VIS® CONNECTIONS

January 2012

We are happy to provide you our publication for nonprofit risk managers, as part of our service to you. The titles in the contents section link directly to their articles. If you need to change the email address to which this is sent, please contact us. Be sure to include your name, organization and address. You also are welcome to call us at 800.222.8920 for assistance.

In this issue…

Do no harm—Protecting employee and volunteer data

By Matt Cullina

Editor's note: *Matt Cullina is chief executive officer of Identity Theft 911 (www.idt911.com), which provides data risk management, identity theft recovery, data breach recovery, and other services. The firm has offices in Scottsdale, AZ and Providence, RI. Mr. Cullina has 15 years of insurance industry management, claims and product development experience. He spearheaded MetLife Auto & Home Insurance Company's personal product development initiatives, managed complex claims litigation and served as a corporate witness for Travelers Insurance and the Fireman's Fund Insurance Co. We appreciate his contributing this article to VIS Connections.*

When physicians begin practicing medicine, they vow not to harm their patients.

Managers at nonprofit organizations have the same professional responsibility, especially after collecting personally identifiable information. Administrators ought to be committed to protecting their employees and volunteers from identity thieves and steadfastly guarding that data. Based on Identity Theft 911's experience helping insurance clients respond to data breach incidents, breaches occur most often due to security lapses by management.

Solid foundational practices for securing data aren't difficult to implement. They don't have to be expensive or time-consuming. And they can reduce risk exposure.

The true cost of lax security

At most organizations, managers are focused on an array of issues. Data security isn't always a priority. However, they should treat data as carefully as cash receipts, because losing data could result in hefty response costs.

Proactive security measures reduce the risk of a breach; provide staff with a basic understanding of data systems, inventory and backup processes; and are significantly less expensive than *reactive* costs. For small to medium-size organizations, proactive steps may run between $2,500 and $10,000. When done reactively, costs could run anywhere from $15,000 to more than $50,000, depending on the extent of the breach.

Forty-six states and the District of Columbia have enacted laws that mandate how organizations must respond to a data breach. Those requirements can lead to significant costs in the event of a large data theft.

The main intent of the laws is to ensure that organizations notify affected parties about a breach. A notification letter can be drafted in-house. But a legal review of the document to ensure that it complies with state notification requirements could run between $1,500 and $2,500. And printing and mailing costs range between $1 and $2 per letter. If 10,000 people are affected, that adds up to $10,000 to $20,000.

The type of data stolen also could drive up response costs even more. Identity thieves armed with stolen Social Security numbers can open new lines of credit and wreak havoc on victims' credit records. Under those circumstances, victims would benefit from credit monitoring, which runs between $25 and $100 per victim who signs up for it. Not all will. But if only 10 percent of 10,000 people affected by a data breach opt for the service, an organization would incur $25,000 to $100,000 in credit monitoring costs.

Technically, state data breach notification laws don't require organizations to offer credit monitoring, and state attorneys general have no authority to mandate it. But they could pressure organizations, which have to consider their reputation, to offer the service.

Best practices to secure data

.

Organizations lose staff members' and volunteers' private data in different ways—all easily avoidable. Whether it's a misplaced box of paper files, a stolen laptop or a missing smartphone, managers should keep their eye on the ball by following best practices to securing information.

The first step to take is to outline the process for receiving and handling sensitive data. What information do you have? Who has access to it? How is it stored, protected and destroyed?

This assessment may be done internally or by a contractor who has expertise in data risk management. Typically, outside firms are more familiar with the threat environment, risks, policies and procedures, as well as best practices associated with different organizations. They can also create a data risk management plan, which can reduce exposure to sanctions and litigation.

Here are five basic security measures to better protect data:

1. **Shred it.** Identity thieves get birth dates, driver's license numbers, Social Security numbers and other data by Dumpster-diving or going through recycling bins. Use a crosscut shredder to destroy paper files containing sensitive data.
2. **Lock it up.** File cabinets, file rooms or other areas that store documents containing private data about clients, staff members and volunteers should be locked.
3. **Use password-protection and encryption.** *Always* encrypt sensitive information. Inexpensive or even free encryption functions are readily available. Create strong passwords for smartphones and laptops; change them quarterly.
4. **Properly dispose of electronic devices and tools.** Implement policies on how to destroy old computers, disks, tapes, CDs, memory devices and any other equipment that may contain sensitive data. It is often best to physically destroy the devices when they are no longer needed.
5. **Screen all employees and volunteers.** Implement hiring practices for all employees and volunteers, especially those with access to sensitive information. Use criminal and background screening companies. All staff members and volunteers who have access to sensitive information—including cleaning crews, technicians, administrative assistance, and temporary employees—should sign a confidentiality and security document.

Even if managers do everything right to secure data, something still could go wrong—as it has recently for Sony Corp. and Citigroup Inc. So the last line of defense is insurance. Cyber-risk policies are available to nonprofit organizations, large and small. More than 50 carriers offer cyber-risk insurance programs. Your insurance agent or broker can provide more information.

