ST.CLAIR
Solutions
Newsletter

Presented by
St. Clair CPA Solutions
Summer 2018

Is it Time for Your Business to Purchase Cyber Insurance?

Every day a new cyberattack, data breach, or unauthorized release of sensitive information is announced. As technology rapidly changes to improve our businesses, many business owners are finding it cumbersome to keep up with IT security, compliance regulations and understanding cyber liability insurance policies.

Most of us have heard about the major security breaches throughout the past few years. In 2017, Equifax found itself the victim of hackers who were able to gain access to over 145 million names, Social Security numbers, birth dates, street addresses and, in some instances, driver's license numbers. Now let's imagine if all of the personal client information you have in your system was hacked and multiply that number by $233. According to the 2018 Cost of Data Breach Study by Ponemon Institute, $233 is the per capita cost of data breach in the United States.

Hackers are not the only threat. Ransomware can hold your data hostage until you pay a specific fee, but even after you pay, you are not always guaranteed access to your information.

Another threat are your own employees. If a laptop is misplaced or stolen, or if an employee uploads a virus from a CD, flash drive or SD card onto a computer that is connected to your network, there is a possibility of the virus shutting down your system and disrupting your business.

Is your business covered for a malicious cyber event?

Threats are a constant and businesses need to be prepared. On July 23, 2018, the headline of *Investor's Business Daily* reads "AI Disrupts Cybersecurity". "While Artificial Intelligence has improved lives in medicine and other industries, in the wrong hands, hackers can use AI to launch more potent attacks." Cloud-computing service providers are working to improve their security services for clients and the US Defense Department is working to announce a new artificial intelligence strategy sometime this summer. In the interim, your business needs to be prepared for the unknown.

We asked Frank McGee, of The McGee Insurance Group in Merchantville, New Jersey, to provide a high-level overview of what businesses should look for when shopping for a cyber insurance policy.

"No two businesses are the same, and no two cyber insurance policies provide the same coverage," said McGee. "Many first-time buyers of cyber insurance need to be educated on what costs are covered by insurance if a breach occurs. Many times, loss of revenue, business interruption expenses, or remediation fees are add-ons to a policy and not necessarily covered on a standard cyber policy. You need to work with an insurance firm that can determine the specific cyber risks for your company and provide the proper insurance policy to cover these risks."

In This Issue

Cyber Insurance (continued from page 1)

If a cyberattack does occur, business owners need to work with a trusted advisor such as a Certified Public Accountant. An accountant can greatly facilitate the claim handling process by determining an estimate of costs for the amount of time, effort and other resources necessary to resolve the data breach including notification to your clients, regulators or compliance officials. Additional costs to consider include lost business opportunities, the defection of clients, business disruption, costs of acquiring new clients, costs associated with restoring data to your system and restoring the reputation of your business. All of this information will be necessary for a successful resolution of an insurance claim.

After an attack, your business will most likely need an audit, consulting, legal representation and a plan to assess ongoing risk. All of these additional expenses can be paid for with a properly structured cyber liability insurance policy. Recently the Accounting Institute for Certified Public Accountants (AICPA) issued guidance for practitioners to provide a general-purpose report on the effectiveness of an entity's cybersecurity risk management program. To learn how a cybersecurity risk management program can help your organization, please contact one of our professionals.

Michael Mostochuk leads our Enterprise Risk Management practice and works with clients who need SOC reports, risk assessments and business advisory services. To schedule a call with Mike, please contact our Pennsylvania office at 610-862-1998 or email Mike at mmostochuk@stclaircpa.com.

Recent Study Reveals Cost, Means and Ways to Stop Fraud

Would you leave the front door unlocked to your business or not-for-profit organization? Of course not. That would give thieves easy access to your assets. Yet a surprising number of organizations don't have strong antifraud controls in place to protect against dishonest people inside their organizations. And theft from insiders — also referred to as "occupational fraud" — can be costly.

Fraud losses vary significantly, depending on the nature of the scam and how soon it's detected. Globally, the median loss is $130,000, according to the findings from the 2018 Report to the Nations on Occupational Fraud and Abuse by the Association of Certified Fraud Examiners (ACFE). Here's a closer look at who was affected and how much was lost, as reported in the latest version of this biennial study.

Victim Organizations

Fraud can strike any organization regardless of the nature of its operations or its size. The latest ACFE study included 2,690 fraud cases occurring between January 2016 and July 2017.

Cost, Means and Ways to Stop Fraud (continued)

While the news media focuses on high profile fraud incidents involving public companies, the median loss for those companies was only $117,000. Private companies suffered far greater losses — their median loss was a whopping $164,000. By comparison, the median losses for government and not-for-profit entities were approximately $118,000 and $75,000, respectively.

