message from the board

Mid-Columbia Members,

November is here and the holidays are fast approaching!

We hope you enjoyed last month’s luncheon presentation on “Fighting Today’s Fraud.” This month we are welcoming Andrea Greenwell and Jessica Shaw from Washington River Protection Services’ Ethics and Compliance for “Internal Audit and Conflicts of Interest.”

We have great news, Steve Hunt is coming back for a one day excel seminar where he will provide hands-on training from some of excel’s most basic to its advanced. We have a tentative date set for Tuesday, April 7, 2020 so mark your calendars! More details to come.

Have a great month and happy auditing!

Mid-Columbia Chapter Board Members

audit career center
Advance your internal audit career or strengthen your team with The IIA’s Audit Career Center resources.

upcoming webinars

PSAC Virtual Symposium: Preparing Public Sector Auditor’s for Today’s Terrain

Members-Only: Blockchain Technology: What Internal Auditors Should Know

2020 Seminar Details:
“Excel For Auditors”

PRESENTED BY: Steve Hunt, Internal Audit Manager for Spokane Teacher’s Credit Union
When: Tuesday, April 7, 2020
Where: CBC, Pasco Campus

This one day hands-on seminar will break down excel from basics through advanced tips that you can later implement in your field of work. Bring your laptop!

Stay Tuned for More Information to Come!

About Steve Hunt:

Steve Hunt earned his Bachelor of Arts degree from Eastern Washington University majoring in both Management Information Systems and general business management. He maintains the CIA, CISA and GIAC certifications. Steve is a self-proclaimed Excel guru. In his free time, Steve enjoys woodworking, DIY home projects, playing with his four children, backpacking and camping.
**WHAT’S IN THE NEWS?**

**Fraud Basics:** “It’s not just VCRs they’re after anymore” Tips for Identifying Fraud in the Workplace:
By Sean McGrath, CFE, CPA

Audit programs: Sure, effective audit programs will help detect unauthorized access to information. Most internal auditors and fraud examiners can design appropriate audit procedures to detect fraudulent behavior. However, a well-designed audit program shouldn’t be reactionary; it has to proactively dissuade employees from committing fraud. Organizations should give all employees anti-fraud training and then administer annual assessments and mandatory tests.

Organizations that communicate their audit programs to all employees will reduce potential fraudsters’ perceived opportunities to commit fraud. However, simply advising employees that an auditing program is in place will do little to prevent would-be fraudsters if organizations don’t facilitate programs effectively. They must run regularly scheduled audits for all those who have access to databases that store confidential information.

Organizations should notify employees when it will review their audit logs and audit results but also — and this is important — run surprise audits when key players are at work and when they’re away from the office.

Don’t hide it: If your organization discovers unauthorized or fraudulent activity notify all employees. This sounds basic, but many organizations keep their internal investigations under wraps. While you shouldn’t share personal details of the fraudster and the crime, tell everybody you caught an employee.

Sharing the detection of fraud with employees has a two-pronged effect. Foremost, it proves that your auditing program is effective, which should deter similar employee behavior. Secondly, it sets a tone from the top that management doesn’t tolerate such behavior.

**12 Quick Ways to Protect Your Company From a Business Email Compromise Scam**
Oluwaseun Akomolafe, CFE
Fraud Analyst, Interswitch

Business email compromise (BEC) scams have never been more pronounced than they are now. Last month, the FBI executed their most sweeping takedown ever of BEC scammers, resulting in 281 arrests in several different countries. Even large global companies like Toyota aren’t safe from this type of scheme, as they found out when a BEC scam led to the loss of $37 million from one of their parts suppliers. Small
and medium-sized businesses aren't safe from the attacks, either. A California firm got hit by a scam that resulted in $46 million in losses. The ACFE has been talking about how to protect your company from a business email compromise scam since 2016, and the scheme has only gained momentum since then.

Here's the problem. In order to stay ahead of your competition, your organization probably uses tools and processes which make decision-making faster, removing traditional bottlenecks which can stiffen business in a very competitive, profit-oriented environment.

But this is just how BEC scams can slip between the cracks. They come in ways that typically mimic or follow normal business interactions, but include an unusual and urgent request for money, data or both. The endgame of the attacker is the decider here. Some fraudsters might share the information in a public space just to show how vulnerable an entity is, which can wreck an organization's reputation, while some fraudsters are only focused on financial gain.

Since 2013, when the FBI began tracking this emerging financial cyber threat, organized crime groups have targeted large and small organizations in every U.S. state and more than 100 countries around the world — from nonprofits and well-known corporations to churches and school systems. Losses are in the billions of dollars and climbing.

It is noteworthy that BEC is now one of the most common and prolific fraud schemes. With that chilling thought in mind, here are 12 quick ways you can protect your company from a business email compromise scam:

1. Run scheduled and periodic scans of email activities of top management, especially those charged with finance approvals.
2. Periodically review your email subfolders. Some fraudsters, after gaining access to a legitimate email account, might create subfolders with a rule to ensure fraudulent emails are separated from the usual view of the authorized mail owner.
3. Always closely read the sender’s email address of every single email. Check for misspelled words. For example, upper case ‘i’ and lower case ‘L’ are deceptive characters and difficult to notice with just a quick glance.
4. Check for grammatical errors or inconsistencies in mail composition compared to what you are used to in dealing with vendors, coworkers or your superiors.
5. Stolen or misplaced identification documents should be reported to the police or internal security as a matter of urgency.
6. Embrace dual-level approval for transaction payments relating to third parties.
7. Do not rely on one medium of communication (especially emails) for financial approvals. Other documented processes should be adopted to run parallel for payment approvals.
8. Disperse authority. For example, the finance person should not be responsible for all payment lines.
9. Regularly reconcile bank statements. This will help to flag suspicious activity in a timely manner and deter further exposures.
10. Regularly inspect and review the corporate email control panel for redirect rules that are unusual or suspicious.
11. Limit information about employees on social media and the company website, especially information about job duties and descriptions, organization hierarchy and out-of-office details that show delegation of authority.
12. Continuously educate and train employees on email security by staying up to date on the latest trends and stories in BEC scams.

October is National Cybersecurity Awareness Month, so it’s a great time to share these tips with your friends, family and coworkers. As simple as this fraud scheme may sound, the losses that arise from it are often big and quite damaging. The more you share your knowledge, the more effective you’ll be at protecting your company from business email compromise and other similar schemes.

**DID YOU KNOW?**

 Leakage 50 million pumpkin pies are baked every year, and according to the American Pie Council, 1 out of 5 Americans has eaten an entire pumpkin pie by themselves.

 Leakage The first recorded recipe for “modern” pumpkin pie was published in 1796 and it was called “Pompkin Pudding.” The first pumpkin pies were actually whole baked pumpkins stuffed with assorted spices and apples.

 Leakage The world’s largest pumpkin pie weighed over 350 pounds and was made with 80 pounds of pumpkin, 36 pounds of sugar, 144 eggs, and baked for six hours!