BY DAVID ZETOONY & LOUISE NUTT

Managing Data Breaches

DATA BREACHES ARE COMMON: more than 300 major breaches involving more than 100 million consumer records are reported each year. Almost every breach is unanticipated and extremely costly (studies indicate that companies often pay between $50 and $79 per lost record).

Like most companies, franchisors have significant quantities of sensitive data that often includes information on customers, employees, and their franchisees. Franchisors face an additional obstacle: their franchisees often collect large quantities of sensitive data about their customers and their employees. When franchisees experience data security problems, those problems often have a ripple effect that creates severe reputational (and often legal) costs to the entire franchise system.

Promoting good data security practices internally—and among franchisees—is essential. The following steps may help reduce the chance of a data security breach occurring in the first place, and the costs of dealing with a breach if (or when) one does occur.

1. Have an up-to-date security policy. Many companies (including franchisors) do not evaluate security risks regularly. Every business should consider evaluating its data security policy at least annually. Reviews should include how the business is collecting information, the types of information being collected, what steps have been taken to keep that information safe, and internal policies regarding use of technology. An annual review is a good time to consider new (and old) technological threats. For instance, a good security policy should take into account where breaches occur. Consider the following rough breakdown of the types of breaches, and ensure your security policy addresses each:

- 40 percent laptop thefts (half stolen outside the company, half stolen inside);
- 20 percent human or software error;
- 15 percent non-laptop theft;
- 15 percent hackers; and
- 10 percent employee intentional acts.

2. Train franchisees on data security. The FTC recently suggested that a company can be held liable for giving sensitive information to another company that does not employ good data security practices. This raises the question of whether a franchisor is liable for a franchisee that does not use good security practices. Although this legal issue is currently the subject of debate, as a practical matter the bad security practices of a franchisee can be devastating to the business reputation of the entire franchise. As a best practice, provide routine training to franchisees on topics such as 1) recommended procedures for data disposal of data, 2) data security, and 3) mandatory and recommended procedures for responding to data security incidents—in short, any situation that might involve an unauthorized person getting hold of sensitive data.

3. Require franchisees to notify you of security incidents. Often, franchisees do not have the expertise or knowledge to properly investigate and respond to a data security incident. To protect the brand and to ensure that data security incidents are handled quickly and appropriately, franchisors should consider requiring franchisees to report data security incidents to them immediately, to fully comply with any legal obligation to investigate the incidents, and, if legally required, to report the incident to governmental authorities and consumers.

4. Create a consumer notification policy. Almost every state has passed a statute requiring companies to notify consumers in certain instances in which data becomes "breached." Most notification statutes, however, provide that if a company creates a policy for notifying consumers consistent with the law's "timing requirements," then a company complying with its own policy will be "deemed" in compliance with the statute. Fashioning a recommended notification policy for all franchisees, in addition to a policy for internal reporting and procedures, can help avoid some of the largest costs associated with consumer notifications. For instance, a data breach notification policy may provide that a company can alert consumers of data security breaches using email instead of regular mail.

5. Keep a written chronology of the breach. The hours and days following a breach are usually hectic. Few franchisors or franchisees keep a formal log of what the franchisee or franchisor knows, and when the information was discovered. Have your attorneys (or whomever is investigating the incident) keep a detailed written chronology that can form the basis of what may ultimately become an incident response report, which can save countless hours reconstructing the events.

Conclusion

Perhaps the most important rule to keep in mind in the context of data security is to learn from past incidents, and to continually re-evaluate how you and your franchisees protect information and respond to security events. Setting time aside each year to reassess your overall security practices, and time after each security event to consider where the company responded well, and where the company's response could be improved, can save a large amount of time and money down the road. ■

David Zetoony *is an attorney at Bryan Cave LLP in Washington, D.C. He has assisted dozens of companies to respond to data security incidents and government investigations resulting from data security breaches, and is the co-author of* Data Security Made Simpler, *a publication of the Council for Better Business Bureaus. Contacted him at david.zetoony@bryancave.com. Louise Nutt is an attorney at Bryan Cave in Los Angeles. She can be contacted at louise.nutt@bryancave.com.*