10 Steps Nonprofits Should Take to Increase Cybersecurity

By Karen Schuler, CFE, IGP

Cybersecurity has become a top-of-mind issue for organizations across both the nonprofit and for-profit sectors. From the 110 million Target customers whose credit and debit cards were compromised in 2013 to the more than 250 million Google and Yahoo! email usernames and passwords that were exposed by Russian hackers last month, we're constantly bombarded by news of major companies being hacked and consumers' data being stolen.

Most Nonprofit leaders might ask themselves, "Who would want to hack my organization?" but recent ransomware attacks on U.S. hospitals send a clear message that few organizations are exempt from hacking activity. According to the 2015 NetDiligence Cyber Claims Survey, nonprofits made up 4 percent of cyber claims, while hospitals, listed as a separate category, made up 21 percent of claims—the most affected sector among those surveyed.

In fact, nonprofits are particularly vulnerable, given that they often retain vast amounts of donor information, including financial information as well as staff employment and insurance data. Many philanthropic organizations are operating under tight resource constraints, and cybersecurity measures may not have historically been a top priority. If you have not paid attention to your organization's cybersecurity policies, now is the time. Here are 10 steps that can help you better govern your information and assets.

1. Identify the Program Champion

Prior to initiating a program that helps to better govern your information and assets, it is extremely important to obtain sponsorship from those charged with governance and senior management. Without this, programs tend to be less successful. The goal of the champion is to help you make the business case to promote better cyber governance throughout the organization. Your champion will help you identify key stakeholders (such as the board of directors, managers, auditors, etc.) as well as individuals that could contribute to a committee, and will help to map out initial rules and procedures for making decisions related to an organization's data privacy and protection.

2. Assess your risks

Risk management is a team effort and should include representatives from Information Technology, Legal and Compliance, Human Resources, Accounting and Finance, and Operations. The risk assessment team's first project should be to inventory your organization's systems and data, ranking data types and systems by levels of importance and sensitivity. Following your inventory and vital records ranking, it is important to determine if one of your assets failed, if data was lost or stolen and whether HIPAA privacy rules were violated. For each of these potential threats, list ways to avoid or mitigate the risk, as well as the cost of each mitigation strategy and a plan to respond to an incident. In order to keep pace with changing technology, it's important that organizations review their risk management practices regularly.

3. Analyze your data

To help minimize risk, detect fraud and limit unauthorized exposure of your assets, organizations should utilize

analytics to help make reasonable assessments of risks and potential threats. Best practices are to take proactive measures periodically (or in reaction to non-specific compliance concerns) that involve the use of investigative techniques and limited legal and forensic accounting principles. A gap analysis can help you evaluate the efficacy of your organization's policies, procedures and controls to help you enhance protection and deter and detect compliance failures. It can also help you determine whether the organization conforms to best practices for the industry and for organizations of a similar size. Further investigation, including forensic technology or due diligence, can follow if it appears there is a high risk of compliance failures. This in-depth analysis provides insight into your organization's policy changes and, ultimately, when implemented, leads to improved controls.

4. Form a committee to develop the program

Once an organization has a cybersecurity program in place, it should also select a committee that can consistently oversee its implementation and meet regularly to determine its effectiveness and adjust the program as needed. This committee should include representatives from all key areas of your organization. It is also important to select one owner of the program to ensure that the team follows through with its responsibilities. Additionally, it is critical to determine roles, responsibilities, supporting personnel and materials, and individuals that should be consulted and informed of the committee's activities. Ultimately, this committee will build the organization's overall governance strategy, framework, policies, teams and processes to establish a strong data protection and privacy program.

5. Improve controls and governance strategy

Using the analytics and lessons learned, stringent internal controls need to be developed, implemented and monitored across the organization. Organizations should work with their technology, financial, operations and other teams to leverage analytics as they develop a data governance strategy, improve their compliance capabilities and deliver intelligence and consistent reporting throughout the organization. The committee should work across the different departments to build governance structures to distribute the roles and responsibilities of different participants in the organization.

