VIS CONNECTIONS

 Spring 2015

We are happy to provide you our publication for nonprofit risk managers, as part of our service to you. 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. For risk management guidance between the quarterly issues of *VIS Connections,* we invite you to follow our blog at www.volunteerinsure.org.

Bitter lessons at Sweet Briar

"We saw updates at each meeting, but were given little insight into the conversations and data behind them," wrote one alumna and former board member of Sweet Briar College, in an op-ed piece in *The Washington Post*.

Others with close connections to the all-female school near Lynchburg, VA have used both traditional and social media to claim that the board's decision in late February to shut down the school this August because of "insurmountable financial challenges" was reached with no attempt to communicate with stakeholders who might have had useful ideas about how to keep Sweet Briar viable.

Never in 114 years have the board and administration of Sweet Briar, with its 700 students and staff of 300, received so much attention, and not much of that attention has been good. Immediately after the board announced its decision to close, a Website and Twitter account – www.savingsweetbriar.com and #SaveSweetBriar – were launched. As of this writing, these

stakeholder groups claim to have raised $14 million toward a $20 million goal, even as they dispute the college's claim that the financial challenges are all that insurmountable.

The Amherst County, VA district attorney filed an injunction to prevent donor funds from being used to close the school – a case that has made it to the Virginia Supreme Court. One exhibit in the lawsuit is a thank-you letter written to a donor February 16 – just two weeks before the board's decision – that reads, "Estate gifts have played, and will continue to play, an important role in ensuring the strength of Sweet Briar College…"

That donor happened to be this year's commencement speaker. At that event in May, Columbus, GA Mayor and 1987 Sweet Briar graduate Teresa Tomlinson directly criticized Sweet Briar's leadership for its failure to engage bright people other than themselves. "If your ideas are so good…then test them against the critical eye of stakeholders," she said in her commencement address.

Whatever the merits, or lack thereof, of the decision to shutter the institution, its board made crucial errors that a fully realized risk management plan might have prevented:

- Lack of communication with stakeholders – and lack of disclosure, as indicated by the thank-you letter to Ms. Tomlinson -- meant that the decision took alumnae, staff, faculty and donors by surprise, and seemed precipitous.
- The Sweet Briar leadership did not anticipate the public relations mess (and three lawsuits) its decision would cause, indicating the lack of a disaster plan. Disasters aren't just about fires, floods, oil spills, criminal acts and product recalls. Proper planning asks, "What will our stakeholders think if we take this action? What will they *do*?"

"This kind of situation illustrates why boards must understand that part of being good fiduciaries is actively listening to constituents. An insular boardroom places the organization and the interests of stakeholders at risk," wrote Ruth McCambridge, who has followed the Sweet Briar case closely for *Nonprofit Quarterly.*

Would any of your stakeholders have a good reason to complain that your board makes important decisions without effective two-way communication between the board and the stakeholders?

The other side of the risk-perception gap

The Sweet Briar turmoil described above began when leaders mishandled their response to a threat that was not known to others. But communication failures also occur in the opposite configuration -- when leaders themselves are too far removed from a threat to see what others see every day. An article in *Hospitals and Health Networks* newsletter describes how a risk assessment team from Western Litigation identified this kind of "risk-perception" gap.

A new management team began implementing new procedures aimed at increasing patient safety, but was concerned that frontline employees seemed uninterested and even uncooperative. Interviewing those employees, the risk team learned that they had safety concerns of their own: security cameras in the employee parking lot and walkways had been out of order for years. Many had family members drop them off at work rather than park in that lot, or they arrived in groups so they could walk from the parking lot to the buildings together.

"The staff perceived that management had more concern for patient safety than employee safety," Pamela Popp of Western Litigation wrote.

Management was unaware of the staff's concern, or even the fact that the cameras didn't work, because they parked in a different area. Once they were notified, they installed working cameras, and the risk assessment team documented an improved attitude among employees, toward the new management team.

Preventing this kind of problem…New leaders need information!

