Vol. 7, No. 1 2016

OutReach

A Christian Brothers Services Publication

Into the Light
Breaking the Silence on Domestic Violence

Key Strategies for Selecting the Right Employee Benefit Plan

Risk Pooling Trust Members Enjoy 10 Consecutive Years of No Rate Increases

CHRISTIAN BROTHERS SERVICES

CYBERRISK, CYBERSECURITY AND DATA BREACHES, OH MY!

**THERE ARE TWO KINDS OF ORGANIZATIONS:
THOSE THAT HAVE BEEN HACKED AND
THOSE THAT DON'T KNOW THEY'VE BEEN HACKED**

In protecting your organization and the data entrusted to you, you can be right 999 times out of a 1,000, but a hacker only needs to be right once. Within your organization, you are likely doing everything you should, from living your mission and your charism to creating and executing your strategic plan. As you consider the risk management component and activities of your plan, take time to fully consider your cyberrisks.

YOUR POTENTIAL CYBERRISK EXPOSURES

Who are your various stakeholders, what types of data do you collect and store from them? Your website has become your electronic front door. Do you know everything that is in your "house" and accessible to those who come to visit your website? The same rule applies to your Facebook and other social media outlets in use. We are a long way from websites simply being electronic billboards for organizations with static text and PDF versions of brochures. All of these various online assets now comprise your overall digital presence. Be sure you know what constitutes your digital presence and what cyberrisks are lurking around which may require review and evaluation.

Start with data you collect and store, especially confidential, proprietary and individually identifiable (CPI) data, in electronic or paper form. You may have donors or customers from candy or music sales that help support your mission. What would happen if this CPI data was breached and made available in the public domain? Main risks, regardless of organization size, generally include loss/disruption of business, reputational harm, identity theft and resulting litigation. Consider the potential impact a breach of CPI data might have on your overall revenue and fundraising. No organization can afford not to address cyberrisks. Plan prudently to protect your organization and revenue stream.

All the data you collect and store likely falls into one or more of the following categories:

PII - Personally Identifiable Information

PHI - Protected Health Care Information as defined by HIPAA

NPFI - Nonpublic Financial Information

PCI - Payment Card Information

All this data has value to a hacker looking to steal and sell it on the black market. Price lists exist and are affected by supply and demand, and it's easy for a hacker to sell their ill-gotten data. As you evaluate your data risks, the rule of thumb is - if you don't need it, don't collect it and certainly don't store it longer than you might need it. Remember, all it takes for a hacker to wreak havoc on an individual is to get just one or two pieces of data (e.g., last name, DOB, SSN, ZIP code, mother's maiden name, etc.) about their target. One piece of data may be all it takes for a hacker to go to a website, click the "forgot password" link and pretend to be you. Once they assume your identity on that website, they have access to your credit card on file at that site and can repeat the process at other websites, over and over again. What would happen if they assumed your identity or one of your stakeholder's identities on a banking site?

Of course, we have the advancement of information technology and the internet to thank for these modern day cyberrisks. Without that single pair of wires every organization has to connect themselves to the internet, there would be no need for Chief Security Officers (CSOs). It is unfortunate the internet allows bad things in with the good. In the end, know you have data that others want, and you have a digital presence that needs to be tended to and protected 24x7x365. Good goals to have include keeping your organization out of the headlines and off government radar screens while keeping your Chief Information Officer (CIO) and Chief Executive Officer (CEO) out of jail.

CURRENT STATE OF CYBERSECURITY

The current state of cybersecurity in early 2016 has a variety of studies that illustrate no organization, industry or locale is 100 percent bulletproof when it comes to the compromise of data. Many of the same threats exist year after year, and there are activities an organization can easily take on to reduce risks and improve their overall security posture. According to Verizon's 2016 *Data Breach Investigations Report*, about 80 percent of confirmed data breaches are caused by external actors, and 80 percent of those hacks had a financial motive. Every organization should create a security awareness program, no matter how basic, to begin to address cyberrisks. You cannot afford not to create such a program.