6. Enhance efficiency and balance your investment

Organizational efficiency doesn't only result in long-term cost savings; it also reduces room for error, fraud and other cybersecurity issues. There are several steps an organization can take to increase its efficiency, including enhancing automation to reduce manual processes that are subject to mistakes and subjective evaluations. While implementing these processes involves an initial cost, in the long term, increased efficiency can help to limit expensive losses, improve consistency across the organization and reduce redundancies throughout operations, technology and file storage. Finally, we have found that automation and appropriate controls aid organizations in improving their data availability and quality to ensure that information sent to clients, donors and customers is accurate. Nonprofits may be intimidated by the potential financial commitment, but it's essential for them to effectively balance their investment in different areas of data security. For example, if a nonprofit invests heavily in cyber insurance, but forgoes conducting appropriate assessments and implementing necessary controls, it may leave itself vulnerable.

7. Incident response tabletop exercise

Once an incident response plan is developed, a best practice for an organization is to conduct a simulation to see how the plan works in action. Key steps to conducting an incident response exercise include:

- Determining if team members understand their roles and responsibilities as they relate to responding to an incident
- Generating awareness that incident response is important
- Ranking gaps, weaknesses and strengths throughout the organization
- Assessing current team members' capabilities
- Identifying outside parties that will be required (e.g., outside counsel, forensic examiners, cyber investigators, notification companies)

- Identifying any additional mitigation and remediation strategies

In completing this simulation, you may find that your response plan needs to be adjusted to address new risks identified. Be sure to implement insights resulting from the exercise into a revised plan.

8. Determine if cyber insurance is right for your organization

In the process of developing a cybersecurity program, nonprofits may want to consider cyber insurance. In order to determine if cyber insurance is a smart investment, be sure to:

- Evaluate marketplace cyber insurance providers, including product types and coverage limitations
- Understand areas of risk and vulnerabilities through scenario-based analyses
- Determine business interruption and recovery costs through incident simulations
- Develop and understand coverage adequacy thresholds
- Align expectations with coverage requirements
- Understand current coverage
- Determine policy options
- Develop a review frequency to maintain continuous coverage optimization

9. Build a comprehensive program

Once all of the above steps are completed, organizations should put together a comprehensive cybersecurity plan, data protection plan and privacy program, outlining potential risks, policies, responsible parties and procedures. Organizations should be sure to consider business operations, legal, compliance, technology, security, data, information and records.

10. Develop a communications strategy

For many organizations, effective communication is an aspect of cybersecurity that often falls by the wayside. A communications plan provides updates, as required or necessary, to your personnel, clients, board members and other stakeholders. Training your staff can help to remove certain threats within your organization. Ensure that your communications strategy includes a training component, which will help your teams better understand their requirements and responsibilities in protecting the organization. It's essential to develop an overall communications and training strategy to deliver information in a consistent and meaningful way in the event of a cyberattack.

Conclusion

Cyber and financial crimes against nonprofits don't often make the front page like hacks of major financial institutions and retailers, but threats are still looming. Organizations should act proactively to implement comprehensive cybersecurity programs now to avoid worries in the future.

Article reprinted from the BDO Nonprofit Standard blog.

New Governmental Accounting Standards Board (GASB) Pronouncements

By Patricia Duperron, CPA

GASB has several new pronouncements that will be effective in the current year and future years:

Fair Value

GASB Statement No. 72, *Fair Value Measurement and Application*, addresses accounting and reporting issues related to fair value measurements. Fair value is defined as the price that would be received to sell an asset or transfer a liability in an orderly transaction between market participants at the measurement date. For those who also audit other nonprofit and for-profit entities, this definition should be familiar as it is the same as Accounting Standards Codification (ASC) 820. Fair value is an exit price and is not adjusted for transaction costs, such as broker fees when selling an investment. The assumption is that the transaction takes place in a government's principal market or the most advantageous market if there is no principal market. The principal market is the one with the greatest volume of activity for the asset or liability. The most advantageous market is the one that maximizes the price that would be received.

