracts the employee, logs on to the computer, and retrieves information without being caught. Hollywood might have simplified the sequence of events somewhat. However, it makes a good point. Creating the company's information security policy is the responsibility of management. Making security a part of everyday business requires full participation by employees.
5. **Limit access.** This means investing in state-of-the-art security software and programs that make sensitive data sites "hacker proof". It also means limiting access only to employees who need restricted data to perform assigned business duties. If your business stores sensitive information in drawers and filing cabinets, secure them with locks.
6. **Know your contractors.** These days, outsourcing is unavoidable in the course of doing business. However, each external source has potential implication for your information security plan. Before you outsource your web hosting, IT service, payroll, call center operations, and other business needs, verify the security practices of the vendors. If you engage the services of a contractor to shred your company's paperwork, ensure that they follow appropriate secure disposal procedures.
7. **Have a damage control plan.** Given the complexities of today's business environment, your company may not always be able to prevent information security breach. In the event of a breach, damage control becomes critical. For example, it is important to know your company's reporting obligation under the law. You may be required to notify customers, law enforcement agencies, credit bureaus, and other businesses affected by the breach. Having an action plan in place will facilitate your management of a security breach.

Protecting customers' personal information is a legal requirement. Information security makes good business sense. A company's privacy policy is a statement of commitment to its customers. Implementing best practices, such as the ones suggested in this article, will help your compliance with the law. It will also help in consolidating the trust between you and your customers.

About the author: Rachel Agheyisi is a business writer who specializes in white papers and case studies that address regulatory compliance and business intelligence issues. Related articles are available on her website at www.reportcontentwriter.com.