NAVIGATING CYBER SECURITY IN NEVADA

BY LAURA M. TUCKER, ESQ.

As small businesses become more technology-dependent, the risk of suffering a data breach rises. Wading through the options for protecting your law firm (or advising your client on how to protect his or her own business) can be overwhelming, but fortunately, Nevada law provides guidance. While the information in this article serves as a starting point for data security, it is only a general overview of this vast and critical subject.

Nevada Law– NRS 603A et seq.

If you or your client handles sensitive or confidential information, setting up a plan and implementing security measures should be a top priority. A "data breach" is defined as an incident in which sensitive, protected or confidential information has potentially been viewed, stolen or used by an individual who is unauthorized to do so. Under NRS 603A.030, any business entity or association that handles, collects, disseminates or otherwise deals with non-public personal information is a data collector and is therefore subject to the provisions of NRS 603A *et seq.* If a data collector maintains records containing the personal information of a resident of the state of Nevada, that entity shall implement and maintain reasonable security measures to protect those records from unauthorized access. NRS 603A.210.

Nevada law provides that personal identifying information (PII) include a person's first name or first initial and last name, in combination with any one or more of the following:

- A social security number;
- A driver's license, authorization card or ID card number;
- An account number, credit or debit card number (in combination with the security code, access code or password permitting access to the person's financial account);
- A medical or health insurance ID number; or
- A username or unique identifier in combination with a password, access code or security question permitting access to an online account. NRS 603A.040.

Additionally, any business that collects payment card information in connection with the sale of services must comply with the current version of the Payment Card Industry Data Security Standard (PCI Standard). The PCI Standard itself could be the subject of a multi-day course; in a nutshell, the PCI Standard is a set

of security guidelines designed to ensure that all companies accepting, processing, storing or transmitting credit card information maintain a secure environment. The PCI Standard applies to any organization, *regardless of size* or number of transactions, that accepts, transmits or stores any cardholder data. The current PCI Standard can be found at the PCI Security Council's website at www.pcisecuritystandards.org. It is not enough that your third-party payment processor is PCI compliant; your business must also be PCI compliant.

Preparing for a Data Breach

No matter how small your firm or your client's business may be, preparation is key to defending against a data breach. Should a data breach occur, a data collector will not be liable for damages if that data collector is in compliance with NRS 603A and the breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees or agents. NRS 603A.215(3).

Often, data breaches result from negligence on the part of an otherwise well-meaning employee.

If your budget allows, consider outsourcing your security to a reputable company specializing in small business protection. While the upfront expense may seem steep, the price could save money in the long run. However, even without the funds to hire a technology expert, small businesses can take several preventative measures to protect against a breach.

First, every employee in the business, from the secretary to the CEO, should be trained and included in a business-wide technological security policy. Often, data breaches result from negligence on the part of an otherwise well-meaning employee.

Second, inventory and review the PII you possess. Next, develop and follow, without exception, written policies for data use, retention and security. Ask yourself:

- What kind of data do you have, and how sensitive is it?
- What protections do you currently have in place?
- Where does the PII reside, who has custody of it, and who can access it?

These policies should be re-evaluated and, if necessary, updated at least every six months. If you do not have a cybersecurity policy in place, contact your insurer to explore the cost of obtaining one.

Third, have a crisis management plan in place, and regularly hold drills to ensure that it is effective. Identify the members of a crisis response team. This group includes a person who is responsible for

continued on page 10

continued from page 9

NAVIGATING CYBER SECURITY LAW IN NEVADA

data breach prevention, detection and security; legal counsel responsible for notifications to underwriters and regulators; and human resources and marketing point people, responsible for internal and external communications and reputation management. Any mitigation strategy should be flexible, so that one can anticipate known risks and plan accordingly, and determine how to neutralize a breach as quickly as possible.

Legal counsel included in this plan should be familiar with notice requirements in Nevada and any other states where customers reside. In Nevada, any data collector shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay. NRS 603A220(1).

Fourth, encryption is key. You should password and PIN-protect *every* device. Do not forget smartphones, tablets, laptops and other devices that access your network. If an employee uses a personal phone to access firm email, require that he or she encrypt that device in the event that it is lost or stolen while not at work. Change generic passwords on routers. Have all employees update their passwords regularly, and make sure the passwords are complicated. Use multi-step verification when possible. Make servers and files need-to-access; every employee does not need to get to every file. Finally, review system logs manually or use an automatic tool to check for suspicious activity. If your budget allows, consider retaining a third party to conduct a systems security risk assessment on an annual basis.

Have all employees update their passwords regularly, and make sure the passwords are complicated.

Responding to a Data Breach

Suppose the worst happens: despite all of your careful planning and encryption, a data breach occurs. First of all, do not panic. This moment is when your crisis management plan springs into effect. Seek an outside forensics team (preferably one you have previously vetted) and legal counsel as soon as possible to guide you through the next steps.

Next, limit data exposure and determine the scope of the breach. Make sure you know how to isolate a system without simply turning it off. If the source computer is known, take it off the network. At a minimum, figure out how many systems were accessed, what data type was exposed, etc. Determine what information was stolen and look for the source of the breach. Was the information also a communication to which attorney-client privilege attaches? Do not wipe the servers; this will destroy evidence that could help the forensics team or law enforcement.

Notify staff and law enforcement, as well as your insurance and business partners, of the breach. Do not forget to contact any third-party service providers to determine if they were also affected or might have even been the source of security weakness. Know what steps you must take in order to trigger available insurance coverage. When the cause of the breach has been identified, implement recommended remediation actions and update internal policies concerning the use, retention and security of data.

Finally, if required and if law enforcement does not forbid it, notify the victims of the breach. Generally, those affected will want to know how and what happened, what information was accessed and what your business is doing to prevent further harm. Remember that managing your reputation begins with your response to the breach. Once the crisis has passed, begin rebuilding your brand and treat it as a learning experience to improve in the future. **NL**

LAURA M. TUCKER'S BIOGRAPHY CAN BE FOUND ON PAGE 6.