TULSA WORLD

Five Questions with Tom Vincent

Posted: Friday, December 4, 2015

By ROBERT EVATT World Business Writer

Attorney Tom Vincent stands at the Gable Gotwals offices in Tulsa. MATT BARNARD/ Tulsa World

Tom C. Vincent II is an attorney with the law firm of GableGotwals, where he leads the firm's Cybersecurity and Data Privacy Group.

1. Why did GableGotwals create a cybersecurity practice group?

Information has become much more accessible and transportable — essentially, more vulnerable — over just the past few years. This increased vulnerability has resulted in cybersecurity becoming a concern in areas of law — employee conduct and corporate policy development, for example — where it previously hadn't.

Our Cybersecurity and Data Privacy Group was formalized to better provide clients with a complete resource center for not only these traditional issues, but also for new issues exclusive to cybersecurity and privacy.

2. What sort of businesses are vulnerable to cybercrime?

Any business with electronic information is vulnerable. Incidents involving stolen personal information tend to gain more public attention, but what business owners may not realize is that their commercial information may be targeted as well.

As an example, for a small business its financial and pricing information may be of value to its competitors. On a larger scale, inside information of public companies can be valuable to those looking to profit in the stock market.

3. Briefly, what are some common forms of cybercrime?

The most basic version is simple physical theft — someone breaks into an office or vehicle and steals a laptop, for example. The unfortunate thing for the victim is, while the criminal's interest may not have been in the data (just in the laptop itself), the victim may have a responsibility to notify those individuals — customers and employees — whose data was on the laptop.

In addition, criminals may use "phishing" or "spear phishing" — blanket or targeted emails designed to gain access into company systems.

4. What do criminals do with information once it's stolen?

If the ultimate target is the data itself, it may be utilized or sold — whether personal or company information. Just this year, the Securities and Exchange Commission filed fraud charges against 32 defendants in connection with a scheme involving trading on confidential company information — this "outsider trading" (trading on inside information by individuals outside the company) generated over $100 million in illegal profits.

5. What are some things businesses can do to protect themselves?

When it comes to the types of attacks that may be directed at companies large and small, awareness is often the strongest defense. Business should train their employees regularly on basic email and Internet security issues — for some employees, this may be their first experience with email or the Internet. Also, a point person — someone in information technology, typically — should be established, to communicate issues identified by the company — just because one employee figures out an email is a hacking attempt, doesn't mean they all will.

Robert Evatt 918-581-8447
robert.evatt@tulsaworld.com

http://www.tulsaworld.com/business/5questions/five-questions-with-tom-vincent/article_2ec77d8c-4758-5cb0-af59-5968c16ac102.htm