HAND 75 ARENDALL
LLC ▪ LAWYERS

CYBERSECURITY
Alert

There is no greater threat to American businesses today than insufficient cybersecurity. The threat includes, among other things, the risk that a company's records, record-keeping system, or other digital information will be held hostage and unretrievable by ransomware; the risk that personally identifiable information ("PII") of customers or employees will be hacked and stolen, resulting in identity theft and massive potential civil liability for the company; and the risk that a company's trade secret information will be hacked, acquired, and either sold to or used by competitors to the company's detriment and damage.

In 2015, businesses worldwide paid over $325 million in ransom to obtain access to their business data that had been blocked by ransomware; that figure is expected to more than triple in 2016 as cybercriminals have turned their focus to this high-yield low-risk cybercrime. It is critical for businesses to address, prepare for, and protect against, a ransomware hack of their digital information.

The ransomware hack has become so profitable that it appears the incidence of PII theft and trade secrets theft has actually decreased; the profit from those thefts is more difficult to realize than is the profit from document ransoming. These are, nevertheless, threats that a business should not ignore.

Is your cybersecurity system up to date? Have you conducted an internal audit of your cybersecurity system and assessed its effectiveness in light of the growing cyber threats? Here is an abbreviated list of questions any business must be able to answer:

1. Who might initiate an attack against the company?
2. What information does the company have that might be stolen or held hostage?
3. What are the risks to the company in the event of an attack?
4. What tactics could be used to initiate an attack?

An effective internal audit will alert a company to the nature and the extent of its risk of a cyber-attack; the results are often frighteningly enlightening. A company unable to properly assess its risks with an internal audit – and it is a very difficult assessment – should promptly seek an external audit so as to clearly understand its cybersecurity risks.

Understanding its cybersecurity risks is an important first step for any company, but it is a short step in a long race. Once the risks have been identified, a further analysis is required, calling for answers to these questions, among many:

1. How can the company minimize the risks of a cyber-attack?
2. How can the company minimize the effects of a cyber-attack?
3. How can the company minimize the financial consequences of a cyber-attack?
4. How will the company respond in the event of a cyber attack?

This alert was prepared by Hand Arendall's Cybersecurity Practice Group. For further information or assistance, please contact George Walker.

George M. Walker
Practice Group Chair
gwalker@handarendall.com
251-694-6296

Practice Group Members:

Roger L. Bates
Joseph L. Cowan
Kelly Thrasher Fox
Christopher M. Gill
C. Dennis Hughes
Carolyne B. Jones
Sarah Outlaw McLaughlin
J. Burruss Riis
Christopher S. Williams

By answering these and other relevant questions, a company can put together a cybersecurity program that will offer the company its best opportunity to prevent a cyber- attack or, in the event it is a cyber-attack victim, that will offer it the best opportunity to avoid or minimize the consequences of the cyber-attack.

Hand Arendall's Cybersecurity Practice Group is uniquely positioned to provide a business with comprehensive counseling on cybersecurity, from overseeing an external audit to development of an effective cybersecurity program. Our practice group includes transactional and litigation attorneys because cyber-attacks implicate both business and litigation issues. We have in-house IT support and access to outside tech support to perform an external audit.

If your company maintains business information, employee or customer information, or trade secret information on or in any computer system, and if you are not able to conduct an effective internal audit or are not able to develop an effective cybersecurity program, we will be happy to consult with you and to assist you in protecting your assets and your information to every possible extent from a cyber attack.

If you have questions about cybersecurity or about the services we offer in this regard, please contact George Walker at (251) 694-6296.