Facebook Under Investigation by the Federal Trade Commission

03.29.18

Everyone not purposely ignoring the news recently, has read the headlines about Facebook's breach of privacy rules with its release of personal information to Cambridge Analytica and the subsequent potential impacts on election results.

Facebook's chief information security officer recently tendered his resignation after unsuccessfully advocating for greater disclosure about foreign government misuse of Facebook to influence elections. Sandy Parakilas, a former Facebook privacy expert added, "The people whose job it is to protect the user always are fighting an uphill battle against the people whose job it is to make money for the company."

Security and privacy will always be on the expense side of the ledger, never the revenue side. Until organizations accurately evaluate the potential impact of breaches, security will not get the attention it deserves. One result of Facebook's breach of trust is an ongoing Federal Trade Commission (FTC) investigation, with fines almost certain to follow. As a result, Facebook has lost over $40 billion dollars in stock value over the past few days – loses generally agreed to be a direct result of the data breach headlines.

The Facebook investigation is just the latest in a series of investigations, many of which have resulted in FTC suits against numerous defendants. Over the years, the FTC has grown more active in investigating security and privacy breaches.

Originally, 16CFR Part 314: Standards for Safe-Guarding Customer Information was poorly understood and not rigorously enforced. Since 2015 though, the FTC has significantly ramped up its guidance efforts. In November 2015, the FTC published Start with Security: A Guide for Business. This handy Guide focuses on how to avoid a breach and also provides a list of 10 best practices. Then in late 2016, after having previously provided breach avoidance guidance, the FTC published a data breach response guide, Data Breach Response: A Guide for Business.

While providing enhanced guidance, the FTC has also been busily investigating and fining organizations for lacking preparedness. Just a few of the organizations who've settled with the FTC include: Target, RadioShack, Oracle, Snapchat, LifeLock and many, many more.

If your organization deals with personal data, you could be next on the FTC's investigation list due to a breach. To stay compliant under 16CFR Part 314, at the very least, you should consider the five following steps:

1. Designate a security officer and grant them the authority to get the job done
2. Perform a risk assessment that identifies reasonable threats
3. Test systems and personnel to ensure they're securing information as expected
4. Manage service providers to minimize threats to your organization
5. Harden systems to secure vulnerabilities revealed as a result of the above steps

By starting with these basics, your organization can reduce the risk from hackers and demonstrate due diligence in the unfortunate event a breach occurs. The cost of a data breach is almost always more than many organizations think. Penalties for violating the FTC agreement can go as high as $40,000 per day per violation. Can you afford that risk?

It is important to address the breach registration now. BPM's Information Security Assessment practice helps organizations protect against threats before it's too late. Contact us today to learn how we can help.

© 2020 BPM