In addition, there are subtle distinctions between the types of fraud schemes that strike small and large organizations.

To Catch a Thief

Small and large organizations also differ in how they catch fraudsters. Tips were the detection method in 29% of the cases involving small entities, compared to 44% of the cases involving large ones. This could result from the prevalence of reporting hotlines, which are more common among larger companies than small ones with limited resources.

Overall, tips are the most common way fraud is initially detected. But it's important to remember that outside stakeholders can also provide tips on unethical behavior. In the 2018 study, 21% of tips came from customers and 9% came from vendors. So, it's important to educate your supply chain partners about any reporting mechanisms you set up.

Top 5 Fraud Schemes by Size: Percent of Cases		
Rank	< 100 Employees	100+ Employees
1	Corruption (32%)	Corruption (43%)
2	Billing (29%)	Non-cash schemes (22%)
3	Check tampering (22%)	Billing (18%)
4	Expense reimbursement (21%)	Cash on hand (14%)
5	Skimming and cash on hand (20%)	Expense reimbursement (11%)

Internal Controls

Beyond tips, a robust system of internal controls can help detect and prevent fraud. The latest study found that 15% of frauds were detected by internal audit procedures and 13% by management review.

Control	Percent Reduction in Fraud Loss
Code of conduct	56%
Proactive data monitoring and analysis	52%
Surprise audits	51%
External audits	50%
Management review	50%
Hotline	50%

What are the critical elements of an internal control system? In terms of lowering fraud losses, the most effective internal controls in the 2018 study were:

On the flip side, weak internal controls often provide dishonest people with the opportunity to steal assets or "cook the books." In the 2018 study, a lack of internal controls and the ability to override internal controls were cited as the leading factors that contributed to fraud. Together, these factors were present in nearly half of the fraud cases in the latest study.

In addition, the 2018 ACFE study inquired about the types of antifraud controls fraud victims had implemented. The report revealed that 25% of frauds at larger organizations were caused by a lack of internal controls. In contrast, 42% of frauds at small organizations stemmed from weak controls. This finding helps explain why fraud seems to hit smaller organizations harder than larger ones.

Lessons Learned

Over the last two decades, the ACFE's fraud report has taught important lessons including: No organization is immune to white collar crime. Driven by this report and recent high-profile public fraud cases, companies have increasingly implemented antifraud controls in recent years.

Cost, Means and Ways to Stop Fraud (continued)

How do your internal controls measure up? Although strong internal controls don't guarantee that fraud won't occur at your organization, they can minimize your losses. We can help evaluate your internal controls and recommend areas of improvement as well as investigate suspicious behaviors and anomalies for signs of white collar crime.

How to Fight Fraud Head-On

Honest employees are an organization's first line of defense against white collar crime. Here are some ways you can encourage employees to join in the fight:

Invest in training. Educate staff on the red flags associated with fraud from within and outside the organization. This helps detect and prevent fraud. It also sends a powerful message about your intention to fight fraud no matter where it originates. Employees must perceive a high probability that fraudulent activity will be detected. The perception of detection is often sufficient enough to dissuade those inclined toward unethical behavior.

Engage management in the fight. Managers must be seen and heard reviewing controls and urgently correcting weaknesses that might be detected. If your organization's managers are perceived to be unwilling or unable to review the controls, they may inadvertently be sending a message that it's safe to commit fraud.

Set up a hotline. Anonymous fraud reporting hotlines are an effective method of obtaining tips about unethical behavior. Unfortunately, many small organizations shy away from this option, because they see it as too expensive and difficult to administer. A number of providers offer hotlines designed with small organizations in mind. The cost per employee is minimal in relation to the fraud it can help to uncover and the losses avoided.

The 2018 *Report to the Nations* found that employers were much more likely to be tipped off if they offer reporting hotlines. The study found that tips led to the detection of fraud in 46% of the cases involving organizations with reporting hotlines, but only 30% of the cases involving organizations without hotlines. Another interesting finding: More than half of complaints were submitted via email or an online form. This suggests that companies with telephone-only reporting hotlines should consider adding more technology-based channels for reporting fraud.

Frances Sperling Feldbaum is one of our subject matter experts in the not-for-profit industry at St. Clair CPAs, P.C. To schedule a call with Fran, please contact our New Jersey office at 856-482-5600 or email Fran at fsfeldbaum@stclaircpa.com.

Federal Tax News

The Social Security "wage base" could increase to $132,300 for 2019.

The Social Security Administration's Office of the Chief Actuary (OCA) is projecting that the wage base will increase from $128,400 for 2018 to $132,300 for 2019. The wage base is the maximum amount of earnings subject to Social Security tax. Although the OCA has just projected next year's amount, the actual wage base will be announced in October. The OCA is also projecting that the Social Security trust fund will become insolvent in 2034.