The episode with the security cameras reminds us that when new senior staff or board members join an organization, those already on board can help both the new people and themselves, by communicating essential information about current projects. From The Indiana Nonprofit Resource Network (www.inrn.org), in its "Teamwork Tips and Trends" document:

"Most projects experience a change in executive, volunteer or team leadership, eventually. Be prepared with a status assessment, acknowledging contributions and successes. Welcome new perspectives. If the project takes a new course, take the lessons with you and make the next direction an even better choice."

Cybersecurity – Preventing the inside job

In March, a Frederick, MD man was sentenced to six months in federal prison for hacking into the computer system of his former employer, Service Coordination, Inc., a Frederick nonprofit that provides case management services for developmentally disabled persons. According to news reports, Alexander Afonso used a current employee's login information, without that employee's knowledge. Once inside the system, he emailed himself records of more than 11,000 clients of the organization – records that included Social Security, Medicare and Medicaid information, as well as other sensitive data of the kind that identity thieves buy every day.

In addition to implementing new data-security measures, Service Coordination had to notify all clients whose information was at risk, address individual concerns regarding the breach, and

provide a year of identity theft protection monitoring services for those clients. These are just a few of the expenses that can be incurred after a cyberattack, depending on the type of organization, the nature and extent of the loss, and state laws. Forty-seven states now require that those whose personal information might have been accessed in a security breach be notified. According to a study just released by the Ponemon Institute, the typical cost of the notification alone is $154 per record. Other expenses can include business interruption costs, loss of disaffected clients, the cost of engaging public relations professionals to mitigate damage to the organization's reputation, fines for regulatory violations, and legal defense in class-action lawsuits.

Nonprofit organizations can be just as much at risk of cyber threats as high-profile victims such as Sony.

"Protesting that 'no one would ever do such a thing to us; we're a nonprofit' is playing ostrich and burying your head in the sand," says Marilyn Donnellan, founder emeritus of Nonprofit Management Services, LLC who has served as an executive and consultant of nonprofit organizations for more than 30 years. She notes that nonprofits routinely house data that can be valuable to a hacker, including Social Security numbers, birthdays and other information on clients and staff, client health records, donor information and credit card numbers, and the organization's own financial records.

"Unfortunately, there are many nonprofits (especially smaller ones) that are so focused on providing programs they ignore critical risk management issues, including cybersecurity. All it takes is one significant breach of security for your reputation to be destroyed. Don't let it happen to your nonprofit," Marilyn says.

Hackers are targeting smaller organizations now. Security and technology firm Symantec's 2014 Internet Security Threat Report found that small and mid-size organizations accounted for 61% of targeted attacks in 2013, up 11% from the previous year. Still, many potential victims do not see the threat; Hartford's survey of small businesses found that 31% believe a cyberattack would have no effect on them.

Playing defense

In a recent article, Lisa Berry-Tayman of security consultant idt911 offered three suggestions for preventing cybertheft, including theft by insiders:

- **Access controls** – "No one person, including those in Information Technology, should have access to everything."
- **Policy and enforcement** – Make it clear to all staff, volunteers and contractors that anyone violating your policy on protecting confidential information will be subject to termination and lawsuits. "Enforcement is crucial to quashing ideas of information theft by a malicious insider."
- **Layered approach** – *Security controls and technology* are to protect the

organization's information from the outside world. *Privacy policy* dictates what information is collected and used. *Governance* determines how that information is used within the organization. "If Sony had done this (layered approach), perhaps Brad Pitt's phone number wouldn't be circulating on the Internet," Lisa writes.

Marilyn Donnellan emphasizes the importance of educating the board of directors, in terms that members understand rather than technical jargon, about how cyberattacks can occur, and the threat that they represent to the organization. "Without the knowledge, board members will not recognize the critical importance of the issue and will be less willing to approve cyber security as a line item in the annual budget," she says.

Insurance

Cybersecurity insurance policies are available to help pay the cost of recovery from a cyberattack. Because those recovery costs can be significant, even for small organizations, a policy is worth considering. If you need more information, please contact VIS Executive Director William Henry at 800.222.8920.