The pronouncement provides for three valuation techniques: the market approach, the cost approach and the income approach. The valuation technique should be consistently applied, maximize the use of relevant observable inputs and minimize the use of unobservable inputs. The hierarchy of inputs used to measure fair value falls into three categories: Level 1 is quoted market prices for identical assets or liabilities; Level 2 is for observable inputs either directly or indirectly; Level 3 is unobservable inputs. Illustrations 1-3 in Appendix C of GASB Statement No. 72 provide examples of Level 1, 2 and 3 inputs. Illustration 5 of Appendix C provides example disclosures.

Certain items currently measured at fair value will now be measured at acquisition value (an entry price): donated capital assets, donated works of art, historical treasures and capital assets received in a service concession arrangement. Certain items that were excluded by GASB 31 continue to be excluded from fair value calculations. Some examples include investments in 2a7-like pools, money market instruments that have a remaining maturity

at time of purchase of one year or less, and investments in life insurance policies.

The pronouncement defines an investment as a security or other asset that (a) a government holds primarily for the purpose of income or profit and (b) its present service capacity is based solely on its ability to generate cash or to be sold to generate cash. The purpose is determined at acquisition. Illustration 4 in Appendix C provides examples for applying the definition of an investment. The pronouncement will be effective for the years ending June 30, 2016, and will require restatement of prior periods.

Pension Standards

GASB Statement No. 73, *Accounting and Reporting for Pensions and Related Assets not within the Scope of GASB 68 and Amendments to GASB 67 and 68*, applies the approach to accounting and financial reporting established in GASB 68 to all pension plans that are not within the scope of GASB 68, with certain modifications. Because plans that are not held in trust do not have any assets accumulated, the total pension liability must be recorded instead of the net pension liability under GASB 68. The discount rate must be the yield or index rate for 20-year tax-exempt bonds with an average rating of AA/Aa or higher. Governments cannot use the long-term rate, which would allow for a smaller liability. Any assets held to pay pension benefits should be reported as assets of the employer.

Amendments to GASB 67 and 68 relate to information about investment-related factors and clarify that only information about trends that the plan has influence over should be presented. It also clarifies that payables to a pension plan for any unpaid financing obligations are not separately financed specific liabilities as defined by GASB 67. The last amendment relates to recognizing revenue for support of nonemployer contributions to a pension plan and requires that the contribution be recognized in the same period as the change in the net pension liability is recognized. The amendments will be effective for years ending June 30, 2016.

GASB Statement No. 78, *Pensions Provided through Certain Multiple-Employer Defined Benefit Pension Plans*, addresses an issue related to union-sponsored plans that are not governmental plans but provide benefits to governmental employees as well as employees of other employers. Even though the plans meet the requirements of GASB 68, they are not governmental plans and report under Financial Accounting Standards Board (FASB) guidance. Because of this, governments were not able to get the information from the plans that was required by GASB 68. The pronouncement excludes such plans from GASB 68 and instead requires pension expense to be recognized equal to the employer's required contributions during the reporting period. There is a specific note disclosure required and 10-year required supplementary information (RSI) schedule of employers' required contributions with retroactive reporting for all 10 years. The pronouncement will be effective for years ending Dec. 31, 2016, with early application encouraged.

GASB Statement No. 82, *Pension Issues*, addresses three issues that arose during implementation of GASB 67 and 68. The first relates to the definition of covered payroll included in RSI. GASB 67 defined covered-employee payroll as the payroll of employees that are provided pensions through the plan. GASB 25 and 27 defined covered payroll as all elements included in compensation paid to active employees on which contributions to a pension plan are based–basically pensionable wages. Using the new definition, plans had a hard time getting the total payroll information from the employers as employers only reported to the plans the amount of pensionable wages. This pronouncement changes it back to the old definition: compensation paid to employees on which contributions are based. Restatement will be required for all prior year ratios included in RSI.

