untangle

WHITEPAPER
OCTOBER 2017

NETWORK SECURITY BEST PRACTICES FOR NONPROFIT ORGANIZATIONS

Today's not-for-profit organizations must be keenly aware of their data management, governance and security needs, as more services and tasks are processed digitally. Everything from donor information to contribution records needs to be handled with great care in order to adhere to best practices and industry regulations. There are many characteristics that separate nonprofits from privately owned businesses, but the pressing need for a comprehensive network security solution isn't one of them. To excel and thrive in the digital age, nonprofit organizations must employ high-quality network management solutions.

There are a number of factors that nonprofit leaders should keep in mind when evaluating their current network capabilities and opportunities for improvement. First is the issue of transparency. Perhaps no single factor separates charities and non-governmental organizations from other institutions more than the need to show donors, contributors and auditors precisely where funding is being allocated.

Another major point of consideration is regulatory compliance. According to the National Center for Charitable Statistics, there are more than 1.5 million tax-exempt organizations operating in the United States[1], each one potentially faced with various regulations dictating how data should be managed. Because a given nonprofit may handle a wide variety of information, including health records, financial reports and payment statements, it may be beholden to multiple regulatory bodies and guidelines. Demonstrating compliance should be a primary concern for all nonprofits, regardless of size or operational scale.

Finally, nonprofits must find a way to overcome the widespread technological obstacles encountered in this sector. A lack of resources or in-house expertise cannot stand in the way of putting baseline cybersecurity safeguards in place.

TARGET FOR BREACHES

When it comes to selecting a target for their next attack, cybercriminals don't overlook nonprofits; in fact, they often see them as soft targets. As we have seen recently, small and very large companies have been victims of wide-scale breaches. For nonprofits, it is no different. 63% of not-for-profits suffered at least one breach in 2016, according to a survey conducted by the SCCE and HCCA.[2] In August 2017, Kaiser Permanente, one of the largest not-for-profit health plans, revealed that approximately 600 members in Riverside had their sensitive information breached, including names, medical records and procedures.[3]

While Kaiser Permanente is a very large not-for-profit, smaller organizations are not immune to breaches. In January 2017, Little Red Door, a small, Muncie, Indiana-based nonprofit, fell victim to a ransomware attack. Hackers gained access when an unsuspecting employee clicked on a phishing email, which locked down the network and demanded payment to release the files.[4]

This type of hack also proves a point that nonprofits need to protect themselves from within. According to an SCCE survey, lost devices (20%) and lost paper files (45%) were the top reasons a breach occurred. When it comes to digital assets, access management is another concern nonprofits must consider when determining the right solution for their network.

Untangle offers the network monitoring and governance capabilities needed by nonprofits. System administrators can establish granular rules and policies to only allow authorized users access to data pertinent to their job.

Regardless of the size, scale or focus area of a nonprofit organization, Untangle has the tools needed to properly secure and monitor its network environments.

THE COST OF COMPLIANCE

While nonprofits may be given some special treatment by the government, this does not extend to data management regulations. Like members of the healthcare, financial services and retail industries, nonprofit institutions are expected to diligently follow certain guidelines regarding the handling, storage and safeguarding of information. Depending on the nature of the information traveling across an organization's network, a nonprofit may be faced with regulations relating to the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standards (PCI) or the Sarbanes-Oxley Act (SOX), among other legislation and industry guidelines.

For instance, if a nonprofit handles electronic health records or other forms of patient medical data, it would need to be compliant with HIPAA regulations or face potentially massive financial penalties. With HIPAA, a single infraction could result in a fine of up to $1.1 million.[5] That figure may be at the high end of HIPAA's punitive measures, but even lesser offenses can bring stiff fines. The average cost of a single data breach across all industries was $3.62 million in 2017, according to a study from IBM and Ponemon Institute.[6] If an organization is found to have been neglectful in its data management and security responsibilities, including not addressing the issue promptly, the fines only go up from there.

ESTABLISHING A SECURITY STATEGY

That's why nonprofits need to do everything in their power to not only safeguard their networks and protect sensitive information, but be able to demonstrate that they have operated in good faith when it comes to data management and protection. A good data security strategy begins at the network level, preventing unauthorized users from accessing nonprofit assets.

Untangle has numerous features that effectively lock down networks and prevent malicious activity from occurring. A high-quality firewall is critical here, establishing concrete rules for allowing or blocking incoming traffic. From there, Untangle canalso provide nonprofits with intrusion prevention capabilities that help spot suspicious network activity and alert administrators.

Application control is another feature that nonprofits will likely need with their network management and security tools. This enables administrators to dictate precisely who can access network-based applications, preventing unauthorized users from compromising sensitive information and assets.

Having these network security protections in place will help nonprofits prevent malicious acts as well as demonstrate their own dedication to best practices if a breach does occur. The reporting capabilities offered by Untangle can be extremely helpful in this regard, highlighting network activity and application access at a granular level. The combination of security and governance afforded by Untangle will be a major asset for any organizations concerned about staying compliant with data management regulations.

UNTANGLE FOR NONPROFITS

There's no need for nonprofits to break the bank in order to obtain a high-quality network security solution, however. Untangle offers an all-in-one, affordable solution that can handle all the network security, monitoring and control tasks that smaller organizations require. Budgetary restraints shouldn't prevent a nonprofit from getting the protection it needs to remain transparent about its financial transactions and compliant with current regulatory standards. Regardless of the size, scale or focus area of a nonprofit organization, Untangle has the tools needed to properly secure and monitor its network environments.

To excel and thrive in the digital age, nonprofit organizations must employ high-quality network management solutions.

SOURCES

1 http://nccs.urban.org/data-statistics/quick-facts-about-nonprofits
2 http://www.corporatecompliance.org/Portals/1/PDF/Resources/Surveys/2016-data-breach-survey.pdf?ver=2016-12-12-073403-497
3 http://www.pe.com/2017/08/30/kaiser-permanente-says-600-riverside-area-members-affected-by-data-breach/
4 http://www.kqed.org/news/story/2017/05/20/236473/small_indiana_nonprofit_falls_victim_to_ransom_cyberattack?source=npr&category=technology
5 https://www.beckershospitalreview.com/healthcare-information-technology/healthcare-breaches-cost-6-2b-annually.html
6 https://www.hipaajournal.com/healthcare-data-breach-costs-2017-8854/

Untangle, Inc.
100 W. San Fernando St., Ste. 565
San Jose, CA 95113
www.untangle.com

ABOUT US

Untangle is an innovator in cybersecurity for the below-enterprise market, safeguarding people's digital lives at home, work and on-the-go. Untangle's integrated suite of software and appliances provides enterprise-grade capabilities and consumer- oriented simplicity, bringing a new generation of smart security to homes and small-to-mid-sized businesses. Untangle's award-winning network security solutions are trusted by over 400,000 customers, protecting nearly 5 million people, their computers and networks around the world.

For sales information, please contact us by phone in the US at +1 (866) 233-2296 or via e-mail at sales@untangle.com.