AEGIS
PREMIER SOLUTIONS

Cybersecurity: What You Don't Know Can Put Your Organization At Risk

AEGIS crm

Aegis Premier Solutions is committed to maintaining thehighest standards and providing exceptional service to our nonprofit clients.We are a leading provider of nonprofit services such as caging,donor management,merchant services,and acquisition funding.

Our suite of products offers an end-to-end solution from acquisition funding to donation processing and the management of donor and campaign data. We help you work smarter and make it simple. Let Aegis Premier Solutions help you focus your time on fulfilling your non-profit's mission!

The Aegis brand includes three unique companies – Aegis Premier Solutions, Aegis Processing Solutions and Aegis Premier Technologies – that have joined forces to provide our clients with an A to Z suite of services to help navigate through the various aspects of fundraising.

Security is at the forefront of our business mission. Your organization and your donors can rest easily knowing information is secure in state-of-the art data centers, monitored 24/7/365. Our experts ensure your system is always up-to-date, correctly configured, and is PCI DSS compliant.

Table of Contents

Safeguard Your Organization

Cybersecurity is a reality on a global level and being prepared to recognize a potential threat, implement a plan when someone reports a suspected security breach, and follow the proper reporting requirements are some of the ways you can safeguard your organization and donors.

These organizations and others have had what used to be public information in a phone book, that is now considered private, stolen from them in one way or another. In addition to names, addresses, and phone numbers many of these breaches included credit card and social security numbers as well.

What You Don't Know Can Put Your Organization at Risk

Here are some examples of the impact a security breach can have when personal information is stolen from an organization:

Target

- ~40 million credit and debit accounts may have been impacted
- ~61 million people had their personal data stolen
- Paid $10 million to settle a class-action lawsuit

Yahoo

- 500 million accounts were stolen in 2014 and reported in 2016
- First breach in 2013 compromised over 1 billion accounts

Utah Food Bank

- 10,000 donor records stolen in a single breach
- Stolen information included names, addresses, and credit card numbers

The table below identifies more information about security breaches that includes the company name, impact, and source for more information:

Company Name	Impact	Source
Experian Credit Bureau	15 million T-Mobile customers	The Huffington Post
Democratic National Convention	20,000 emails and thousands of attachments	PC World
Community Health Systems, Inc.	4.5 million patient data stolen including social security numbers	Los Angeles Times
Urban Institute	700,000 nonprofit organizations	The Huffington Post

The Identity Theft Resource Center data states that in 2016 there were 1,093 reported data breaches that included a total of 33.6 million records. This is a 40% increase over 2015 and employee error or negligence caused 8.7% of those breaches.

In benchmark research study sponsored by IBM, the United States averaged $7.01 million in total costs for a data breach in 2016 which is a 7% increase over 2015. The average cost per lost or stolen record is $221 and increases 2015 costs by 2%.

When a security breach happens, not only can it be expensive and take a lot of time to resolve it can also break the trust donors have with your organization. Other ways a breach can have negative impacts include damage to your organization's reputation and loss of future revenue.

At Risk Activities

Recognizing the activities that put your organization and donors at risk are important to reducing the chances of having a security breach. At risk activities include:

- Collecting credit card data and processing payments online.
- Storing information on mobile devices and cloud services or systems.
- Allowing access to personal information without proper safeguards.

While these are just a few of the activities that can increase your chances of a breach, this article in CIO Magazine describes more you should be aware of to better protect your data.

Limit Your Risk

While knowing about the activities than can put your organization at risk of a breach is important, you also need to learn more about how you can limit your risk for a breach. You should track and monitor your data, especially online donations, for suspicious activity.

Unexpected increases in online donations or activity is a red flag so look at your merchant account to further investigate a potential threat. **If you believe there is a breach of your merchant account, you can stop further threat by suspending that account while you resolve the issue.**

Incident Response Plan

An incident response plan documents how to deal with a potential threat. If a donor reports that they believe their information has been compromised:

- What questions will you ask to get the information you need to track the potential threat?
- What are the reporting requirements for the state where the donor lives and where your organization is located?

- Who in your organization is responsible for investigating a possible breach and reporting it to the proper authorities?

These are a few of the questions you should be answering with your incident response plan. If your organization is found to be responsible for a breach and you don't have a plan, you can incur additional fees and penalties.

Data Encryption

Encrypted data has no value to thieves so using encryption to protect the information stored on computer systems and servers is one of the most effective ways to ensure the security of your data. In addition to protecting your data, consider encrypting your email communications too.

When you incorporate data encryption, access to your data is restricted to those who do not have the key and helps mitigate the risk of a security breach. While data encryption can be a big investment for an organization, ask yourself what is your data worth and are you doing everything you can to protect it from being stolen?

Employee Training

With 8.7% of all security breaches in 2016 happening because of employee error or negligence, training employees on best practices for protecting private information can reduce the chances of a breach.

Your training plan should be included in your incident response plan and document things such as:

- Protecting company devices including computers, laptops, and mobile phones.
- Procedures for reporting a potential breach.
- Roles and responsibilities for safeguarding sensitive information.

Data Loss Prevention Technologies

Preventing data loss is another critical component of limiting your risk for a security breach. While there is no single solution that effectively prevents data loss, there are best practices you can use that fits the needs of your organization. The National Institute of Standards and Technology identifies these best practices:

- Prioritize loss modes (data at rest, data at the endpoint, and data in motion) to identify those at risk and then focus on those with the highest impact if a breach happens.
- Protect your data without disrupting normal business activities.
- Create a flexible and modular architecture that addresses your most important requirements.

Cyber Insurance

Just like you insure your life, home, and car you should also insure the private data you store on your donors. If your organization does not have cyber insurance, we encourage you to consider this type of protection.

Privacy and data breach insurance covers expenses associated with notification costs, credit monitoring, regulation claims, fines and penalties, and identity theft. Cyber insurance is your first line of defense and should include privacy coverage (first-party and third-party liability) as well as network security coverage (client data breach and cyber extortion) to fully protect your organization.

In the article What is cyber insurance and why you need it in the May, 2016 issue of CIO Magazine, you can learn more about reimbursable expenses and what to look for in a policy.

Resources

The more you know about protecting your organization and donors from cybersecurity risks, the better prepared you are to quickly respond to a threat. In addition to the information linked in this handout, here are some additional resources you can use to learn more about cybersecurity.

- Identity Theft Resource Center
- Cybersecurity for Small Business
- Incident Response Planning

Feel free to contact our subject matter expert, Lori Read to answer any questions you have about cybersecurity and protecting your organization from a threat.

Disclaimer

The information provided in this document and companion webinar recording is made available by Aegis Premier Solutions, Aegis Premier Technologies and Aegis Processing Solutions. This information is provided as an overview of legal responsibilities related to cybersecurity.

Aegis does not provide legal advice and none of our representatives are lawyers. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a lawyer or insurance expert if you need additional information related to cybersecurity liabilities and insurance coverage.

AEGIS
PREMIER SOLUTIONS