

October 30, 2013

Resources

[JW Cybersecurity Practice Area](#)

[Contact JW](#)

www.jw.com

2013: Year of the Mega Breach Cybersecurity Awareness Month - A Good Time for a Crisis Audit

By [Bill Cobb](#) and [Irma Jacobson](#)

Already this year, hackers have perpetrated seven "mega breaches" (breaches involving over 1 million records each), compromising and exposing over 112 million total records. The average size of a data breach in the U.S. this year has been approximately 28,765 records at a cost of \$188 per record, for a total \$5.4 million in costs per breach on average.¹ In comparison, the average cost of a mega breach involving a malicious attack in 2013 is \$277 per record. In 2013, mega breaches alone will cost U.S. industry over \$20 billion. The seven mega-breaches in 2013 include:

- Adobe (video, photo, and web design software): 2.9 million records; estimated cost: \$545 million;
- Living Social (discounted gift certificates): 50 million records; estimated cost: \$9.4 billion;
- Evernote (business organization software): 50 million records; estimated cost: \$9.4 billion;
- Facebook (social networking): 6 million records; estimated cost: \$1.13 billion;
- Washington State Courts: 1 million driver's license numbers; estimated cost: \$188 million;
- Schnucks (grocery store chain): 2 million credit cards; estimated cost: \$376 million; and
- www.drupal.org (web and application design): 1 million records; estimated cost: \$188 million.

This year hackers also accessed databases at the *New York Times* and the Federal Reserve.

In 2013, the majority of breaches are due to criminal and malicious cyber-attacks which comprised 37% of all data breaches in the U.S., compared to 35% of data breaches due to third party or user errors. The businesses most commonly targeted are those in the healthcare, financial, and pharmaceutical industries.

The average total cost of a U.S. data breach (\$5.4 million) consists of the following component costs (all averages): \$400,000 for detection and escalation costs (includes investigations, audit services, crisis team management, and communications to executive management); \$565,000 for notification costs (includes creation of data bases, determination of regulatory requirements, engagement of experts, and secondary contact information); \$1.4 million in ex-post response costs (includes special investigations, remediation activities, legal expenditures, product discounts, identity protection services, and regulatory interventions); and over \$3 million in lost business (includes abnormal turnover of customers, increased customer

acquisition activities, reputation losses and diminished goodwill).

Importantly, companies that had an incident response plan in place prior to the breach experienced an average reduced cost of \$42 per record, which translates to an average savings of almost \$1 million for the affected company. Companies that had a strong security posture at the time of the breach experienced a reduction of \$34 per record, which means an average savings of over \$800,000 for the affected company. In addition, companies that engaged consultants at the time of the breach experienced a reduction of \$13 per record, which means an average savings of over \$300,000 for the affected company. These few preventative postures can be enough to save an average U.S. company over \$2 million in total costs, almost 50% of the average expense incurred by a company experiencing a breach.

Not only does having a data breach crisis response team in place lower the data breach costs of a company, the absence of a well-qualified team can actually increase the data breach costs of a company. For example, well-meaning, but unnecessary reactions to a data breach, such as providing notification to affected users (when the law does not require such notification), cost U.S. companies on average \$37 more per record in 2013. This action alone increased the total cost of a data breach by almost \$900,000 per company on average.

Data breaches are expensive whether accidental or malicious. Companies experiencing a data breach are likely to incur significant direct costs as well as indirect costs such as future loss of business and goodwill with current customers. It is therefore important for every company to be prepared in order to reduce the impact of a potential data breach as much as practically possible. By far the most profitable investment in prevention is for a company to have a response plan in place at the time a breach occurs.

Is your company prepared to respond to a cyberattack or data breach? Contact us about obtaining a cybersecurity crisis audit. In the event of a data breach or cyberattack, ask for the JW cybersecurity response SWAT team.

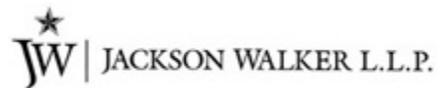
If you have any questions about this e-Alert, contact **Bill Cobb** at 512.236.2326 or bcobb@jw.com or **Stephanie Chandler** at 210.978.7704 or schandler@jw.com.

For more information regarding Jackson Walker's Cybersecurity practice, [CLICK HERE](#).

¹All cost data for the average U.S. company is based on actual loss data as collected by the Ponemon Institute. These are neither estimates nor extrapolations. The study excludes mega breaches because they are atypical to the industries they affect, thus, the costs related to mega breaches, are estimated based on the actual breaches reported by the affected company and the actual costs reported by the Ponemon Institute using a conservative estimate of \$188 per record. The actual costs can vary. The research is a global study conducted annually by the Ponemon Institute, LLC and is available at Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis*. To view this study, [CLICK HERE](#).

*If you wish to be added to this e-Alert listing, please [SIGN UP HERE](#).
If you wish to follow the JW Technology group on Twitter, please [CLICK HERE](#).*

Austin Dallas Fort Worth Houston San Angelo San Antonio Texarkana



Cybersecurity e-Alert is published by the law firm of Jackson Walker L.L.P. to inform readers of relevant information in cybersecurity law and related areas. It is not intended nor should it be used as a substitute for legal advice or opinion which can be rendered only when related to specific fact situations. For more information, please call 1.866.922.5559 or visit us at www.jw.com.

©2013 Jackson Walker L.L.P.

Click [here](#) to unsubscribe your e-mail address
901 Main Street, Suite 6000 | Dallas, Texas 75202