CHRISTIAN BROTHERS SERVICES

1205 Windham Parkway
Romeoville, IL 60446
800.807.0100 cbservices.org

Health ▪ Retirement ▪ Property/Casualty ▪ Consulting ▪ IT & Website Services ▪ Catholic School Management

Vol. 6, No. 2 2015

OutReach

A Christian Brothers Services Publication

Cyber Liability and Data Breach Exposures: Identifying the Risks to Your Entity

New Look — Same Mission-Driven Organization

A Partnership to Strengthen Catholic Schools

CHRISTIAN BROTHERS SERVICES

Cyber Liability and Data Breach Exposures:

Identifying the Risks to Your Entity

Risk Management Services

CVS. UCLA Healthcare Systems. Target. Home Depot. Sony. Even the IRS. Every day it seems the media is reporting yet another data security breach of a major organization or company. As more and more data is stored electronically, the question that needs to be answered is not what will we do if we have a data breach, but what we will do when a breach occurs. Any cyberbreach could result in the theft of your own valuable information, or the loss of confidential information belonging to your employees, patients, students, donors or those you serve, not to mention the considerable costs associated with responding to these issues.

While widely-reported cyberattacks have involved financial and point-of-sale data, professional hackers target a broad range of information. Not-for-profit organizations, including those that receive financial donations, operate schools, health care facilities or similar institutions, or those that have large numbers of employees, all have information hackers can steal and sell. Beyond financial information, hackers use cyberattacks to acquire health records, employee records, student records and similar data. Unlike a single credit card number, these types of records provide hackers with complete identity information that commands a higher price on the black market where stolen records are sold. These records can be used to perpetrate identity theft, obtain prescription drugs, engage in Medicare or Medicaid fraud and open new and untraceable credit accounts, among other activities.

The resulting cost to the victim organization includes not only the expense of fixing the breach, but also in notifying those whose records have been compromised. Some experts place the notification costs associated with cyberattacks at $154 *per record*, in addition to the cost of repairing the breach. For an organization with thousands of donor, employee, student, resident or other records, the cost of a cyberattack could easily exceed the victim organization or institution's ability to absorb those costs.

Hackers are also becoming more sophisticated in their attacks, and making it more difficult for victims to figure out an attack has occurred. Hackers previously relied on viruses that constantly transmitted information back to the hacker, making them easy to spot. Now, the viruses act like ticking time bombs, sitting in an organization's system and gathering information for months undetected. Then, on a particular date and time, all of the information is transferred out in one fell swoop, and it is too late for the organization to stop the attack.

In addition to stealing data, cyberattackers are also finding ways to encrypt and hold data hostage, thereby crippling an institution's ability to operate and demanding a ransom before the information is unlocked. While the entity may be able to restore its data without resorting to paying the ransom, the time and costs associated with that work are often significant, as are the losses in productivity while the problem is addressed and the subsequent notification costs.

To protect itself, your organization must consider all the ways a hacker could gain access to your systems and to your data. Consider the following:

- → Are the places where your critical data is stored connected to the Internet?
- → Do you use a wireless system that is not locked down?
- → Are your employees able to use personal devices to access sensitive information, or can they use company equipment on unprotected networks?
- → Are your employees vulnerable to "spear-phishing," where they click through an email or web pop-up that lets the hacker in?
- → Are other users, such as vendors, students, employees and patients, able to access your networks through electronic portals?

Cybersecurity and technology professionals can also help identify areas of vulnerability.

One means to protect your organization from the costs associated with these inevitable attacks, is to consider the coverage options available to you. Christian Brothers Services and the Christian Brothers Risk Pooling Trust offer limited coverages that assist members in managing the risks associated with these issues. Please contact your account manager to evaluate your organization's specific risks and the steps you should take to ensure that your organization is protected in the event of a breach. ☼

Mollie E. Nolan Werwas is an attorney and partner with the law firm of Kopon Airdo, LLC. Kopon Airdo, LLC serves as the national coordinating council for Christian Brothers Risk Management Services.