VARNEY CAREs

COMMUNITY • ACCOUNTABILITY • RELATIONSHIPS • EXCELLENCE

Varney & Associates, CPAs, LLC | 120 N. Juliette Avenue, Manhattan, KS 66502

Vol. 1 Issue 4 | July 2019

INSIDE THE ISSUE

How Safe is Your IT Environment?

By Rich Boggs, Information Technology Director

We all think that we are above the rest and won't be attacked. Nobody will ever hack our systems because we are always very careful in what we do. We know nobody will guess our passwords, and we are 100% sure that the websites we visit are authentic and nothing would ever come from that. In today's world, you can never be too safe when operating a PC. Below are what we believe are the top eleven best practices in keeping your business as safe as you can. Remember, it isn't a matter of if we will be attacked, it is a matter of when. Are you prepared?

1. **Training is crucial**

   Information security is your number one priority and if your people don't know policies and procedures, you might be exposed to significant risk. Train all employees and Board members on IT security principles, policies and procedures. Consider offering training with tests at the end to ensure the information is understood.

2. **Protect your information on ALL computers and servers**

   Is your data encrypted at rest and in transit? Do you allow confidential information to be stored or saved on workstations?

3. **Have a firewall that is up to date at the edge of your network**

   Make sure this firewall has the latest firmware. Does it have intrusion protection services (IPS) installed? Stateful packet inspection (SPI)? What about Gateway Anti-Virus, Spam filtering, application filtering? Make sure your firewall is best suited for your business so that you know you are best protected from all the risks you are exposing yourself to. Does somebody in your organization look at the logs for this every day?

4. **Make sure you are securing mobile devices**

   Most people think about cell phones or laptops when the term mobile devise comes up. What about tablets, USB drives, portable hard drives, backup tapes that might be moved from site to site? Do you have policies in place that state these devices must be encrypted? Do you allow confidential information to be stored on them? What is the action to be taken if one is lost? Can you remote wipe them? Do you physically inspect computers to control the connectivity with mobile devices?

5. **Backups, Backups, Backups**

The most important thing you can do is backup your critical information. The rule of backups is to have three copies of your data. One in production, one backup copy of that data onsite stored on a different device, and one copy of that backup data offsite. We also find that, when using a backup storage device on your local network, it is more secure not to add that machine to the domain. In the event you inherit some kind of local network virus or malware, that machine will not be infected if the virus or malware gets ahold of credentials that has access to your backup storage device. Keeping it separate is a good idea.

6. **Control physical access to all computers and networking equipment**

All equipment should be in a place where it is hard for the general public to gain physical access. On top of that, each user should have a unique username and password to gain access to all systems. If you want to make it even more secure, don't allow the same usernames for each system.

7. **WiFi networks**

Do you have one? If so, is it secure? Is it hidden? Do you allow public access? If so, is it on a different network than the rest of your network?

8. **Wire and ACH systems**

When you implemented these systems, did management change the default dollar amounts? These systems are generally setup by default to let hundreds of thousands of dollars through, sometimes millions of dollars. Go in and change the setup so that each user is limited. Do you allow your system administrator to send or verify wires? They probably shouldn't. And somebody other than them should review the logs every day.

9. **Limit employee access to data and the ability to install software**

Employees should not be able to have access to every folder on the network. They should only have access to what they need, not what they "might" need. Employees should also be restricted from installing software to company equipment.

10. **Patching**

Keeping your systems up-to-date with both Microsoft and non-Microsoft patches is vital to your organization. There are several pieces of software on the market that can help you with this and have great reporting features. Don't let that automatic update fool you. Be sure to check at least monthly to ensure that patching is happening correctly.

11. **Password Security**

Your password should never be able to be found in any dictionary. It shouldn't have repeating values, and it should have at least one uppercase, one lowercase, a special character and a number and at a minimum, should be nine characters long. We understand that there are some systems out there that will not allow this, but make sure you are making it as strong as possible. Passwords should also not be reused in less than a year, nor should a user have the ability to change their password more than once in a twenty four hour period. User should be locked out after three to five unsuccessful login attempts so that hackers can't continue to use that account. One last note, if you are having a hard time figuring out a good password, don't use a "word", develop a phrase. They are much easier to remember.

While these steps are not meant to be all-inclusive, they are great measures to ensure the security of your bank environment. We, as business owners and end users, must take information security very seriously. It only takes one wrong click to invite the bad guy in.

Rich Boggs
IT Director

Rich Boggs is a seasoned IT professional with Varney & Associates, CPAs, LLC, with over 22 years of experience as an IT Specialist. He is responsible for the firm's IT needs, and regularly performs IT consulting projects, including IT assessments, cybersecurity audits, and vulnerability assessments. You can reach Rich at rboggs@varney.com or 1-800-240-5004.

"Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge." - Bruce Schneier

KSU Accounting & Technology Conference

October 3rd and 4th, 2019

https://conferences.k-state.edu/accounting-technology/

Fraud Prevention in Small Governments

By April Swartz, CPA, CGFM, Owner

Is it possible for a city comptroller to steal over $53 million from a city of just 16,000 people with an annual budget of less than 10 million? The answer is **yes**. *All the Queens Horses* is a Netflix documentary of this very fraud scheme that took place in Dixon, Illinois. Why did the government officials not detect the fraud? How could a fraud exist for over 20 years without detection? Is fraud – like this one, but smaller in size – occurring in your own government? Establishing an anti-fraud culture is more important than ever for small government entities.

