Are You Safe From Hackers?
By Todd McMurtry

Just this past summer, the Hacker "Anonymous" released reams of information stolen from the FBI. Anonymous reportedly did this to embarrass ManTech, the contractor that handles the FBI's cyber-security. This bold attack shows how completely vulnerable each entity is to determined hackers. The international accounting firm, Deloitte, recently released a detailed overview of the criminal threats posed by hackers, emphasizing that cyber crime is a significant and underappreciated risk for business. It found that cyber attacks were increasing in frequency, that the hackers are outwitting the defenders, and that an underground economy has evolved around stealing data. Most ominously, the Deloitte report found a nexus between cyber crime and other threats such as industrial espionage, terrorism, and foreign security services. Certainly, most companies are not major international players worthy of a John LeCarré novel, but most businesses have bank accounts that might be vulnerable to a cyber criminal.

One of the most relevant points of the Deloitte article was its reference to how hackers can infiltrate a business and go undetected for months. In that time, they can engage in fraudulent wire transfers resulting in a loss of a company's funds and/or loss of customer data used to then steal from customers. The end result of such a crime would surely be both a catastrophic loss of reputation and potentially a fatal financial blow. As well, hackers can target a hospital's medical records, personal financial information, and sensitive business data. All of these items have value. Furthermore, loss of a customer or patient's personal and medical data may result in liability to the entity that allowed the data to be taken. Knowing that hackers present a present danger to most business and service providers, what practical steps should one take to limit the liability they cause?

First, obtain proper insurance. Many insurance companies now offer what is called Cyber-insurance. It helps protect businesses from hackers and other computer related risks such as inadvertent loss of data. Cyber risks are generally not covered by traditional insurance, so it is important to know what an insurance policy actually covers and to seek additional cyber liability coverage, as needed. Look for coverage for losses arising from data destruction, extortion, theft, hacking, and denial-of-service attacks. Also, seek protection from losses caused to others arising from errors and omissions, failure to safeguard data, or defamation. An insurance company may also assist in assessing a company's particular cyber security needs, further insulating the company from liability.

Second, properly destroy your old computers, smart phones, and other electronic storage devices so that data does not inadvertently fall into a criminal's hands. Companies like 2trg, with facilities in Ohio, Kentucky and other states, provide safe destruction of electronic storage devices (2trg.com).

Finally, evaluate interaction with customers and clients. When a business retains a customer's sensitive personal data, it can limit its liability for inadvertent disclosure of that data. It can require that claims be arbitrated instead of pursued in court, prevent pursuit of a class action, and limit total damages.

While it appears that hackers like Anonymous have the upper hand and can attack at will, that does not mean that you or your company are completely vulnerable. By taking the few basic steps outlined in this article, you can substantially limit the risks posed by hackers—today's high tech thieves.