2018 Cybersecurity New Year's Resolutions

January 8, 2018

2017 may be behind us, but for businesses that gather and maintain client and transactional data (which is almost all of us), the cybersecurity risk is not. From independently owned businesses to multi-national corporations, all businesses have valuable information that makes them a direct target for cyber theft. Take this opportunity to put your mind at ease, by committing to some simple New Year's resolutions to help protect your business and prevent a cybersecurity or data loss in 2018.

Porzio Compliance Services 2018 Cybersecurity Resolutions

Password Policies

How often do you require employees in your organization to change their passwords? The best practice for many businesses is to change all passwords every 90 days. If you don't already have a password policy in place, institute one now to make it more difficult for hackers to access your systems and data.

Data Backup

Do you backup your data daily? When was last time you tried to restore a backup? Schedule a backup restore exercise the 1Q18. If you are attacked with ransomware, where hackers freeze your system in demand for bitcoin, an up-to-date backup can save your system.

Employee Training

Employees are your first line of defense. Evaluate your company training programs to ensure that your employees have been trained in basic good cyber hygiene. Focus on preventing phishing attacks by teaching employees how to identify questionable emails and what to do if they suspect they have received one. A short employee training session in the first half of the year can prevent malware from entering your system through your employees.

Financial and Data Security Controls

A spearfishing attack is when your employee or your bank receives a directive that appears to be from a trusted source, but it was created by a malicious actor to divert data from your systems or money from your account. To help mitigate this risk, have a policy in place that requires a phone call to be made before certain data or money is transferred, either internally within your organization, or to an external account.

Insurance Coverage

Cyber insurance policies generally cover loss of data. Crime policies generally cover loss of money that is stolen from an account. Sit down with your insurance consultant in the early part of 2018 to make sure that you have coverage for all possible risks. Ask about special riders like a "social engineering rider" to your crime policy to provide coverage before you discover you have been a victim of a theft.

Merchant Credit Card Transactions and PCI

Do you take credit cards as a form of payment? Did you know that if the credit card data is potentially compromised, not even necessarily stolen, you may be liable to MasterCard, Visa, American Express on a per card basis? Anyone who takes credit cards must be PCI Compliant. No later than right after tax season speak to your Merchant Services consultant to ensure that your processes, and any third party vendors' processes, meet PCI compliance standards. You can view more about PCI and PCI compliance in our detailed article, New Year's Cyber Security Resolutions: PCI Compliance [LINK]

Incident Response Plan

What is the first thing that you would do if you thought that your data was compromised? If you can't go to a document that answers that question, consider putting together a team in 2018 that can help to create an Incident Response Plan for your organization.

Schedule a Cybersecurity Audit

What you don't know, can hurt you. Don't be caught off guard – while an IRS audit may not be top on your list of favorite things, an assessment and audit of your current cybersecurity landscape is an incredibly valuable tool to help you allocate resources for protecting private data and minimizing cyber security risk.

Mark your calendar for April 16, 2018 to arrange two assessments:

1. A compliance map of the laws and regulations will help you address data privacy and cybersecurity issues by state so that you can operate your business knowing that you are complying with the myriad of state and federal laws and guidelines.

2. A gap assessment of your current operations against cyber security best practices.

If you would like further information or would like to learn more, Porzio, Bromberg & Newman, P.C., together with Pozio Compliance Services, LLC, Colotraq and Sobel & Co., are hosting a series of roundtable discussions on the topic of data breaches, cybersecurity, and data protection. If you would like to attend, please click here to be added to the invite list.