TULSA BUSINESS & LEGAL NEWS

Friday, October 30, 2015 12:00 am

By Ralph Schaefer TB&LN correspondent

# Law firm now has a cyber security practice

No one thinks about computer security until they are hacked and personally affected. When security is breached, whether it is a missing laptop that contains government, corporate or personal data, or whether it is hacked electronically from a central computer system, a crisis has been created for many people.

Officials scramble to let clients know the company data has been hacked and limit the damage.

These incidents are not uncommon in today's fast-paced technology world, although some of the problems might have been avoided.

GableGotwals Law Firm now has a cyber security practice to guide companies with problems through resolution maze and provide preventive measures guidance.

Tom C. Vincent II in Tulsa and Diana T. Vermeire in Oklahoma City are leading the firm's efforts in the firm's new practice area.

"We at GableGotwals advise clients on not only how they collect, maintain data, protect and secure it, but also ensure best practices to the customer's benefit," she said. "We deal with a clientele from Fortune 500 companies, to major to small corporations and mom and pop shops. Everyone who collects information from a customer needs to be concerned about whether or not they are adequately securing and protecting client and company information."

Basically, businesses are collecting and retaining massive amounts of information that effort comes up against the need for the data and privacy security for customers, Vermeire said.

It is both a cyber security issue and the issue of the cloud, technology and electronic and hard copy data. Ultimately it is about the need to protect that information.

It also is a fact of life that nowadays technology tends to drive corporate practices rather than the other way around, Vincent added.

As tablets become more and more popular, corporate practices tend to accommodate them. While the guiding principle focuses on convenience, protection considerations must be factored in.

“We are seeing it from the banking industry which is making cyber security a top priority,” he continued. “Bank employees and directors must be aware of their cyber security responsibilities. The financial services industry and others are developing and maximizing the use of technological devices. They are going through restructuring pains as these additional controls are identified and implemented.”

There is a sense of urgency for companies of all sizes to recognize and understand the need to develop safe systems, Vermeire said. Those who fail to do so will find themselves woefully behind as issues grow and become increasingly significant.

Concerns center around the improper accessing of data, whether by a third party, criminals or whomever might see the sensitive information.

It also could be the inadvertent disclosure by well meaning, but negligent, employees.

Vincent noted the recent Securities and Exchange Commission attention and action taken where the security breach occurred within a company that resulted in illegal trading profits.

Recent statistics show that negligent human behavior at all levels primarily on the part of employees is responsible for about 30 percent of the breaches. Offenders have included company presidents, administrative assistants and employees at all levels.

Negligent but well-meaning employees make mistakes that lead to the greatest risk for companies, Vermeire said. Heavily regulated industries such as banks are very aware of their responsibilities. Third-party vendors often are less cognizant of their obligations to their business partners.

An extreme example could be a contractor servicing the copy machine that doesn’t adequately destroy the data contained on a hard drive that would put a client company at risk.

Clients are advised several ways, Vermeire said. They can address a situation by having or removing a hard drive and retaining it.

They could contractually require vendors take steps to destroy the hard drive. The important thing is someone must be responsible to ensure the destruction is properly done. It is part of the service the vendor provides.

Laptop thefts also rank at the top of the list.

Vincent said state statutes differ and companies must be aware of their responsibilities in making their responses.

“We work with clients to draft an appropriate complete response and get it to the clients in a timely manner,” he said. One client informed the affected customers about a laptop theft, pointed out their possible risk and advised the company of steps being taken so it wouldn’t happen again.

Those customers were reassured because of the immediate action and didn’t feel like they would be surprised or that some information had been withheld. Regulatory agencies can be involved in the notifications and that is another reason that front-end notifications are so important.

Laptops and related security issues should be a concern to companies, Vermeire said.

“We try to help clients think through their options with this equipment and determine what makes the most business sense to them,” she said. They shouldn’t be available to anyone if they aren’t needed.

Restrictive codes should be put on any laptops and all units numbered.

Companies often have hundreds of laptops, but couldn’t say which unit was assigned to which employee, Vermeire continued.

Mobile devices that can transfer information must be identified and monitored to prevent security breaches, Vincent said.

The loss of smartphones, tablets, flash drives, portable hard drives and other devices provide unexpected problems.

“A lost $1,500 laptop may be perfectly clean, but that missing $20 flash drive containing years of company information would be devastating,” he said. “The usual lost laptops and cell phone scenarios are more about getting immediate cash than the potential for finding and using information that can be capitalized on.”

Another security threat occurs when third parties secretly access company networks and wait for critical data to be sent.

The host company is unaware of the situation and routinely conducts its business.

The breach occurs when an employee inadvertently opens a link that provides the access, Vermeire said. Companies must have proper technical safeguards in place.

“That is one of our discussion points with clients,” she said. Employees must understand their vulnerability and make certain they are not exposing the company’s network to criminal activities.

Employee training is critical, Vincent said. One employee obtained information they shouldn’t have had access to and mentioned it to another employee. A negligence lawsuit was filed against a firm as a result.

Improper access doesn’t mean a third party breaking in and stealing it, he added. It could mean someone has access to that information and doesn’t know how to properly treat it.

Vincent and Vermeire stay on the cyber security forefront and understand the changes in the law and know the best practices so they can advise clients to guard against data security breaches and ensure their client’s privacy.

“Diane and I have talked about what we are able to offer clients through our perspectives and at the end of the day, we like to think that our relationship with our clients as something to the effect that we worry so they don’t have to,” Vincent said. “Worry doesn’t keep us up every night, but there are some nights that it does.”