

**RCW**

Report Content Writer
www.reportcontentwriter.com.

AUTHOR: Rachel Agheyisi

EMAIL: rachel@reportcontentwriter.com.

TWITTER: www.twitter.com/rachel_rcw.

Financial Information Security is a Three-Legged Stool

In September 2008, I received one of those notices you hear about, but think will never happen to you. It was a letter from my mortgage lender to let me know that *"an employee may have sold unauthorized personal information about you to a third party"*. In short, there had been a data breach at the company.

Cancelling my account was not a viable option. Therefore, I immediately signed up for credit monitoring with all three credit bureaus. I have become extra vigilant with all my bank and credit card accounts. Each month, I spend extra time reviewing each statement. It is not only troubling, it is inconvenient to be on high alert.

Unfortunately, my story is not unique. Millions of consumers have had their privacy compromised by the financial institutions who promised to safeguard their personal, sensitive information.

The divergence between the security some companies promise on paper and what happens in fact puts a dent in consumer confidence. When I opened my account, the mortgage lender provided me with privacy statements as required by federal and California laws. However, their information security policy was only good on paper. Like a one-legged stool, it did not hold up in reality.

Financial services businesses under the jurisdiction of the Federal Trade Commission are subject to the provisions of the FTC's Safeguard Rule. Under the Rule, each business is required to ensure an effective information security plan.

An information security plan stands a better chance of success if it incorporates these three key elements:

1. **Risk assessment:** The plan needs to identify and anticipate internal and external threats to the integrity of customer data. Information security requires proactive planning for real and potential vulnerabilities. Risk assessment is an effective tool for such strategic planning.
2. **Accurate Compliance Language:** The growing incidence of data breaches shows that some businesses are not honoring their stated compliance obligations. The document needs to reflect accurate compliance language. Information security plan is more likely to succeed if it is based on realistic expectations.

3. **Governance:** Obviously, governance is a function of the size of the company. There is hardly a shortage of hierarchy and titles in large enterprises. The point of compliance governance is who is in charge? Information security is more likely to succeed with effective governance involving accountability and coordination.

The problems of identity theft and fraud make information security a big deal for everyone. Data security builds customer confidence. It is good for business. It is the law. It needs a platform of success that incorporates risk management, compliance, and governance.

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.