Approximately 55 percent of threats to an organization's data come from within due to errors made by staff in handling data, misusing data and by losing mobile devices, in addition to threats from external actors. Employees need to know they are a target, and the organization is only as strong as its weakest link, systems and people. Consider creating a security awareness program that focuses on anti-phishing, creating and maintaining strong login credentials and patching known system vulnerabilities.

Phishing is the act of a hacker sending an email message to an employee trying to make it look like it came from someone they know or a company they usually interact with, trying to get them to click on a link so they can obtain valid login credentials (i.e., ID and password) to an organizational system. An email phishing attack sounds easy because it is easy. Any hacker can make an email message look identical to an authentic message. Gone are the days when hackers used broken English and easy-to-spot fake email messages. Phishing is quick, easy and cost-effective for the hacker. And it works … a lot. Twenty-three percent of people open phishing messages and 11 percent click on the attachments. Systems might be good, but people are likely the weakest link in your security electric front door, especially curious people who click links and attachments without even knowing what it is they are clicking on. One ill-advised click may cause crimeware to be installed on the victim's computer. A particularly nasty version of crimeware is known as ransomware or cryptovirus. Once installed on a computer, it encrypts and locks the entire machine, which could be a server as easily as it could be a single person's computer, and demands that ransom be paid for the machine to be unlocked. Even if the ransom is paid, there is no guarantee the hacker will be nice enough to send the key to unlock the unit.

Cyber liability coverage is growing rapidly and has crossed the $2 billion mark for annual premiums.

You can combat phishing by educating your employees about the risks of phishing and to be very careful about screening their emails. Additionally, ensure all anti-virus and malware detection software is up to date and consider using a service that screens the known bad messages from your inbound email before they even get to a person. The Department of Homeland Security administers a site, staysafeonline.org, that provides education for organizations, employees and their families.

The Department of Homeland Security administers a site, staysafeonline.org, that provides education for organizations, employees and their families.

Another lock on your security front door should be implementing complex passwords which should contain a minimum of 12 characters and must include upper and lowercase characters, a numeric and a special character and that expires every 90 days. A complex password would take a modern computer system about 40 years to crack. As passwords get longer, they can get more difficult to remember. Note that password maximums are usually 256 characters. Consider promoting pass phrases to your employees, which could be as easy as a simple sentence with four words (e.g., "I Love My CIO 8") separated by spaces with a number added which eliminates the need for employees to write down their password and post it on their monitor or keyboard.

All software has vulnerabilities whether it's Microsoft Windows, Adobe Acrobat, your favorite web browser or other software programs. Every piece of software has known vulnerabilities, and the manufacturers work hard to patch their software systems to protect against those vulnerabilities. Make it a part of your security plan to obtain and apply these patches frequently and regularly. Hackers are still exploiting vulnerabilities that were made known with patches created over two years ago. There is a gold mine of systems for hackers out there going unpatched. Bring your systems current and close those holes to help seal your electronic front door.

The new normal in the state of cybersecurity, human firewalling, will remain ineffective to sophisticated social engineering and phishing attacks and software vulnerabilities are an issue. Create a security awareness plan to help protect your organization. The traditional perimeter defense approach to security is being replaced with a multi-layered approach driving towards proactive intelligent security. There are new models emerging for identity and trust, and when in doubt, encrypt, encrypt, encrypt. Make security awareness a daily activity not just an annual activity. Consider the following checklist to create a comprehensive cybersecurity program to mitigate cyberrisks:

- Complete an IT risk assessment
- Review IT governance model
- Review IT policies, standards, procedures and guidelines
- Review identity management and access controls
- Review operations center monitoring and management tools
- Enhance infrastructure
- Inventory all IT hardware, software and data assets
- Review and update your security awareness program
- Bake security into application acquisition and development
- Conduct third party vendor security assessments
- Repeat for continuous improvement

Helpful Tip

Beware of pineapples -- not the fruit! A pineapple is a fake or rogue Wi-Fi access point. It will look like the authentic, original access point, but will most likely contain a common misspelling in the name. Most people may not pick up on the misspelling and blindly connect to it. In turn the pineapple is connected to the real network and while it allows all traffic through, it also records it looking for sensitive data, including valid IDs and passwords.

