CPA
Practice Advisor

technology that can catch them long before they can cause serious damage. Here are 5 things you can do today that will help your team fend off future attacks.

Aug. 24, 2021

By Catherine Dahl.

Accounts payable fraud is an all too common occurrence in today's ever-increasingly digital world. According to a recent survey by the Association for Finance Professionals, nearly 75% of all organizations were targeted by a fraud attack in 2020 – a truly staggering statistic. After the disruption caused by the pandemic, companies might feel ill-prepared against a possible security breach.

Cyber-criminals may have become craftier, but we now have access to the latest technology that can catch them long before they can cause serious damage. Here are 5 things you can do today that will help your team fend off future attacks.

Revisit your approvals strategy

manager needs to be involved in approving their expenses and if they are over a certain dollar amount, a senior manager needs to be involved.

- Assign two people to approve payments: Tighten your controls around how funds leave the business by assigning payments approval to more than one senior leader. This will bring accountability into the process.

- Support purchases with an approved Purchase Order (PO): Depending on the business size, purchases going over a certain amount should be supported with a PO that goes to a senior manager for approval.

- Periodically audit invoices as they go through the process.

Formalize the vendor setup process

Often there is no authorized plan to add new vendors except for a check request or an email submission. Setting up new vendors needs to be a strictly controlled process. This prevents any one person from having too much control over financial funds and minimizes the risk of fraud. You can document a vendor onboarding plan that identifies the method of payment, primary contact to initiate change, payment processing time, escalation process, etc.

A common sign of external fraud is a bank change request, often in the guise of an odd email asking the payment to be wired to another account. To avoid this, the accounting department can use a bank change form to initiate change. This means, when your AP team receives a call or email asking for banking details to be amended, it can only be processed once the form has been filled by the assigned individual. Another option is to ask questions to confirm the legitimacy of the request: *What's the last invoice amount? When was the last payment made?*

Ask questions about expenses

While employee education is important to deter external fraud, strict controls within

documented.

Secure proper backup for all expenses and invoices. A packing slip is not an invoice, an order confirmation is not an invoice, and a screenshot is definitely not an invoice. The same goes for expenses. Request for original receipts and credit card statements with the name and account number of the expense owner – secure all the backup documentation that proves that the expense was paid for by the claimant.

All hands on deck

Your employees are the best resource you have when it comes to identifying a threat. Managers do not always have the time to look out for potential risks and should be able to trust their team to be the first line of defense.

The same study reveals that common sources of fraud include easy targets like forged checks, stolen cards, or full-on account takeovers by career hackers and spyware. But perhaps the most dangerous type are business email compromise scams: criminal gangs posing as legitimate vendors, mysterious third parties requesting sudden bank changes, or even worse, an imposter pretending to be a senior executive demanding an immediate transfer of funds.

By coaching your employees on how to recognize these red flags and raise the alarm, you won’t have to deal with the lost time and money that comes with dealing with fraud.

The case for digital transformation

Another tactic to prevent payments fraud is to digitize and automate your accounts payable process. By taking human error out of the equation, an automated AP workflow solution will be able to spot duplicate payments much easier and faster, as well as flag any errors or suspicious activity in real-time. Accounting teams can then investigate the problem and decide whether it was a mistake or a potential fraud

payable (AP) automation software. A CPA for more than 25 years, Catherine has steered Beanworks to become one of the fastest-growing organizations in British Columbia. Catherine is an advocate for diversity, equity, and inclusion in the workplace and has been championing this cause within Beanworks since its inception back in 2012.

Accounting • Auditing • Benefits • Technology

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.