The pronouncement also clarifies that a deviation from actuarial standards is not considered to be in conformity with the requirements of GASB 67 or 68 for selection of assumptions in determining the total pension liability. GASB became aware that actuaries may deviate from the actuarial standards to derive reports for plan management but this pronouncement bans such practices for external financial reporting.

The last issue relates to employer-paid member contributions, commonly referred to as employer pick-up. When an employer pays contributions on behalf of members they should be classified as member contributions for GASB 67 plan statements and as employee contributions for GASB 68 reporting and included in salary expense. The issue arose because GASB 67 and 68 required those payments to be classified as employee contributions if the employer reported salary expense; otherwise the payments were classified as employer contributions. This became a challenge for cost-sharing plans in determining an employer's proportionate share of the collective net pension liability (NPL). Because the allocation of pension amounts is based on contributions, some employers would be allocated a larger share of the NPL if they picked up member contributions. GASB concluded that those payments should not be pension expense. The pronouncement is effective for years ending June 30, 2017.

Other Postemployment Benefits (OPEB) Standards

GASB Statement No. 74, *Financial Reporting for Postemployment Benefit Plans other than Pension Plans*, addresses reporting for state and local government OPEB plans that are administered through trusts and replaces GASB Statement No. 43 for those plans. While the financial statements will be very similar to current statements, the pronouncement provides for enhanced note disclosures and new Required Supplementary Information (RSI). RSI will consist of (1) schedule of changes in net OPEB liability and related ratios; (2) schedule of employer contributions (if actuarially determined); and (3) schedule of investment returns (annual money-weighted rate of return). Each schedule should be for the most recent 10 years.

The pronouncement also requires the net OPEB liability to be measured as the total OPEB liability less the amount of the plan's net position and specifies the approach to measuring the liability (entry age normal as a level percent of pay). The discount rate will be the long-term rate to the extent there is a plan net position and the municipal bond rate once net position is depleted. However, one blended rate is used. To do this, governments will need to project future revenues and payments. The pronouncement will be effective for years ending June 30, 2017.

GASB Statement No. 75, *Accounting and Financial Reporting for Postemployment Benefits other than Pensions*, establishes requirements for governments that provide their employees with OPEB through a trust and replaces GASB Statement No. 45 for those government employers. The most significant change is that governments will now be required to recognize their net OPEB liability, which is the difference between the total OPEB liability (the portion of the present value of projected benefit payments that is attributed to past periods) and the value of OPEB assets available to pay pension benefits. Additional note disclosure and the first two RSI schedules from GASB 74 will be required. This requirement also applies to cost sharing, multiple-employer plans and plans that are not administered through a trust. Unlike pension plans, which most governments have been funding for quite a while, many OPEB plans are severely underfunded, and the liability to be recorded will be significant.

The statement mirrors the pension requirements of GASB 68. Most changes in the net OPEB liability will be included in current period expense. Other components, such as changes in economic assumptions, will be recognized over a closed period equal to the expected remaining service lives of all employees that are provided benefits. Differences between expected and actual investment rate of return will be recognized in expense over a closed five-year period. The pronouncement will be effective for years ending June 30, 2018.

GASB is working on Implementation Guides for GASB Statements 74 and 75 and expects to issue the Statement 74 Guide draft in October 2016 and finalize it in February 2017. The Statement 75 Guide draft should be issued in June 2017 and finalized in Nov. 2017.

Other GASB Pronouncements

GASB Statement No. 77, *Tax Abatement Disclosures*, will not result in any accounting or reporting changes but will require specific note disclosures in the financial statements. Tax abatements are widely used by state and local governments to encourage economic development. Tax abatement is defined as an agreement between a government and a taxpayer in which the government agrees to forgo tax revenues and the taxpayer agrees to take a specific action that contributes to economic development or achieves a public benefit. The statement requires disclosure about a reporting government's own tax abatement agreements and those that are entered into by other governments that reduce the reporting government's tax revenues (such as when a city or county enters into an agreement that reduces a school district's tax revenue). Disclosure requirements include the number of tax abatement agreements entered into during the reporting period; the total number in effect at end of the reporting period; the dollar amount by which tax revenues were reduced during the period; and a description of other commitments made in the agreements. Disclosures should be organized by each major program and should continue until the tax abatement agreement expires. The pronouncement will be effective for years ending Dec. 31, 2016.

