How Secure is AP Automation?

By NE Docs | November 4, 2019 *0 Comment*

We’re always glad to hear this question. Accounts Payable Automation simplifies the AP processing workflow and improves performance by reducing errors and costs. But in this day of ransomware attacks and corporate data breaches, is automation safer than current manual processing methods? We certainly think so and will explain why.

Financial processes have always faced numerous security risks from external as well as internal threats. These include fraud, hacking, skimming, check tampering, and incorrect expense reimbursement. These risks continue to threaten your organization’s finances and reputation. But automation can reduce the risk by removing manual processes, requiring authentication of users, and applying ongoing security checks.

The first step to understanding the security risks for your AP processing is looking at the common causes of data breaches. The second step is getting familiar with how automation of your AP processing workflow actually works by working with a trusted expert who can help you determine your risks.

Common Causes of Data Breaches

Let’s look at the five most common causes of data breaches according to Hollywood, Florida-based

WHOA.com, a managed IT services firm.

# 1 – Outdated, Old or Unpatched Computer Systems

A computer vulnerability is a defect in a system that can leave it open to a cybersecurity attack. What often happens is that overburdened IT resources do not keep up to date with patches to remedy those old security vulnerabilities, permitting hackers a free pass to your company's most sensitive information.

# 2 – Mistakes

When we humans are involved in performing manual tasks, there is a higher risk of errors and accidents. For example, employees may use weak passwords or accidentally send sensitive information to the wrong recipients. Other mistakes happen when employees share password/account information, or unknowingly fall for phishing scams where bad actors convince the victim into divulging information that risks personal or company data. (Phishing involves sending fraudulent communications that appears to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.) By automating your accounting processes, you remove the possibility of human error.

#3 – Malware & Ransomware

Unfortunately, there are bad players around the globe bombarding our personal and company systems and devices with malicious software referred as "malware." You may have heard such terms as spyware, ransomware, viruses or worms. Malware breaches a network through vulnerability. For example, a user clicks a link or email attachment that then installs the malware code, which may:

- Block access to key network and file components in demand for money (ransomware)
- Obtain secret information by transmitting data from the individual's hard drive (spyware)
- Disrupt computer resources and services, rendering the device inoperable

# 4 – Insider Fraud or Misuse of Information

Insider misuse is the deliberate abuse of company systems by an authorized user, typically for personal gain. The issue is that this person is someone that the organization trusts. Whereas, preventing insider abuse is almost impossible, damage can be limited by compartmentalizing information on the network or cloud. The fewer files and systems a single user can access, the harder it is to abuse.

#5 – Device Theft

Another risk is the physical theft of a device that holds your company's sensitive information. This can include such devices as laptops, desktops, smartphones, tablets, hard drives, thumb drives, CDs and DVDs, or even servers. A simple best practice is to reduce the opportunities for removing data-storing devices from the work environment.

Secure Your AP Processing with a Proven Strategy

The key to securing your automated AP processing solution is working with a trusted expert in AP

Automation who can layer end-to-end security checks along the entire AP process, essentially “baking” security into every aspect of the AP processing workflow.

NEdocs provides a leading cloud-based AP Automation platform that helps medium and large organizations in all industries remove paper from processes, eliminate the wasted time caused by manual invoice processing, add layers of data security and reduce costs associated with inefficiencies within financial departments.

Vision360 Enterprise automates the processing (routing, approving, coding, matching and posting) of supplier invoices as well as purchase order requisitions, check requests, payment processing and electronic expense reports. Organizations can further leverage their ERP investments by using the Vision360 platform to automate and connect their AP processes with their ERP financial system.

Safe and Compliant Solution

Compliant with the SOC 2 Type II controls, this solution ensures your AP processing is secure by eliminating the common issues exposing companies to data breaches. For example, the solution has controls in place to ensure system components are automatically updated whenever software manufacturers provide updates, closing system gaps that could potentially be vulnerable to attackers.

Disaster recovery and backup resources as well as fraud detection and prevention components guard against loss of data or intrusion by bad actors that are looking to insert malware. The automated processes control who has access to AP processes and data throughout the workflow, preventing mistakes and abuse. The platform generates tremendous savings to organizations by eliminating paper-based processes, streamlining the routing, coding, matching and posting of supplier invoices.

For further information about AP automation and how you can deploy a safe, secure solution, call NEdocs today at (603) 625-1171.