Introducing the Fisher Phillips Privacy and Data Security Blog!

Insights
7.24.15

Introducing:the Fisher Phillips Privacy and Data Security Blog!Near and dear to us privacy practitioners, we seek to bring readers the latest and greatest privacy and data breach news as it affects the workplace and consumers worldwide.Please let us know if you have any questions and feel free to comment!Our first article follows:

This Week in Data Breach:
To begin our reporting we take the opportunity to highlight a growing issue for employers and consumers alike:what happens when you rely on the Internet for your business in any way, you get hacked, and you suffer a data breach.Whether you suffered issues from the recent Anthem breach, the Premera Breach, or for public employees, the OPM Breach, data breach is a reality that any employer, business or other entity that touches the Internet or data must address.

This week in data breaches brings additional victims.To wit, just last week, a Vancouver, Canada-based photo site host was discovered to have caused the breach of customer and employee information of Walmart and CVS across Canada and the United States.Then, UCLA Health, which includes the UCLA Medical Center and 150 other primary and specialty offices in California, announced that "criminal hackers" accessed parts of its computer network.While the statement further announced that there was no evidence of actual breach, the FBI is now investigating.Last but not least, Avid Life Media, which owns cheating site AshleyMadison and AdultFriendFinder.com (breached two months ago when its data was stolen and leaked), announced that hackers apparently averse to AshleyMadison had stolen large caches of user data from the site, including employee network account information, company bank account data and employee compensation information.The hackers, calling itself the "Impact Team", A statement from the company on July 20 acknowledged the breach:

TORONTO, July 20, 2015 — We were recently made aware of an attempt by an unauthorized party to gain access to our systems. We immediately launched a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature, and scope of this incident.

We apologize for this unprovoked and criminal intrusion into our customers' information. The current business world has proven to be one in which no company's online assets are safe from cyber-vandalism, with Avid Life Media being only the latest among many companies to have been attacked, despite investing in the latest privacy and security technologies.

attacked, despite investing in the latest privacy and security technologies.

. . . At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber–terrorism will be held responsible.

Avid Life Media has the utmost confidence in its business, and with the support of leading experts in IT security, including Joel Eriksson, CTO, Cycura, we will continue to be a leader in the services we provide. "I have worked with leading companies around the world to secure their businesses. I have no doubt, based on the work I and my company are doing, Avid Life Media will continue to be a strong, secure business," Eriksson said.

As the foregoing breaches illustrate, hackers and breaches are not going away anytime soon.Aside from the business implications of such privacy violations, the most immediate threat may be failure to comply with regulatory requirements applicable to employers and businesses.These might include, without exclusion:the Gramm-Leach Bliley Act, The Federal Trade Commission Act, HIPAA's Privacy Rule as modified by the HITECH Act, FERPA, practically every states' (47 as of June 2015) own data breach notification requirements, and if you happen to practice in the European Union—the EU Privacy Directive.

Employers and companies can take proactive steps to avoid breaches and ensuring regulatory compliance through educating management on regulatory requirements, as well as through establishing compliance and technology security-based rules.This may include routine self-audits and review of systems to ensure security, audits of vendors who provide security, and considering the need for cyber insurance.At a minimum, as data breaches continue, employers, and especially business associates (now required to do so under the HITECH Act), should conduct privacy assessments to determine security risk and how to mitigate those risks. We can help you with those.

Stay tuned for future articles on these topics!

Have a comment or question? Please use our comment feature below.