GASB Statement No. 79, *Certain External Investment Pools and Pool Participants*, establishes the criteria for an external investment pool to measure all of its investments at amortized cost. If a pool meets the criteria and measures its investments at amortized cost, pool participants should also measure their investment in the pool at amortized cost. If the pool doesn't meet the criteria, the pool should apply the provisions of paragraph 16 of GASB 31. This statement was issued to address changes the Securities and Exchange Commission (SEC) made in the Investment Company Act of 1940, Rule 2a7, which contains the regulations applicable to money market funds. Under GASB 31, pools that were "2a7 like" were allowed to use amortized cost. Due to the SEC change in the 2a7 rules, GASB issued this statement to update the guidance for pools. The pronouncement will be effective for years ending June 30, 2016.

GASB Statement No. 80, *Blending Requirements for Certain Component Units*, requires that component units incorporated as a nonprofit, when the primary

government is the sole member, should be reported as a blended component unit. Component units that are included in accordance with GASB 39 are excluded from this statement. The pronouncement will be effective for years ending June 30, 2017.

GASB Statement No. 81, *Irrevocable Split-Interest Agreements*, provides recognition and measurement guidance when a government is a beneficiary of a split-interest agreement. Governments will be required to recognize assets, liabilities and deferred inflows of resources at fair value at the inception of the agreement and must re-measure them annually. Examples include charitable lead trusts, charitable remainder trusts, life-interest in real estate and charitable annuity gifts. The pronouncement will be effective for years ending Dec. 31, 2017.

Other GASB Projects

GASB issued the Exposure Draft, "Certain Asset Retirement Obligations," that applies to certain asset retirement obligations, such as nuclear power plants and sewage treatment facilities, which would require governments to recognize a liability and deferred outflow when the liability is both incurred and reasonably estimable. Similar to the rules over landfills, the liability should be based on the current value of the expected future outlays. The expected effective date is for years ending Dec. 31, 2018.

GASB issued an Exposure Draft, "Fiduciary Activities," related to fiduciary activities which would establish criteria for reporting fiduciary activities and replace agency funds with a new custodial fund for activities that are not held in trust. For activities for which a trust agreement exists, an investment trust fund or private purpose trust fund will be used. Pension funds not held in trust would be classified as custodial funds. The expected effective date is for years ending Dec. 31, 2018.

The GASB Exposure Draft, "Leases," would require governments to recognize a lease liability and an intangible right-to-use lease asset. Lessors would recognize a lease receivable and deferred inflow of resources and would not derecognize the underlying asset. This differs from private sector standards. Short-term leases (maximum term of 12 months or less) are excluded. The expected effective date is for years ending Dec. 31, 2019.

GASB is reexamining the financial reporting model and GASB Statement Nos. 34, 35, 37, 41 and 46, and GASB Interpretation No. 6, and considering presentation alternatives for resource flows. It recently initiated projects to re-examine going concern disclosures and footnote disclosures.

GASB is also reviewing debt extinguishments when only existing resources are placed in an irrevocable trust for the purpose of extinguishing debt and has tentatively decided that in-substance defeasance treatment should be applied. The difference between the reacquisition price and net carrying amount would be recognized immediately, unlike GASB 7 and 23, which allow for the difference to be deferred. GASB expects to issue an exposure draft on this topic in August 2016 and to be finalized in May 2017.

The GASB Omnibus Project will address several practice issues covering a variety of topics. An exposure draft is planned for September 2016 and the final is expected in March 2017.

Is a Merger for You?