The insurer will require that you maintain minimum standards, specified in the terms and conditions of the policy and/or your application, to protect your confidential information. An insurance company is contesting a $4 million claim by a California healthcare provider whose patient records were compromised, for alleged failure to meet those requirements. Read the policy exclusions carefully. Cybersecurity policies are evolving, so there can be significant differences in coverage, as well as in cost.

Resources

All Things Data Breach is a LinkedIn discussion group.

The Identity Advocate and idt911 are among the providers of identity and data protection, fraud prevention and other security services. (VIS has no relationship with either.)

Paying the cost to have no boss

"Holacracy" sounded like a great concept. No one at Zappos, the huge online clothing and accessories retailer, would supervise anyone else. Employees would meet in "circles," as equals, and decide among themselves who would do what, and when, and how. It is an extreme example of "flattening" an organization, to empower employees to make their own decisions rather than simply follow procedures established by top management. The only problem was, as reported by the *Wall Street Journal,* 210 employees – 14% of the Zappos workforce – quit.

Some were disappointed that they had no opportunity to advance to positions with more responsibility and pay; many others grew tired of the time-consuming "circle" meetings. Zappos says Holacracy still is evolving. "It's not like turning on a light switch," a spokesman said. But the fact that it wasn't immediately and universally embraced suggests there still might be some value in having procedures, and holding everyone – including volunteers – accountable for following them. Anyone should be free to make suggestions that might influence those procedures, but everyone should follow what's in place at any given time.

Much has been said and written about empowering volunteers to decide for themselves how they will do their work, especially those who have had successful careers. ("If we don't do that, they'll leave! They're Baby Boomers, and expect to get their way!") From a risk management point of view, however, empowerment does not work. If volunteers (or paid staff, for that matter), do not have direction from you, they are likely to improvise, and the results might not be very good. We have had claims in our volunteer insurance program that resulted fromsuch improvisation.

So, establish and communicate your procedures (after inviting and considering volunteers' suggestions), and hold volunteers accountable for following them. Discipline or even terminate them if they don't. Sometimes in a close-knit organization, people can be reluctant to criticize others. However, that reluctance creates a risk, and it can hurt you.

Directors and officers liability – consider separate limits

If a lawsuit against your nonprofit organization names individual employees as well as your directors and officers, your policy limits could be depleted in defense of the employee(s)…unless you have separate limits just for your directors and officers.

Reserving separate limits of liability for directors and officers can provide vital protection if, for example, an employment-practices lawsuit names the executive director and the human resources director, in addition to the board. Typically, the additional limits would apply once underlying limits have been exhausted.

From the publication *D&O Compass:* "If D&O coverage is written with a $1 million limit, consider buying at least an additional $1 million dedicated limit for directors and officers, especially if the D&O limit is shared with the policy's employment practices liability and fiduciary coverages."

The insurance companies that CIMA and Volunteers Insurance Service Association represent offer such additional, separate limits on directors and officers liability insurance, for a very reasonable additional premium. For more information, please email **Aaron Jones** at CIMA, or call him at 800.222.8920.

The value of a volunteer's time -- $23.07 is the average

The average value of a U.S. volunteer's time was $23.07 in 2014, according to the newest report from Independent Sector. That value is based on hourly earnings of all production and nonsupervisory workers on private, nonfarm payrolls, as reported by the Bureau of Labor Statistics. The time values range from $19.31 in Arkansas to $39.86 in the District of Columbia. (Click the link above for a map showing the values for each state.)

While the Independent Sector values most often are used in volunteer recognition events and communications with supporters, they also can be used in financial statements and grant proposals, as long as certain criteria established by the Financial Accounting Standards Board are met. There is more information about that at http://www.fasb.org/pdf/fas116.pdf.

Whatever your volunteers do, and whatever Independent Sector or anyone else says is the value of their time, all of us at CIMA and Volunteers Insurance Service Association appreciate their work – and yours.

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 (800.222.8920 or 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.