Rendigs
ATTORNEYS AT LAW

Business Briefs
Legal Update

Donald C. Adams
Partner

Email: DCA@Rendigs.com
Direct: 513 381 9361
Fax: 513 381 9206

The Dawning of the Age of Cyber Awareness Part 1/3

In 2015 alone, cyber experts indicate that losses due to cyber crime exceeded $400 billion dollars worldwide. Attacks were not limited to the huge retailers, medical providers, financial groups or shipping ports; in fact many hackers don't know the company they have breached until after they have gained access. Anyone who has records of personal information is subject to risk.

Many hackers don't steal the information but merely make it impossible for a company to access pertinent and necessary data by encrypting or locking the data on the infected systems. In this manner they can hold the information hostage until the company pays the ransom to the hackers who then provide the key to unlock the data. Several of my clients faced with this dilemma have chosen to pay the ransom, which in most cases is relatively cheap ($500 to $5000), rather than hire cyber experts.

Most state laws only require disclosure to clients or customers if there is a reasonable belief that the security breach may lead to identity theft or fraud. Only three states in the country have no security breach notification laws: Alabama, New Mexico and South Dakota. Security breach notifications laws vary between states but the gist of all these laws is consumer protection and notifying individuals whose information has been accessed.

The Ohio statute, ORC 1349.19 Private disclosure of security breach of computerized personal information data, requires notification to any resident of the state whose personal information was or reasonably is believed to have been accessed by an unauthorized person

Rendigs, Fry, Kiely & Dennis, LLP
600 Vine Street, Suite 2650
Cincinnati, Ohio 45202

and this access causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. The statute defines the type of notice necessary and places caps on notification expenses between $10,000 and $250,000. A failure to provide proper notice can lead to investigation by the State Attorney General or monetary sanctions.

Note however, that where the information has not been stolen but has been rendered inaccessible, there is no requirement to report this breach to your customers. Not surprisingly, companies have been hesitant to report the cyber breach to the authorities due to personal pride or the fear that customers would get wind their company has poor data security and customer information may not be properly safeguarded.

Let's face it, a security breach is bad for business. It is more than just a loss of information, it is a breach of trust between you and your clients or customers. There is also a potential for huge monetary loss to both the business and customers. Businesses are responsible for expenses like forensic investigations which can run $500.00 per hour, legal defense costs which insurance experts in a NetDiligence study have pegged at $434,000 on average, as well as crisis services like credit/ID monitoring averaging $499,000. The average claim amount for a major cyber insurance provider averaged $643,000 per claim. One claim alone could doom a small business with no insurance coverage in place.

Businesses must face the reality that it's not a matter of if an attempt to breach data security will happen but when. The key for successful businesses is how they will handle the breach. Are policies in place regarding how employees should notify IT of a potential breach? Employees don't want to tell managers that they may have opened an email containing the Pandora's box of malware and contaminated the system. Employees need to be trained as to how to handle questionable emails and internet information and to report suspicious activity to the appropriate IT personnel or managers without employment repercussions. Many companies are establishing emergency response plans in advance of any breach. These plans outline data backup procedures beforehand, IT and management roles in response to a breach, and criteria for determining whether notices to customers are required, as well as when and how such notices will be communicated.

Don Adams'*s practice focuses on civil litigation in the area of medical defense litigation, transportation, maritime and wrongful death and injury. He defends hospitals, corporations, nursing homes, and physicians. He counsels clients on risk management and quality assurance matters.*

Aaron M. Monk *is an associate in the firm's Business Services and Family Services Practice Groups. He assists both startup companies and existing businesses in a broad range of general corporate issues including company formation and governance, private equity financing, employment/independent contractor agreements, and intellectual property assignment agreements. Aaron also counsels families in legal areas related to succession planning in both business and personal wealth.*