Cybersecurity and Franchising

Breaches can transform a business headache into a legal nightmare.

BY LEE PLAVE, CFE

FOR 238 YEARS, THE men and women of our country's armed forces have faced down threats. They remain on the front line protecting our physical security. But threats have evolved, and in the digital world in which we all live and transact — we are all on the front line in ongoing cyberattacks against our businesses and against our own selves.

To address our strategic national interest, the U.S. Dept. of Defense launched the U.S. Cyber Command, part of the U.S. Strategic Command. Still, the threat is so considerable that despite the best efforts of CYBERCON, we all still face the daily risk of cyberattack.

As business owners, we know that the task of securing our own operations can seem daunting. But the best way to proceed is to take this methodically and in pieces, as suggested by the old adage "how do you eat an elephant — one bite at a time." Merely because cyberattack is so pervasive doesn't spare companies of the need to be reasonable and vigilant in protecting their data and, ultimately, their market position and brand name. Besides, offering up a "nobody-cares" defense because "it happens to everyone" violates George Washington's maxim on excuses: "It is better to offer no excuse than a bad one." And law enforcement authorities, from state attorneys general to the Federal Trade Commission, may be particularly unmoved by businesses that try to assert that defense.

From a brand perspective, data breaches may represent an existential threat to the viability of an entire franchise network, including the party that suffered the data breach as well as of the franchisees and the franchisor who fly the same flag.

From a legal perspective, data breaches may result in the liability and exposure to lawsuits from customers, law enforcement authorities and shareholders, especially if the victim is a publicly traded company, and the PCI Security Council. When breaches happen where the business didn't take reasonable and relatively simple precautions, or where the business did not keep a promise made to its customers, that can transform a business headache into a legal nightmare.

Here are some practical tips to get your arms around the cybersecurity issue:

1. **Assess Your Organization.** Engage professional assistance to help identify vulnerabilities and determine what reasonable steps you can take to secure your data and maintain that security. Tom Epstein, CFE, CEO of Franchise Payment Network, said that more than simple precautions are needed and that a full assessment is in order.

2. **Be Aware.** The vulnerability isn't limited to point-of-sale systems. In a recent interview, Epstein observed that most POS systems are Payment Card I-compliant, but the rest of the chain needs to be considered. For example:

   - While your credit card processor is probably PCI-compliant, how is transaction data transferred to your vendors?
   - Are the routers in your retail locations properly set?
   - Is there one router for the store that handles both back-of-the-house transaction data and also front-of-the-house Internet access? (Hint: there should be separate networks).
   - Is credit card information taken by hand (e.g., a scratch pad next to the phone) and, if so, how is that information handled and physical copies destroyed?
   - If you decide to adopt mobile payment systems (e.g., Apple Pay, Google Wallet, Level Up) are you doing so properly and professionally?
   - Do you have any franchisees who take payment or collect other data by unauthorized means?
   - Have you installed and updated proper anti-virus (and anti-malware) software on all of the computers that operate within your network in the franchisor's offices, as well as those in the franchisees' offices? (These can be the first line of defense against the unbelievably high volume of malware that can come into the system through attachments to innocuous-looking e-mails.) Also address in the same way the computers and mobile devices that

(Continued on page 24)

(Continued from page 22)

your team (and your franchisees) use to remotely access their office computers.

- Does your staff (and that of your franchisees) use the same tablet to surf the Web (translation: more vulnerable to viruses) as it does to conduct business and record customer data (which would make the data equally vulnerable to attack)?
- Do you properly back-up your data so that a cyberattack won't be cataclysmic? Where is the back-up conducted and is any physical media kept securely (e.g., tape drives, hard drives)?
- Are all passwords used to access the system appropriately complex and changed frequently?
- Do you limit, and run through a malware and virus screen, the data that your vendors share with you (and that you share with your vendors)? (Bear in mind that the hack on Target reportedly came into the system through an HVAC contractor.)

3. **A PCI compliant vendor isn't the end of the inquiry.** Epstein says that each time there is a major breach, vendors release security patches that have to be downloaded and installed not only to remain PCI-compliant, but also to close the window on major vulnerabilities. Those patches need to be downloaded and installed so that the POS systems that were PCI-compliant when purchased stay that way. The PCI Security Council, run by the banks that issue credit cards (including American Express, MasterCard, and Visa), is vigilant about making sure that businesses, including retailers, take the proper actions at every step of the way, not just when they purchase a POS system. In fact, the PCI Security Council has the power under its contracts with merchants to fine those who fail to take reasonable actions to safeguard data.

4. **Set a Policy.** Franchise systems ought to have a data policy, set by the franchisor that sets out standards appropriate to the system. All of the points noted above should be addressed, but there will inevitably be differences in each system. For example, a network of franchises in the food-service business may have one set of concerns, but those concerns are vastly different from those in a home health care franchise. Among other things, a proper policy will address the data that is needed and that should be collected, and what data should never be collected. What antivirus programs are to be installed and on what devices? What emails should never be opened? How data should be used and maintained, and under what conditions may the data be transferred? Are franchisees responsible to report data breaches to the franchisor so that remedial action can be taken swiftly?

5. **Train the System.** In a franchise system, all of the stakeholders — the franchisor, franchisees, all of their respective employees, vendors, etc. — need to be trained about the standard and the data policy. Field operations teams need to be especially attuned to the issues so that they can check on these issues during their own on-site visits and report on vulnerabilities that should be double-checked to prevent breaches. (When those steps are completed, repeat the training process – which is akin to painting the George Washington Bridge between New York and New Jersey, a process that starts in one spot, takes time to be completed around the perimeter of the bridge, and by the time of completion, needs to be restarted.)

6. **Learn More.** Keep abreast of the issues. Here are few helpful resources:

   - The International Franchise Association has launched a collaborative effort with the National Cyber Security Alliance. Additional information can be found at http://www.franchise.org/Franchise-News-Detail.aspx?id=63102 and at www.StaySafeOnline.org.
   - The PCI Security Standards Council (www.pcisecuritystandards.org) provides extraordinary information for merchants, and sponsors webinars to help keep merchants up to date on threats.
   - The Electronic Transactions Association (at http://www.electran.org) is also an outstanding and expanding resource.
   - The Verizon Data Breach Investigations Report (http://www.verizonenterprise.com/DBIR/2014) is an excellent compendium of data on breaches, why they occur and steps businesses can take to mitigate the brand and legal risks.
   - For hints on creating strong passwords, visit the Boston University Information Security and Technology Dept. website: http://www.bu.edu/infosec/howtos/how-to-choose-a-password/. ■

Lee Plave, CFE, is one of the founding partners of Plave Koch PLC, an entrepreneurial law firm based in northern Virginia just outside of Washington, D.C. Find him at fransocial.franchise.org.