The IRS issues next year's inflation-adjusted Health Savings Account (HSA) figures.

For calendar year 2019, the annual contribution limit for an HSA for an individual with self-only coverage under a high deductible health plan (HDHP) will be $3,500 (up from $3,450 for 2018). For family coverage, the contribution limit will be $7,000 (up from $6,900 for 2018). To qualify as an HDHP, a health plan's annual deductible must not be less than $1,350 (same as for 2018) for self-only coverage or $2,700 (same as for 2018) for family coverage. (IRS Revenue Procedure 2018-30)

More than 2 million Individual Taxpayer Identification Numbers (ITINs) will be expiring.

An ITIN is a tax processing number available for certain non-resident and resident aliens, their spouses and dependents who can't get a Social Security number. The IRS is urging people with ITINs set to expire to submit renewal applications soon. Expiring at the end of 2018 are ITINs not used on federal tax returns in the last three consecutive years and ITINs with middle digits 73, 74, 75, 76, 77, 81, or 82. For more info: https://bit.ly/2thxcI8

Is money left in a tip box subject to FICA tax?

Workers and employers pay FICA tax on tips reported to the IRS. In one case, a taxpayer engaged individuals to perform services and paid them only tips left in a tip box by customers. The taxpayer wasn't involved in the collection or distribution of the tips and didn't report the amounts to the IRS as compensation. The IRS, in a Chief Counsel Advice, found the individuals to be employees, and the tips subject to the employer share of FICA under the tax code's "notice and demand" procedures. (CCA 201816010)

A taxpayer's rejected offer in compromise (OIC) is upheld.

An OIC is an agreement between a taxpayer and the IRS to settle a tax debt for less than the full amount owed. But certain requirements must be met. The IRS considers a person's income, ability to pay, expenses and asset equity before accepting an offer. The U.S. Tax Court recently upheld the rejection of a taxpayer's OIC. The court determined that the IRS hadn't abused its discretion in rejecting the taxpayer's OIC. The offer didn't reflect the reasonable collection potential, based on the IRS's local allowances for living expenses. The taxpayer disputed these allowances but failed to prove they were inadequate. (TC Memo 2018-54)

James Knight, CPA is one of our tax practice leaders at St. Clair CPAs, P.C. To schedule a call with Jim, please contact our Pennsylvania office at 610.862.1998 or email Jim at jknight@stclaircpa.com.

In Our Community

Walk Against Hate

On Sunday, June 3rd, hundreds of individuals met at the Marine Parade Grounds located in the Philadelphia Navy Yard to enjoy a morning of family entertainment and camaraderie. The event was in support of the Anti-Defamation League® (ADL) of Philadelphia. The ADL's mission is to protect the civil rights of all individuals, no matter their race, religion or country of origin. Alan Gubernick, Shareholder at St. Clair CPA Solutions, is the current President of the Philadelphia Chapter of the ADL. Dozens of our employees, along with other businesses, their employees, family, and friends from across the Philadelphia region, participated in the 8th annual Walk Against Hate to celebrate diversity and challenge bigotry.

Supporters raised awareness of the injustice of prejudice and bias taking place in the 21st century, while also celebrating tolerance in our community by walking along the banks of the Delaware River and throughout the Navy Yard.

Dress Down for Charity

For a donation of $5, any employee may wear jeans to work on Friday. Each month a new charity is selected from recommendations received by our Employee Relations Committee.

Throughout the month of May, our donations to Little Smiles was in honor of Julia Bitto. In 2017, Julia was diagnosed with Diffuse Intrinsic Pontine Glioma (DIPG), an extremely rare brain tumor. In June, our employees "dressed down" to support the Asthma and Allergy Foundation of America (AAFA), the oldest asthma and allergy patient group in the world. During the month of July, our employees supported The Society of St. Vincent de Paul, a society of trained volunteers In the United States that helps more than 20 million people through visits to homes, prisons, and hospitals.

Professionally Speaking

On June 26th, we met with student entrepreneurs participating in the Haverford Innovation Program this summer as part of Haverford College's Innovation Incubator Fellowship.

Stephanie Sommers, CPA and Glen Dymond, CPA provided a primer on ***How to Start a Business*** to the student entrepreneurs and owners of "Dibs," a community-based food app for college students; "Sekhs," a documentary, videography and photography company and "Beyond the Bell," a 2-hour walking tour of Philadelphia where you will learn about the people, controversies and secret histories that have formed the City.

Special thanks to Shayna Nickel for inviting us to attend!

Keep in touch! Follow St. Clair CPA Solutions on LinkedIn!