LEGISLATION AND PRIVACY & SECURITY

In addition to keeping an eye on and working to mitigate your cyberrisks, also keep an eye on legislation in the privacy and security realms. Currently, 47 states have laws requiring notification in the event of a data breach of personal information, and the laws vary in terms of what constitutes personal information along with the timing of notifications. These breach notification laws are constantly changing and continually being passed regarding data breaches. Be aware of the laws that apply to your organization along with the compliance requirements and penalties for non-compliance. Hopefully one day, Congress will pass one comprehensive law that may simplify compliance activities while also improving data protection.

CYBER LIABILITY AS A CONCERN

Cyber liability within your organization may be a concern. According to Net-diligence, the average cost in 2015 of a data breach was $674,000 including forensics, legal, notification and other costs. If you are considering cyber liability coverage, review your existing insurance coverage to determine if you are adequately covered. Insuring clauses include privacy liability, network security liability, network extortion and internet media liability. Cyber liability coverage is growing rapidly and has crossed the $2 billion mark for annual premiums. The cost of a cyber liability policy to cover your risks and potential claims may be money well-spent; however, be careful not to over- or underinsure.

A BEST PRACTICE APPROACH TO CYBERSECURITY

A best practice approach to cybersecurity is to be reasonable and prudent for your organization, what you do and who you serve. Once you make that determination, you need to decide what types of security levels you should have. You'll need those protections at the network level when you connect to the internet, at the computer and endpoint level for each device on your network and at the data level to protect individual files and data records.

When it comes to data level protection, the most important thing you can do is limit access to sensitive data. Once you consider your digital inventory of what data you have and where it lies, you can then determine who should have access to it. For computer-level security, one important point is to require "complex" passwords or pass phrases.

At the network level, inventory all servers and end points on your network. Pay special attention by looking for devices that should not be connected to your network. Keep in mind that you may not be able to physically see all devices connected to your network, for example, Wi-Fi access points. Wi-Fi access points are easily hidden out of sight and can be a particular concern if they are more than two years old. Wi-Fi security has been changing rapidly, so make sure to scrutinize all access points to be sure they offer modern security protocols. ☼

For information on cybersecurity, contact Tom Drez at 800.807.0100 x 2930.

Tom Drez is the Chief Information Officer/ Chief Privacy Officer/Chief Security Officer for Christian Brothers Services.

A DATA BREACH WALKTHROUGH

If a data breach occurs, best practice calls for an organization to have a Data Breach Protocol or plan in effect, similar to a Business Continuity Plan or a Disaster Recovery Plan.

A DATA BREACH PROTOCOL COULD LOOK LIKE THIS:

- The Chief Executive Officer (CEO) notifies the Board of Trustees.
- The Chief Financial Officer (CFO) notifies the insurance broker of breach and acts as a liaison to the broker for the claim processing and related activities.
- The General Counsel or Legal Consultant ensures compliance with any applicable breach notification law(s).
- The Chief Operating Officer (COO) or Chief Marketing Officer (CMO) oversees development of communications plan to affected constituents and media, as required.
- The COO or Customer Service Department Head coaches call center on response protocols for inquiries by participants or media.
- The Chief Information Officer (CIO) or Head of the Technology Department engages external forensics firm to assist in analysis of breach and method of elimination. They will review all other similar and related systems to make sure any similar vulnerabilities have been addressed.
- Finally, review procedures, protocols and security tools and change as needed to ensure a repeated breach does not occur.

PLEASE NOTE *that if a breach were personnel-caused rather than a technology-related breach (e.g., a staff member accidentally emailed a report containing bulk Social Security numbers to an outside entity) technology forensics would be replaced with an internal procedures review and possible Human Resources involvement and remediation with education.*

REMEMBER, YOUR ORGANIZATION IS ONLY AS STRONG AS YOUR WEAKEST LINK!

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