FTC Guidelines for Small Business Cybersecurity

For Oklahoma Bankers Association – August issue

Rayleen M. Pirnie, AAP
CEO, RP Payments Risk Consulting Services

(Customer perspective article)

No matter what industry you are in, cybersecurity has certainly become an industry buzzword. And rightfully so considering the constant reports of devastating cyber-attacks against businesses; businesses losing millions of dollars, consumer records, and more without knowing what hit them until the damage is done.

What's All the Buzz About

Released in May, the Ponemon Institutes 2015 Cost of a Data Breach Study found that on average, a business paid **at least** $170 **for each** lost or stolen record containing sensitive and confidential information. That figure doesn't include costs related to lost reputation, class action lawsuits, forensics, lost revenue, and fines.

Agencies such as the U.S. Securities and Exchange Commission (SEC), the Payment Card Industry (PCI) Security Council, and the Federal Trade Commission (FTC) have routinely proven that breached companies can expect an in-depth investigation following a breach. Recent FTC fines have ranged from $10 million to $25 million per company (ChoicePoint and AT&T respectively). PCI fines have been known to hit the billions of dollars, leaving big businesses at a substantial profit loss and potentially putting a smaller business out of business altogether. With 60% of small businesses going under within 6 months of being breached[2], achieving cyber security and PCI compliance should be one of your top priorities.

To those businesses who think a breach can't / won't happen to them: Reality check. FBI Director James Comey said it best: "There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked[1]." Not a big company? Security experts agree that small and midsized enterprises (SMEs) are more attractive targets to criminals because SMEs tend to be less secure than larger companies. Cyber-criminals use automated tools to mass produce attacks with little investment and most SME networks can't adapt to or combat the attack. So you really have to assume that someday, someone is getting into your network. What they get, well, that's up to you.

Prevention is the Best Medicine

The FTC wants businesses of all sizes to focus on security and prevention. To aid businesses in developing stronger security practices, the FTC released Start with Security: A Guide for Business in June 2015. The Guide introduces businesses to 10 sound practices that businesses of all sizes should be using.

The Guide is based on lessons learned from more than 50 investigations conducted by the FTC on businesses who were breached. The Guide breaks what are often viewed as complex security steps into easy to implement action items that any level of business can understand. From "Don't Collect What You Don't Need" to monitoring your network properly, the Guide's 10 practices are further broken down into categories, steps and helpful tips.

You don't have to be an IT expert to understand the Guide, but you do need to review it and begin implementation as soon as possible. While this is a "guide" for businesses, it will undoubtedly be what federal entities use in investigations if your business is unlucky enough to suffer a breach. If you find

your business is already meeting these minimum standards, great; but the work doesn't stop there. Security is ongoing and must be updated as threats change. The Guide offers basic security principals; ideally, your security program should exceed the recommendations.

[1] CBS News - FBI Director James Comey

[2] National Cyber Security Alliance

About the Author

Rayleen is the CEO of RP Payments Risk Consulting Services, based in Kansas City, MO. She travels the country presenting at fraud, payments and security conferences on topics ranging from Mobile, fraud, risk management, and regulatory compliance. Rayleen has been writing and presenting for 9 years. Previously she worked financial investigations for a national bank.