Closing the Barn Door
After the data breach

By Paul W. Ross, DE

In many of my previous articles, I have discussed the issues of making your computer systems secure using proper passwords, the joys of encryption, and a raft of strategies for keeping the barbarians from the gates.

Well, what do we do if the barbarians make it past the moat full of alligators and my dog? What do we do if our databases are breached? Bad things happen—apparently pretty often, if you read the newspapers. As they say, Bad news sells, and worse news sells better.

When disasters like this strike, it is a very human inclination to simply deny that there is a problem. You can see what this strategy got the Tokyo Electric Power Company with its reactor meltdown after the earthquake and tsunami! If the company had been more forthcoming from the beginning, both its credibility and the outcome might have been better.

When the truth finally comes out, it is often worse that you hid the problem than the actual problem itself. Keep in mind during this discussion that I am not a lawyer, nor do I play one on television!

Assuming that we have had a serious data breach, we need to reduce the harm to our employees, clients, and vendors.

We need to ensure that the same perpetrator does not strike again. In addition, financial institutions and telecommunications companies are required to preserve certain data for regulatory purposes, which can add to our problems. That means that because of the nature of their business, they have more sensitive data than is normally the case. Of course, we save things “just because we can.” That is a topic for another article.

It is much better in both the short and long run to be up front about a data breach. We need a playbook and a workable strategy for dealing with a security breach. When we address the problem to our clients or to the public, we should put forward the following ideas:

• How the problem arose
• What holes the security breach introduced (and what it did not)
• How those holes can be closed
• What is being done to prevent this from happening again

As important as it is to comply with the various laws and regulations concerning data protection and retention, it is also fundamentally important to prepare ourselves for breaches of sensitive information. Work under the assumption that it is
going to happen somewhere along the line.

Most organizations today follow a series of best practices for notifying individuals when their information is breached. Organizations need to focus on both mitigating the business impact from the data breach and complying with laws. This is simply good risk management.

Most organizations choose to be proactive in notifying individuals in an effort to reduce the damage to brand equity and customer opinion. Also, laws in many states require organizations to notify consumers under certain circumstances.

State laws vary in their definition of what kind of incident requires notification. Some state laws require notification to be triggered by the simple fact that information is lost. Others require notification to be triggered only when there is a confirmed risk posed by the data loss. Also, in some states, triggers differ based on the kind of organization that breaches the information. For example, for-profit corporations, government agencies, and even financial institutions may have greater or lesser legal obligations to notify individuals. You are well advised to have a clear understanding of your obligations, especially if you do business in different states. Err on the side of caution and take an open and proactive stance. Protect your brand! 😐