STRADLEY RONON

Nonprofit & Religious Organizations Alert

WWW.STRADLEY.COM

OCTOBER 5, 2020

Nonprofits Evaluate Risks of Pandemic-Driven Technology

As nonprofits enter the last quarter of a year like no other, many have adapted to the pandemic's challenges through technology. Employees have pivoted to working from home via laptops and wi-fi, staff and client meetings take place on video platforms, and even fundraisers can be held online without either cocktails or chicken dinners. But these technology stopgaps carry their own risks that should not be underestimated by nonprofits.

Consider the news in September 2020 that the Jewish Federation of Greater Washington suffered the diversion of $7.5 million of its endowment fund in unauthorized transfers to international accounts. An investigation is ongoing but indicates access was facilitated through the e-mail accounts of employees working from home, possibly on personal computers. E-mail, remote access, videoconferencing software and file transfer programs used by employees all create potential openings into an organization's information and operations. Many nonprofits also rely on third-party vendors for critical services and software, which come with risks highlighted this summer when the cloud computing provider BlackBaud disclosed a ransomware attack that left its customers' donor information exposed.

Tight budget constraints and a culture that often minimizes operating and overhead costs may contribute to nonprofits giving short-shrift to mitigating these risks. Nonprofits may have minimal staff to assess and respond to technology risks or rely on third-parties whose contracts and locations limit the speed and scope of their response. And while many nonprofits don't consider themselves in the same category of risk as a bank or financial services firm, even organizations without hefty endowments can have significant losses. Information about donors and clients, including their payment information, eligibility for services, health and insurance, or contribution history, can be valuable currency in the wrong hands. The organization also risks losing donors, grants, and the trust of those it serves through its charitable mission.

High-profile losses may be rare, but the organization can lose data in more routine ways that won't make the news in this new virtual environment. Consider the following scenarios:

- An employee needs to be terminated for cause but is working from home with full access to company systems through an organization laptop and accounts. Does your organization have a plan for securing the accounts, as well as the return of the organization's technology?
- Your communications director maintains organization accounts on multiple social media accounts, as well as corporate access to accounts for mailing lists services, website content management software, and news distribution services. Does your organization keep an inventory of accounts and understand how they are used and who else has access to them?
- An employee working off-site loses a corporate laptop and security key fob that provides authentication, or worse, decides to quit without notice and not return these items. Does your organization keep a regular inventory of physical technology assets and have clear procedures for employees to report the loss of phones, computers, or security devices?

Stradley Ronon Stevens & Young, LLP
2005 Market Street
Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
New York
New Jersey
Illinois
Delaware

www.meritas.org

Our firm is a member of Meritas. With 189 top-ranking law firms spanning 97 countries, Meritas delivers exceptional legal knowledge, personal attention and proven value to clients worldwide.

Information contained in this publication should not be construed as legal advice or opinion or as a substitute for the advice of counsel. The enclosed materials may have been abridged from other sources. They are provided for educational and informational purposes for the use of clients and others who may be interested in the subject matter.

Do you have a plan for forensic data recovery, including an understanding of the costs to rebuild or restore lost data?

Legal counsel can be as critical as the right technology strategy in these situations. For our nonprofit clients who are thinking about ways to limit risk, the Stradley Insurance practice has put together an overview of mitigation strategies to serve as a starting point for your own review. And we can help with finding the resources you need to address these issues, whether it means your collection, retention and disposal of data containing personal, financial or health information, reviewing your contracts with technology vendors, evaluating a cyber-insurance policy or claim, preparing appropriate data security policies and procedures, putting in place an employee management plan, or conducting an investigation into a possible loss.

Jennifer A. Gniady
202.419.8436
gniady@stradley.com

Peter Bogdasarian
202.419.8405
pbogdasarian@stradley.com

For more information, contact Jennifer A. Gniady at 202.419.8436 or jgniady@stradley.com *or Peter Bogdasarian at 202.419.8405 or* pbogdasarian@stradley.com.

- **Evaluating your collection, retention and disposal of data containing personal, financial or health information**:
  - New York's SHIELD Act went into effect in March 2020 and requires any person or business owning or licensing computerized data that contains the private information of a resident of New York to implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information
  - Massachusetts' Standards for the Protection of Personal Information of Residents of the Commonwealth require that every person or business owning or licensing personal information regarding a resident of Massachusetts is required to develop, implement, and maintain a comprehensive written information security program and set a minimum floor for the security covering an organization's computer systems and network
  - Although nonprofit organizations are exempt from the California Consumer Privacy Act (CCPA), vendors, providers, and other third-parties are not exempt
- **Reviewing your contracts with technology vendors:**
  - Do your vendors maintain reasonable security programs, including adequate cyber-insurance coverage?
  - Do you have consistent contract provisions related to security and the handling of a cyber incident?
  - What obligations do your contracts impose with respect to the disposal of data?
- **Evaluating a cyber-insurance policy or claim**:
  - Weighing your organization's need and risk
  - Explaining different forms of coverage
  - Assessing the details of compliance with your cyber-insurance policy
- **Preparing appropriate data security policies and procedures**:
  - Does your organization have policies for data classification, password strength, access controls, the use of encryption, data disposal and/or patch management?
  - Do you have an Incident Response Plan?
  - Do you understand the potential benefits and/or drawbacks attached to contacting law enforcement if your organization is the target of a cyberattack?
- **Employee Management Plans:**
  - Evaluating employee risks and planning to train employees to prevent losses, protect data, and report problems.
  - Ensuring your employee handbook and policies reflect organization expectations about technology, data, and devices.
  - Developing a plan for handling remote work, including securing data and devices in the event of a termination.
- **Investigations into a possible loss:**
  - Providing specialized expertise in retaining and directing computer forensic and other services in connection with a cyberattack or a potential cyberattack
  - Analyzing and assessing the legal and contractual duties that could arise from a successful cyberattack on the organization

If you are interested in more information on this topic, check out our recent alert: Mitigating Cyber Risk During the COVID-19 New Normal, which provides provide the best cybersecurity practices for remote work amid the COVID-19 pandemic.