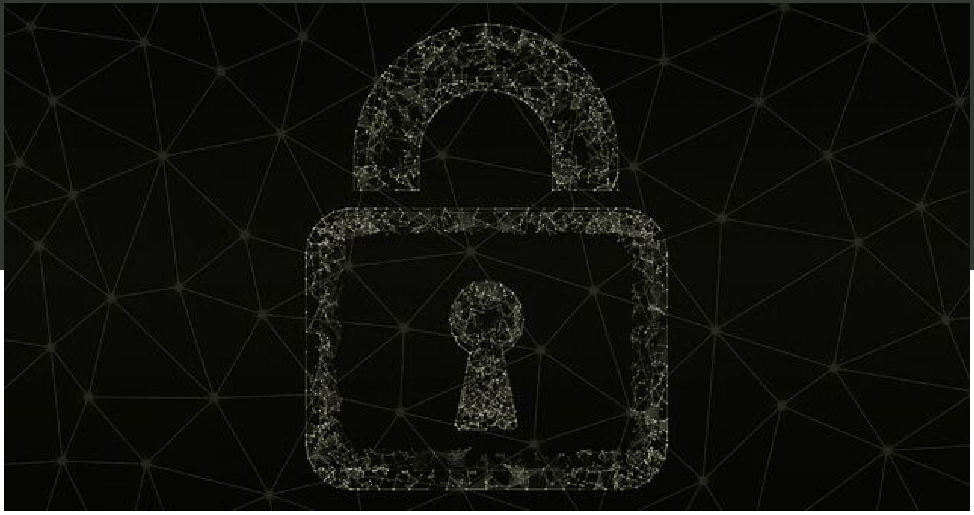
F P L G
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

Nonprofits and Cybersecurity: Make it a Priority

11.30.16 | Linda J. Rosenthal, JD



Not long ago, Harvard University was hacked. So was Penn State University. But they are huge institutions – you may be thinking – likely to interest cyber thieves.

That may have been the mindset of the directors of the Utah Food Bank until – in a single data breach – hackers stole personal and financial data of over 10,000 donors: names, addresses, email addresses, and credit card numbers.

Hacking is big news these days. There is a false belief that cyber threats are aimed at major businesses, governments, news organizations and other political targets. The reality is sobering: The risk is much more widespread, and has devastating consequences, financially and legally. "Cyber threats are a factor for any organization with digital record-keeping. Hackers do not care what you do, only whether you have records they can harvest."

As part of any nonprofit's ongoing risk management strategy, cybersecurity should now be near the top of the list. That means getting informed about: the nature and extent of the threat; what precautionary steps are available, including possible insurance coverage; and the organization's responsibilities under law. Many states, including California, have laws on the books requiring action by any entity that was hacked and where outsiders' data has been compromised.

Resources on Nonprofits and Cybersecurity

Recognizing that this a daunting issue for most people who are not cybersecurity experts, there are, nevertheless, many useful introductory articles and publications. Here are just a few:

- Feeling Insecure About Security? Protecting Your Nonprofit's Data is Not Rocket Science
- Cyber Security for Not-for-profits

- Cybersecurity for Nonprofits: How to Protect Your Organization's Data While Still Fulfilling Your Mission
- Cybersecurity & Nonprofits: A Matter of Time?
- 8 Tips for Better Nonprofit Cyber Security

Laws Applicable to Cybersecurity

In 2002, California took the lead in addressing the duties of hacked entities and government agencies; they must give notice to victims of data theft. Since then, most other U.S. jurisdictions and many nations around the world have adopted similar laws.

California has, from time to time, updated its data security breach notification laws; the most recent were amendments effective January 1, 2016 to California Civil Code sections 1798.29 and 1798.82. "These amendments represent significant changes to [these] security breach notifications provisions. In particular, they impact how to respond to security breaches, how to protect personal information and the scope of what information is protected."

All Californians, including consumer customers, employees, and residents of California, are covered by these amended laws. Although residents of other states or countries are not expressly granted protection, as a practical matter, "the California law has caused millions of people outside California to receive breach notifications. The data protected includes "personal information" which is defined to include an individual's first name or first initial and last name in combination with any one or more of the following data elements: (a) social security number; (b) driver's license or CA identification card number; (c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (d) medical information; (e) health insurance information; and (f) information collected through an automated license plate recognition system.

The data breach notification is not required if either the name or other data elements are "encrypted." The new law defines the term "encrypted" to mean "rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security."

The website of the California Attorney General includes information including a sample security breach notification form.

Conclusion

"No nonprofit or business is too small for hackers to notice. The fact is, small nonprofits often make perfect targets precisely because they are not protected by security teams like many large companies are. Additionally, if your nonprofit has any type of online presence, it can be penetrated using software that scavenges the internet and sends out automated attacks without requiring the hackers to have any prior knowledge of the targets."

All nonprofits should make cybersecurity a priority, setting a tone for the organization to take it seriously, develop data security policies, provide cybersecurity training for all directors, officers, and other personnel, and consider buying cybersecurity insurance coverage.

— Linda J. Rosenthal, J.D., FPLG Information & Research Director