Have You Thought About Encrypting Your Company's Data, And Its Communications? Perhaps You Should

Insights
8.01.19

Alright. So, you've battened down the hatches of your company's premises, to protect your employees and your information. Employees are required to create secret computer passwords they're not to share with anyone, even colleagues. Your policy requires changing passwords every 45 days. You've installed security guards at the front desk, distributed security badges to limit access to your premises, conducted background checks on your new hires. You require signed Confidentiality, Non-solicitation, and Non-competition Agreements with employees to whom you've provided access to your secrets. You've erected firewalls to protect your servers.

Are you done? Probably not. Even if you've done all of the above, and have remained vigilant in enforcing all of those identified protective measures, your company and your data are likely NOT 100 percent protected. What would you do if the hackers make it past your firewalls, or obtained an employee's password to gain access to your company's information? You'll need another layer of defense.

You really need to think about encryption, that, is encoding your data and your electronic communications such that, if (or more likely when) you do suffer a breach, any data or communications the hackers might have reached will still be protected, because it will be indecipherable.

According to the Website StorageCraft.Com, which specializes in this subject, data encryption entails taking your data and translating it into a new form so that only people with access to the encryption "key" would be able to read it. Encrypted data is sometimes referred to as "ciphertext", unencrypted data is termed "plaintext". The obvious purpose of encryption is to protect digital data's confidentiality.

This far into the 21st century, many businesses and public sector employers are abandoning paper files and copies for exclusively electronic (digital) formats. If you employ a sales force, accountants, attorneys or others who interact with, and travel to and from, client locations to conduct your business, they likely are toting their company-issued laptops, tablets and/or smart phones, chock full of both company and client data. If a hack of your electronic files occurs and the data is NOT encrypted, then the data and information stolen could be utilized to the hackers' advantage, and your company's extreme detriment. Not only should the data be encrypted, but those company-issued

laptops, tablets or smart phones also should be encrypted. If employees are sending price quotes, accounting advice, legal advice or other sensitive communications over their devices, that transmission system – typically electronic mail or text messaging, should be encrypted as well.

According to StorageCraft.com, there are two types of encryption, symmetric and asymmetric. Symmetric is more typical and more widely used. It uses one secret key to encrypt and unencrypt data. The sender creates the key, encrypts what they wish to send, then sends it. SEPARATELY, the sender will provide the recipient with the decrypting key. Asymmetric is newer and a bit more sophisticated, utilizing two keys, a public and private key. The public key is provided to those who wish to send you encrypted information. ONLY you or your designated personnel know the second, "private" key, utilized to open and view the data sent to you from outside your organization.

What types of Information should be encrypted?

The most common target for hackers, and therefore information that should be encrypted, is Personal Identifiable Information, (PII) i.e. social security numbers, driver's license numbers, bank account numbers, and credit card numbers. For an employer's/business' information, certainly customer data, financial data, product release information, and research and development data should be encrypted.

If you presently haven't the resources to encrypt all your information, you'll need to make strategic decisions about what to encrypt, what not to. If the information you're considering were on paper, and you think you would shred it, then the electronic version likewise probably ought to be encrypted.

Related People

Andrew Froman
Partner
813.769.7505
Email