By Michael Ward, CPA, CGMA

With more than 1.5 million nonprofit organizations in the United States, it is not unusual to find two organizations serving the same or a related purpose in a given catchment area. This is particularly true in the areas of social services and healthcare, in which numerous organizations have been created to serve various sub-segments, such as individuals with disabilities or those with mental health needs. As community needs evolve and shift, organizations with narrower target populations may not be able to sustain themselves. The 2008 economic downturn placed significant pressure on endowments, donors, foundations and government resources, but organizations serving the neediest populations have been struggling for years.

In 2004, I was serving as the President and CEO of the Lt. Joseph P. Kennedy Institute (the Institute), one of several social concerns agencies in the Archdiocese of Washington. The Institute provided services to children and adults with developmental disabilities. Another organization served individuals with mental health needs and yet another focused resources on the Latino immigrant community. Having several Catholic agencies addressing different segments of the community resulted in the same donors being asked to give to numerous causes, redundancy in administrative and back office functions, and less leverage when approaching state and local governments on contracting and collaboration. After months of planning and deliberation, these three agencies were merged into a larger one designed to meet a broader array of needs. Because few, if any, services were overlapping, the consolidation was primarily in governance and administration. Today, a stronger agency addressing a range of community needs can reach out to donors and government funding services with a unified message and a comparatively leaner organizational structure.

However, a merger may not be the only solution to respond to economic pressure. In 2008, a group of Chicago-based nonprofit organizations considered the possibility of collectively purchasing shared back-office services, creating The Back Office Cooperative. While they ultimately determined there were too many unique accounting and reporting requirements to share in one accounting and finance solution, their efforts coalesced into a group-buying solution, allowing them to gain leverage in negotiating with suppliers, which has already saved several million dollars for its members. The participating organizations offer a broad array of services headquartered in the Chicago area, but some operate in multiple states. A merger was not a solution for these organizations but they nonetheless found immense benefits in combining some of their efforts.

Cost pressure is just one motivator in considering a merger. Integration of services and the ability to better allocate real estate and other resources are also outcomes that can be realized through mergers. The improved outcomes and related growth of in-home support services have fundamentally changed how healthcare for individuals with certain chronic conditions is met. Not too many years ago, lengthy stays in hospitals, intermediate care, or rehabilitation facilities were common. Today, organizations constrained to a certain treatment modality struggle to shift to a decline in demand, with in-home services replacing inpatient and ambulatory services at substantially lower costs. Either by merger or diversification, such organizations need to increase their leverage to remain viable. Combinations in the nonprofit healthcare sector may become more prevalent as these organizations seek to maximize the value of their assets and guard against obsolescence.

Financial Accounting Standards Board (FASB) Accounting Standards Codification (ASC) 958-805, Business Combinations, governs the accounting for nonprofit business combinations, with distinctly

different treatments for a merger versus an acquisition. Under a strict merger, in which a new governing body takes control over the combined activities of the merging organizations, the assets and liabilities of each merging entity are carried forward from their respective balance sheets. Should one governing body take control of the other entity, that combination is treated as an acquisition and the acquired entity's assets and liabilities are recorded at fair value in the balance sheet of the acquiring entity. The difference between the fair values of the assets and liabilities is recorded either as goodwill or as a non-operating item of income or expense depending on the nature of the revenue streams of the acquired entity. This divergence in accounting can be leveraged to extract value on an otherwise cost-constrained balance sheet. If one entity has significantly depreciated real estate used in its operations with a much higher market value, that value could be recognized on the balance sheet if the entity is acquired.

Nonprofit boards and executives will continue to grapple with the best way to generate the greatest value from their assets, seeking to achieve their mission while preserving portfolios from the impact of operating losses. With many nonprofit executives approaching retirement, there may be one less barrier to a business combination—the career path of the current leadership. With over 40 million Americans in retirement (more than at any point in U.S. history and a number that is expected to double over the next 30-40 years), we will need a strong and robust nonprofit sector to address the unique needs of our aging population while still serving the myriad needs of our children and younger adults. It is incumbent upon the leaders in this sector to determine the best structure to achieve that goal.