

CVS Pharmacy

A case in preventing information loss.



Case Study: CVS Pharmacy

In July 2006 and continuing into 2007, television stations and other media outlets reported finding personally identifiable information in unsecured dumpsters outside of CVS pharmacy locations. The dumpsters contained pill bottles, with patient names, addresses, etc.; payroll information; employment applications, including social security numbers; credit card and insurance information, including account numbers and driver's licenses. The information was found in dumpsters in at least 15 different cities throughout the US.

In February 2009, CVS settled with the FTC for \$2.2 million. As part of the settlement the FTC ordered that CVS implement, establish and maintain "a comprehensive information security program." In addition, CVS must obtain a security assessment from an independent 3rd party every two (2) years for the next twenty (20) years.

The FTC defines "a comprehensive information security program" as follows. CVS must designate a person to be accountable for the information security program. They

must identify material internal and external risks to the security, confidentiality and integrity of personal information. Moreover, they must design and implement reasonable safeguards to control these risks.

Analysis

Every organization has a responsibility to protect the sensitive information they have. This responsibility extends to everyone in the organization, not just the IT department. The risks to information security are not just digital but involve people, processes, and technology. While these risks may represent problems that are difficult to solve, doing nothing is not an option.

Ultimately, this may require a culture change within organizations to make security a priority. Culture change starts at the top, and management must ensure through words and actions that cyber security is not optional but is an organizational imperative and fiduciary responsibility.