Twitter Facebook LinkedIn Google+ Blog Press Box Subscribe to our Podcast

CONTACTS

Colleen Madden, Director of Public Relations
Office: 312-422-5074
Mobile: 314-807-1568
colleenmadden@challengergray.com

Blake Palder, Public Relations Associate
Office: 312-422-5156
blakepalder@challengergray.com

FOR IMMEDIATE RELEASE

Companies Spend More on Security Breaches

AS PRIVACY LAW EVOLVES, DEMAND FOR PRIVACY PROFESSIONALS GROWS

CHICAGO, May 17, 2017 – From search engines to social media, every website seems to be collecting user data en masse, and once this data is collected, companies are facing more and more regulations on how they can share or store this data, potentially creating opportunities for workers in this field.

Data privacy is troubling most Americans. According to a survey conducted by AnchorFree, 95 percent of Americans are concerned about what companies may be doing with their data without permission. Greater than half are looking for ways to secure their information, as more Americans utilize e-commerce and social media sites.

"Data privacy is becoming one of the top concerns for consumers and businesses alike. Companies are feeling the pressure from not only customers and clients, but also

employees to protect sensitive personal data being collected," said John Challenger, chief executive officer of global outplacement and executive coaching firm Challenger, Gray & Christmas, Inc.

"This process can be expensive, as companies cover the cost of implementing privacy policies, complying with federal and state regulations, and notifying employees or customers in the event of a breach," added Challenger.

According to the Ponemon Institute, the average cost of a security breach to a company in 2015 was $3.79 million. This is up from $3.52 million in 2014. These costs include government penalties, cost of compliance and notification, and credit monitoring for victims.
Because online data collection is a relatively new issue, the laws vary from jurisdiction to jurisdiction. Under the Obama administration, it seemed as though the federal government was going to protect data using the FCC Broadband Privacy Rule, which would make it more inconvenient for companies to distribute user information. However, in the past month, the Trump administration shut down these regulations before they were even rolled out to the public.

"Federal law protects health, financial, children, and student data. However, many states do not have basic privacy protection, such as a breach notification statute that would force companies to alert customers when their data has been compromised. In other cases, states have more far-reaching laws than the federal government, such as in California, which leads the way in data privacy regulation," said Challenger.

Several states have started to take data privacy into their own hands. Just last week, the Illinois senate approved "The Right to Know Act," which, if put into law, would help to secure user data by requiring companies of a certain size to list the data being collected and list information about third parties who are purchasing the data. Specifically, companies with over ten employees that share data, not necessarily sell it, fall under this legislation.

As with many bills, "The Right to Know Act" drew a certain amount of opposition. According to the Chicago Tribune, Republican Senator Chris Nybo expressed concerns about the difficulties on e-commerce caused by the bill. In the same article, Republican Senator Jason Barickman criticized the bill, saying that data collection should be regulated by the federal government, not by the states.

Until comprehensive, federal laws are set in place, businesses have to keep track and abide by several state and local regulations on the collection and distribution of personal data. This can prove difficult for companies that do business nationwide or internationally or smaller companies that lack the staff dedicated to this issue.

"In May of next year, a sweeping data protection law will take effect in the European Union. The General Data Protection Regulation (GDPR) will likely be the standard that other nations have to meet on data privacy. Any company with international operations in the EU will be impacted by this law," said Challenger.

The implementation of this law, and others as privacy laws evolve, will likely be a boon to professionals in this field. Experts in compliance, legal, and privacy will be in demand from companies scrambling to comply.

Failure to do so could cost companies a minimum of $16,000 per federal offense. The penalty for breaking the Gramm-Leach-Bliley act, for instance, the law that protects financial data, could cost companies up to $1 million, while the penalty for the Health Information Privacy and Protection Act (HIPPA) could reach $1.5 million. These penalties increase if criminal activity is proven.

"Companies will need individuals to comb through current law, and build and implement policies to protect the company and its customers, especially as more and more consumers demand to know exactly what is happening to their data," said Challenger.

###