Nonprofit Technology News October 24, 2016

Don’t Get Spooked By Cybersecurity - Tips for a Secure Nonprofit

Bill Sayre

Here’s a scary fact – in 2015, more than 169 million personal records were exposed as a result of 781 publicized breaches. You likely are aware that Halloween is coming up at the end of the month, but October is also National Cybersecurity Awareness month. This month serves as a reminder that in our connected and digital age, nonprofits need to protect their organizations – and donor information.

Security is an essential piece of the donor care paradigm and donors deserve to know their information is in good hands. Just one breach can be significant enough to scare dedicated supporters from future giving. Security incidents come with a significant price tag as well – research suggests the current cost of a single data breach is $4 million.

While security is important, it doesn’t need to be scary. From encryption to payment card industry security standards, consider these best practices for building a secure environment at your nonprofit:

Account for All of Your Candy Pails & Sort Your Candy; Understand What Needs Protection

Data is like candy to cybercriminals; whether it’s desired for financial benefit, to disrupt your business or simply to create publicity, they want and will take as much as they can get from any source they can find.

The very first thing to understand is what data exists and where it resides. Identify anything, physical or electronic, that includes a financial account, that identifies (or has the ability to identify) an individual by name and/or location, or that can expose proprietary information.

Secondly, identify each storage location – physical documents and electronic records that are stored in offices and storage warehouses, at/by third parties and their partners and by your employees and members – and medium – filing cabinets, pallet racks, servers and PCs/tablets/phones, data tapes, compliance filings, etc.

Once you've identified the type, location and medium, categorize a value and risk factor and a solution option for each, then take a two-pronged approach by securing the high-high (which will likely need more time and investment) and the low-low (which can likely be secured quickly and easily). A great method is to plot a graph, assigning value/risk and solution complexity as the axis, and solving for the bottom left and top right quadrants first.

Don't Get Tricked; Treat Donor Data Securely

The primary objective of cybersecurity is to protect data. Donor data security shouldn't be overwhelming, even for busy nonprofits – organizations can begin with the basics.

This means investing in standard data security software. Firewalls, antivirus, spam/spyware and intrusion detection software create a solid security baseline that not only keeps cyber criminals out, but also can track intrusions should a security incident occur. To further guarantee the security of your network, conducting random network penetration tests on a quarterly basis can highlight vulnerabilities and allow your organization to take action before it is too late.

Swipe Without the Scare: Keep Donor Credit Card Information Secure

Nonprofits and any organizations that regularly deal with credit card information need to follow the Payment Card Industry Security Standards Council's (PCI SSC's) standards for safely processing credit card information. PCI Data Security Standard (DSS) offer a framework that spans prevention, detection and reaction to security incidents, ensuring comprehensive protection. With four levels of rigor, nonprofits should aim to achieve the highest level of compliance to keep donor information safe.

Don't Send Donor Data Into a Haunted House: Remember Physical Security

Donor security isn't complete without focusing on physical as well as cyber elements, and there are many factors that go into creating a safe physical environment, especially for the processing of donations received via the mail. First, donations should be appropriately tracked at all times – from GPS tracking technology on vehicles transporting donations to 24/7/365 video surveillance of the areas where donations are processed. From the time donations leave the post office to their arrival at the donation processing facility they should be tracked and handled by at least two employees.

Nonprofits need to ensure they have right restrictions in place when it comes to employees, as well. This includes background checks and use of IDs, badges and/or biometrics to grant access to the building and restricted areas, where appropriate.

Eliminate All Fear - Consider Outsourcing

Nonprofit leaders are responsible for wearing many hats and donation processing can be a particularly time consuming effort, especially when taking care to put in place appropriate security measures. Outsourcing donation processing can alleviate this fear, while leaving the security of donor financial and personal information to organizations with expertise and time-tested best practices for efficient and secure donation processing.

When considering security, remember that donors are the lifeblood of your nonprofit and expect their information to be carefully managed. Don't let breaches haunt your nonprofit and learn from our recommendations to give donors the best care and security without any tricks.