Security and data protection procedures are everyone's concern

Q: With the recent breach of Equifax, it seems that vulnerability to identity fraud is everywhere. Are there measures I can take on behalf of my company and employees to minimize risk?

Fred A. Leibrock is an experienced trial lawyer who has tried dozens of jury trials and has served as lead counsel in a number of significant cases involving complex, multi-jurisdiction issues.

A: Act now and seek professional technical assistance. Hire the right technical person or firm to help you test your systems, assess your vulnerabilities and implement your security and data protection procedures and recovery plans.

The question isn't whether someone will try to steal your data, but when. You need to be ready.

Q: From a legal standpoint, if my company's data is breached, can my company be held liable for harm to employees or customers whose information may have been compromised?

A: Yes. Although this is a rapidly emerging area of the law, as a general rule an entity that is negligent in safeguarding confidential customer or employee data can be held liable as a result of a breach, or as a result of disregarding legal notice requirements after the breach. The principal question on the issue of liability is whether the entity took reasonable steps before the breach to protect the data, and after the breach to protect and notify the customers or employees. What's reasonable is a moving target that must be determined on a case-by-case basis. However, there are few legitimate excuses in this day and age for a company to not take significant affirmative steps to safeguard electronic data.

Q: What are some of the bigger mistakes that companies make when it comes to protecting their data?

A: According to the Federal Trade Commission, the principal unreasonable practices that result in data breaches include weak password policies, lack of encryption, broad dissemination of administrative passwords, and lack of security between systems with sensitive data and other computers inside and outside the network.

Q: What measures can I take to protect my company from a data breach?

A: Engage in advance planning. To reduce the risks of a data breach, follow the recommendations of the National Institute for Standards & Technology by planning ahead of a breach to: identify the components of your systems and their vulnerabilities; protect the components from penetration;

detect latent threats that may have already penetrated your systems; respond to a breach and recover from a breach. Also, train your employees to be alert to cybersecurity risks.

Q: It seems like all businesses rely on digital data transfer, whether it's using file transfer services or sending sensitive documents through email. How do I continue to take advantage of these conveniences and still secure my information?

A: Avoid unnecessary risks. There are a million affordable products on the market that allow you to encrypt stored data and data in transmission. Use them and be willing to pay for security and data protection. If you must transmit sensitive data over an unsecure network, at a minimum encrypt it with a strong password before transmitting it.

From NewsOK / by Paula Burkes
Published: September 20, 2017
Click to see full story – Data security, cyber threats are everyone's concern

Click to see Fred Leibrock's attorney profile