The LinkedIn Data Breach: What Can Businesses Learn?

by DonaldScarinci

Information privacy and security are hot topics these days and for good reason. Social media website, LinkedIn was the latest high-profile company to suffer a serious customer data breach.

On June 6, LinkedIn made headlines when it was discovered that hackers had posted 6.5 million LinkedIn passwords to an underground forum. In addition to the negative publicity associated with the breach, the company was subsequently hit with a $5 million lawsuit.

The data breach lawsuit, which seeks class-action status, claims that LinkedIn failed to use "long standing industry standard encryption protocols," which should have protected user information. The company has since increased its security measures, but maintains that the lawsuit is meritless because users have not actually been harmed.

Online shoe retailer Zappos is facing a similar lawsuit after hackers were able to gain access to data belonging to an estimated 24 million customers. A federal judicial panel recently consolidated nine proposed class-action lawsuits.

While these lawsuits may not ultimately be successful, the damage is already done in the eyes of customers. In many cases, the harm to the company's business reputation is greater than the actual legal liability. Therefore, it is important to understand, both from a legal and technological perspective, how to develop sound privacy and security policies that protect sensitive customer information.

Data Privacy

To avoid liability, businesses should create a privacy policy that details how customers' personal information is collected, used, shared, and secured. While most businesses are not legally required to enact privacy policies, they can certainly help avoid future legal headaches.

It is also important to note that businesses that deal with certain kinds of sensitive data such as health records and financial information do have specific legal obligations. For instance, HIPAA regulates the privacy and security of medical information, and the Graham-Leach-Bliley Act stipulates how financial institutions must protect customer data.

Finally, all companies must ensure that their privacy policies extend to employees as well as third party vendors that manage or store data. For instance, employees, consultants, and business partners should all be required to sign non-disclosure agreements that address customer data.

Data Security

With respect to data security, every business must implement reasonable security measures to protect its customers' data and make sure that any third party that handles customer data does the same. While it may not be possible to stop every attack, should customer data be compromised, your security procedures will be under a microscope. Therefore, it is imperative that they meet industry standards.

Should your company fall victim to a security breach, you also have certain obligations as well. For instance, most states have laws that require customers and certain government agencies be notified in the event that customer information is compromised.

Ultimately, it is much easier to prevent a security breach than it is to clean up after one occurs, just ask Sony, Citibank, Zappos, and most recently, LinkedIn.