MINTZ

Happy 2014!

January 03, 2014 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

After a brief hiatus for the holidays and our "12 Days of Privacy" series, we are back.

We have had a series of late year -- and new year -- data breaches in the news. These latest incidents should prompt New Year's resolutions to undertake risk assessments and internal reviews of data security practices in general.

- The **Target data breach** continues to occupy headlines and will for some time to come as more details of the massive data theft become known. The well-known security blog, **Krebs on Security**, has the latest.
- Right before New Year's Eve, a popular Boston restaurant and bar group **disclosed that it had been hacked** -- for a second time. In 2011, the Massachusetts AG's office fined The Briar Group $110,000 for its failures to secure credit card information and we **wrote about it at that time**. The resulting consent order imposed a series of required compliance measures and this latest breach incident puts The Briar Group at risk of violation of the consent order. We will be watching this one -- as should all businesses that collect payment card information.
- On New Year's Eve, a website published a database reportedly containing upwards of 4 million Snapchat user names and phone numbers. Today, the popular app **announced that it is adding an opt-out to its "Find Friends" functionality** -- the functionality that apparently allowed the hacker to obtain the user information. Does your application access user's address books? If so, you should be checking out the **details of the Snapchat breach** and fixing code vulnerabilities.
- And on New Year's Day, Skype was **apparently hacked by the Syrian Electronic Army**, although Skype says that the exploit did not compromise any user data.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.