From bad to worse – Leadership lessons from a scandal

According to grand jury testimony, people associated with The Second Mile nonprofit organization in State College, PA had reason to be concerned several years ago that founder Jerry Sandusky might be abusing children. And yet, the pot kept boiling until last year, when revelations led to the arrests, criminal investigations and resignations that have dominated the news. Now the organization is laying off staff, acknowledging the drastic reduction in financial support that has resulted from the scandal, and is struggling to survive.

As terrible as the Second Mile situation is on so many levels, there are lessons for nonprofit organization managers and boards, that might prevent such an implosion elsewhere – regardless of the organization's mission. The key is to understand how failures in leadership, communication and board structure can take an organization from bad to worse, often in increments too small to notice. You might want to take the opportunity to audit your own organization's practices, for any of the kinds of traps described in this article.

"Founder Syndrome"

The Second Mile bylaws actually provided for a position of "founder," who of course was Jerry Sandusky. Michael Wyland, whose Sumption and Wyland firm in Sioux Falls, SD provides consulting services for nonprofit organizations, points out that the powers of the founder as expressed in the bylaws actually conflicted with the powers of The Second Mile's vice chairman, on the issue of who would lead meetings in the absence of the board's chair. More serious than the bylaws conflict, however, was the board's abiding deference to Sandusky.

"Board members often develop a blind spot to the governance issues in their care, instead focusing on the founder as embodiment of the mission," Wyland says. In organizations with an active founder, he adds that "founders have to be careful to recruit board members who are faithful to the nonprofit organization's mission and who will serve the community as well as the organization. Potential board members need to understand that, by accepting nonprofit board service, they are accepting legal duties to a corporation and to the community which are independent of the founder and his or her wishes or interests."

While the culture of deference to the founder might have been at the root of the Second Mile "blind spot," Wyland also observed several structural flaws or potential flaws in the organization, of the kind that could lead to problems in any nonprofit organization. For example:

- The CEO's spouse also was employed by the organization. According to the Charitable Organization Registration Statement filed with the Commonwealth of Pennsylvania, the CEO was responsible for distribution of contributions, while his wife was responsible for solicitations. "Husbands and wives should avoid sharing responsibility for both the income and expense associated with a nonprofit corporation, especially one with a multimillion dollar budget and significant assets," says Wyland. Also, Internal Revenue Code Section 4958 has strict requirements aimed at preventing a conflict of interest that might result from such a relationship, and the nonprofit's board is responsible for monitoring compliance.

- Publicly available information indicated that the CEO had other employment, including consulting relationships, while at The Second Mile. Employment policies, and any employment contract, should specify to what extent other employment is permissible.

- The bylaws did not limit the number of terms a board member could serve. (And the "founder's" status was continuous.)

- The board had 36 members, which Wyland points out can be too many for the board to act in concert on issues effectively, which often means that the executive committee deals with issues that really deserve the entire board's attention. Nine to 15 members is a better number.

- There was an "honorary" board, but some of its members told the media that they were unaware their names were being used by the organization in this way.

No, let's DO talk about that.

Following the revelations in State College, including the fact that red flags had been ignored or responded to poorly for years, Wharton School professor John R. Kimberly decided to explore the question, "Why do people with integrity behave differently within an organization than they would on their own?" His interviews led to the following conclusions, all of which underscore the need for unfettered communication within an organization:

- People who know about a problem often have limited information. In that situation, they might question their understanding of the problem, or believe that the problem is minor and will resolve itself.

- People often are afraid that if they speak up they will be ignored or misunderstood -- or even punished for questioning authority or being disloyal to the organization.

- Sometimes the system for reporting problems is weak or nonexistent.

- People might know of a problem, but consider it someone else's responsibility to solve.

- When issues are raised, sometimes blame is assigned too quickly, thwarting the kind of thorough investigation that is needed, and creating resentment.

- Sometimes problems are expressed in such ambiguous language that their true nature is obscured. For example, Penn State assistant football coach Mike McQueary testified that he never used explicit terms to describe to Coach Joe Paterno a sexual assault by Sandusky that McQueary said he witnessed in 2002, "out of respect" for Paterno. Also, Paterno testified that he "didn't push Mike to describe it because he was already upset."

- People sometimes fear that confronting a problem will damage the organization, and the people to whom they feel close. Cristina Bicchieri, philosophy professor at the University of Pennsylvania who also teaches business ethics at Wharton, said, “The cozier and more close-knit the group, the less incentive you have to stir the waters. If you are strongly motivated by the sense of not wanting to ruin the group, you might form a false belief about what happened, especially if the situation is ambiguous.”

- Senior management, consciously or not, sometimes creates the impression that certain topics are taboo. As Los Angeles management consultant Don Rossmore told Professor Kimberly, “When an issue is undiscussable, it cannot be managed rationally.”

It is up to an organization’s management to make sure everyone understands and upholds the organization’s values, and understands that no topic is taboo, even if discussing and exploring it might reveal a failure, a need for improvement, or even a wrongful act on management’s part. The survival of the organization, and the well-being of individuals the organization serves, can be at stake.

