Professor Emeritus, Saunders College of Business, Rochester Institute of Technology

Do Nonprofit Directors Face Cyber Security Risk?

Huffington Post -- Posted: 04/26/2015 2:43 pm EDT Updated: 06/26/2015 5:59 am EDT

The cyber security (CS) debacles faced by Target, Sony Pictures and others may seem far afield from the concerns of nonprofit directors, except for the giants in the area, like AARP. However, think about this hypothetical scenario.

A group of high school students hacked into the computer system of a local nonprofit offering mental health services and gain access to records of clients, perhaps even placing some of the records of other teenagers on the internet.

What due care obligations did the board need to forestall the above situation? A move to recruit directors with special expertise in information technology or cyber security would be nonproductive. A nonprofit director has broader responsibilities such as the overview of management, approval of budgets, fostering management and staff growth etc. Similarly, when social media became a prominent issue a few years ago, boards debated the advisability of seeking directors with that specific kind of background. Today, a consult with management is likely to provide guidance to directors on these issues.

After listening to a group of cyber security experts discuss for-profit challenges in this area, I have the following suggestions on how nonprofit boards might respond to similar types of challenges.

1. *Carefully "wall off" all confidential information* -- Have management be certain that private information such as health records, are encrypted and separated from operating data that may be considered public in a nonprofit environment.
2. *Review D&O and other liability policies* -- Determine whether or not the D&O policy protects directors and managers from CS intrusions. (It likely does not, but I understand that some carriers may offer some protection along with smaller policies.) It is clear that most general liability policies do not protect the organization against CS.
3. *Board Encouragement* -- Devote some meeting time, perhaps 10 minutes, to a discussion of the CS topics so that management and staff are aware of the board's concerns on the subject and will take action when necessary. Appropriate due care actions like frequent password changes should become routine. Some checklists are available online, suggesting questions directors might pose to raise awareness on the topic and avoid potential CS breaches.
4. *Can third party payer help?* -- Many nonprofits deal with third party payers with sophisticated CS systems and may offer the nonprofit some advice or assistance.
5. *Education and training of employers* -- Many CS crimes have been successful because employees have violated or forget to effectively protect their working accounts and information. Proper education and training can help reduce these types of lapses.
6. *Finance & Audit Committees* -- Current data indicate that only 24% of nonprofits have a standalone audit committee and 47 percent have a combined finance/audit committee. * In my opinion, neither of these committees have time or expertise to help the nonprofit board stay on message in regard to CS problems.

If a nonprofit, like the one described, is attacked, not only will records be compromised, but also the reputation of the agency will be destroyed, probably along with the nonprofit organization itself. Sony and Target may be able to survive such an attack, but the typical nonprofit may not.

*BoardSource (2015) "Leading With Intent: A national Index of Nonprofit Board Practices," January.

Follow Eugene Fram on Twitter: www.twitter.com/@eugenefram