Many small governments suffer losses from theft since they lack a sufficient number of employees to segregate accounting duties. There are, however, steps you can take to protect the government's resources.

Most government officials don't realize that external audits are not designed to detect *immaterial* fraud. *Immaterial* fraud can be tens of thousands of dollars, or even more. Such officials incorrectly believe that a clean opinion means no fraud is occurring in their organization – this is a mistake. The external audit cannot be considered part of the government's internal control system. Internal controls should be implemented to reduce the risk of fraud.

Effective controls not only safeguard the government's assets, they are important to protect employees from unwarranted and false accusations in the event of a theft or other manner of fraud.

The smaller the government, the *greater* the need for fraud prevention. And yet, *these* are the governments that most often don't have the resources – whether it's money to pay for outside assistance or employees to segregate duties – to prevent fraud. Here are a few ideas for even the smallest of governments.

Low Cost Fraud Prevention Options

- Have all bank statements mailed directly to a member of the governing body (mayor, council member or commissioner), who will open and inspect the bank statement activity before providing the bank statements to the employee that reconciles the accounts. Bank statements should be initialed to document the review. If online statements are utilized, give the mayor online review access and provide a method to document the reviews.

Changes in Yellow Book Audits Regarding Independence…

- Audits performed under generally accepted government auditing standards (GAGAS) are subject to new rules reinforcing the principles of transparency and accountability under revisions published by the U.S. Government Accountability Office (GAO) in July 2018.
- The primary area of concern involves the preparation of financial statements as part of the audit engagement.
- The new guidance states that when preparing a client's financial statements in their entirety from the client's trial balance or underlying accounting records, auditors should conclude that *significant threats* to independence exist. Under the Yellow Book's conceptual framework approach, when a firm encounters *significant threats* to independence, the firm should apply safeguards to eliminate or reduce the threats to an acceptable level.
- Threats are at an acceptable level when a reasonable and informed third party would conclude that the firm could perform the audit without compromising its professional judgment. Possible safeguards the auditors could apply that could be effective for potential threats are: 1) separate personnel perform the audit and preparation of the financial statements; 2) an independent party from inside or outside of the firm performs a second review of the financial statements prepared.
- The revisions to the Yellow Book provide new application guidance on evaluating whether a client has sufficient skills, knowledge, or experience to oversee a nonaudit service, such as financial statement preparation. The guidance provides that an indicator of management's ability to effectively oversee the service would include the ability to recognize a material error, omission, or misstatement in the results, or the reasonableness of the results.

- Once or twice a year, have governing body members pick two months at random and review key bank statement activity.
- Once or twice a year, have governing body members randomly select checks (vendor payments and payroll) and review the supporting documentation.
- Once or twice a year, have governing body members review receipt collections and related documentation; agree receipts to bank deposits and to the general ledger.
- Provide monthly budget to actual reports to the governing body.
- Require two signatures on checks above a certain level; have two of the governing body members on the bank signature cards; supporting documentation should be provided to check signers for review.
- If credit cards are provided to employees, make sure the maximum credit limit is low. Credit card statements should be provided to check signers.
- Use a centralized receipting location; receipts should always be written upon collection of a payment.
- Have your independent auditors make surprise, unannounced visits to examine the receipting system, payroll, and the payment system.

Higher Cost Fraud Prevention Options

- Install a security camera to record all of the collection and receipting activity.
- Purchase fidelity bonds to cover elected officials and employees.

Three Types of Fraud

1. Asset Misappropriation: An employee steals or misuses the organization's resources (e.g., theft of company cash, false billing schemes, or inflated expense reports).
2. Corruption: An employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit (e.g., schemes involving bribery or conflicts of interest).
3. Financial Statement Fraud: An employee intentionally causes a misstatement or omission of material information in the organization's financial reports (e.g., intentionally recording fictitious receipts or understating expenditures).

April Swartz, CPA, CGFM
Owner

April Swartz has more than 36 years of experience working with Kansas governmental entities. She is a CPA and a Certified Government Financial Manager. She has been with Varney for 11 years. April primarily focuses on governmental entities, including audit, budget, and other consulting services. April is a graduate of Emporia State University with a Bachelor's of Science in Accounting. You can reach April at aswartz@varney.com or 785-537-2202.

The 2018 revision of the Yellow Book by GOA is effective for financial audits, attestation engagements, and reviews of financial statements for periods ending on or after June 30, 2020. See www.gao.gov/yellowbook/overview.

The Faces of Varney

While our team may have changes over time, we continue to strive to be the best we can for our clients. At Varney, we are committed to teaming you up with the right professional, best served to meet your needs. Here are the members of the governmental team of Varney:

VARNEY & ASSOCIATES, CPAs, LLC

"Leading the way to your success."

April Swartz, CPA
Owner

Eric Kientz, CPA
Principal

Michelle Crow, CPA
CEO/Owner

Amanda Vankleeck
Principal

Taylor Penick, CPA
Manager

Trisha Bradley, CPA
Manager

Jenn Hildebrand
Manager

Jessica Lindsley
Senior Accountant

Megan Niedens
Senior Accountant

Taylor Oliver
Staff Accountant

Madison Hammett
Staff Accountant

We take care of governmental organizations so they can take care of their communities.