Guidance on insurance for ride-assistance programs

A great many nonprofit organizations, perhaps yours included, have established ride-assistance programs for their clients, or are thinking of doing so. Questions often arise about the appropriate kinds of insurance for that kind of risk exposure, because some organizations own vehicles while others do not; some lease or rent vehicles; some have employees as well as volunteers who drive, etc.

Not only do nonprofit organizations often have questions, sometimes insurance agents and brokers are not aware of all the available options themselves, including the unique VIS® excess automobile liability program that protects volunteer drivers with up to $500,000 above the liability limits of their own auto insurance. For that reason, we recently contributed a blog post to *National Underwriter* magazine’s Website, outlining the primary considerations for protecting nonprofit organizations that have ride programs, and their volunteers.

You can read that article here -- http://bit.ly/xJYKeG. If you have colleagues who might find the information useful, we hope you will forward the link.

The VIS® excess automobile liability coverage can be valuable not only for ride-assistance programs, but for any volunteer-based organization whose volunteers drive – including driving themselves to and from the places where they volunteer. The coverage applies from the time the volunteer leaves home until he or she returns home, as well as during volunteer work. More information is in the “Volunteer Center” at www.cimaworld.com, or you are welcome to email Vicki Brooks or Joan Wankmiller or call them at 800.222.8920.

What donors want to know

They want to be satisfied that your organization is legitimate, they want to see your key financial information, and have enough information about what you actually have accomplished to be convinced that you will use their contribution effectively. Those are the primary findings of “Money For Good II”, a follow-up to the 2010 GuideStar Money For Good study on motivations and behaviors of individual donors, donor advisors, and grantmakers. The reason we are including a mention of the study in this risk-oriented publication is that failure to attract or retain supporters is a risk for nonprofit organizations.

As we have mentioned before, taking the time to complete a robust Form 990 is one way to manage this risk. Now comes GuideStar’s new report, which estimates that as much as $15 billion contributed annually to charitable organizations could be redirected to the highest-performing, most effective ones -- if only those high performers did a better job telling their story.

The study, available on the GuideStar Website, found that about one-third of individual donors do research before writing the check. Of those, most spend less than two hours gathering information – primarily to make sure their contribution won’t be wasted. As one participant in a focus group said, “I can’t determine which is the ‘best’ nonprofit, but I can find out if a nonprofit is bad.” The donor advisors and grantmakers, on the other hand, research almost every potential contribution, and put more emphasis on the measurable impact the nonprofit is having.

One of the appendices in the study identifies six basic categories of givers, and the “core drivers,” or motivations, for each. It might be helpful to note the percentage of all givers represented by each type, and what motivates them:

- *Repayers* (23%) – Support their alma mater, or organizations that have helped them or a loved one directly
- *Casual* (18%) – Give to well-known organizations
- *High Impact* (16%) – Give to organizations they perceive as doing the most good
- *Faith-based* (16%)
- *“See the Difference”* (13%) – Give to local charities, or small ones where their contributions will make the most difference
- *Personal* (14%) – They know the people involved

Resources

GuideStar – www.guidestar.org

Charting Impact – www.chartingimpact.org – Developed by the Better Business Bureau Wise Giving Alliance, GuideStar and Independent Sector, as a common framework for communicating vital information about nonprofit organizations’ mission and accomplishment.

CIMA service team for VIS® members

Volunteer insurance:
Victoria W. Brooks, Account Executive
Joan R. Wankmiller, Account Executive

Directors and officers liability:
Aaron Jones, Account Executive

Laurie S. Coleman, Senior Vice President

Toll-free: 800.222.8920 or 800.468.4200

We are always happy to serve our members. Please let us know, any time we can be of help!

VIS® Commitment

Volunteers Insurance Service is committed to providing its members a complete resource for the nonprofit organization's risk management needs. Our services include:

- Publishing ***VIS® Connections*** as one of our information resources for members;
- Maintaining for members' use a library of information relating to management of risks in the nonprofit organization;
- Researching available and appropriate insurance relating to volunteer activities;
- Designing and administering insurance programs, and compiling underwriting information;
- Providing consultation on risk management issues at no additional charge to our members, via a toll-free line (800.468.4200);
- Assisting members, on request, with matters relating to insurance.

Insurance and administrative services are provided to VIS® and its members by The CIMA Companies, Inc. and/or one of its affiliated companies.

VIS®'s Articles of Incorporation, Financial Information, and a list of the members of VIS®'s Board of Directors are available to VIS® Members upon request.

CIMA licensing information

The following licensing information is being provided in order to comply with state governmental regulations:

Volunteers Insurance Service Association, Inc. is a risk purchasing group formed and operating pursuant to the Liability Risk Retention Act of 1986 (15 USC 3901 et seq.)

Notice to Texas clients: The insurer for the purchasing group may not be subject to all the insurance laws and regulations of your state. The insurance insolvency guaranty fund may not be available to the purchasing group.

Notice to California clients: License #0B01377 and #0A06046, CIMA Companies Insurance Services

Notice to Minnesota clients: License #009285 and #07544084, The CIMA Companies, Inc.

CIMA, one of its subsidiary companies and/or an authorized individual is licensed in all jurisdictions. Please contact CIMA at 800.468.4200 if you would like information about our licenses.