Installing a digital front door to an ERP strengthens cybersecurity measures

Cybercriminals have proven remarkably agile in their tactics to counter manual security measures introduced by most businesses. At the same time, businesses find it challenging to remain in a state of constant vigilance and are finding that implementing the right technology can reduce their risk significantly. Currently, 71% of companies have reported being a victim of a payments fraud attempt in 2021, with 75% experiencing compliance risk. Of note, a significant portion of these fraud scams would not be stopped, even by the most robust cybersecurity, because they focus on tricking a human, not hacking a system.

Three P's: The people process problem

Social engineering, a type of fraud using deception but that is sometimes carried out through a technology hack, has gained traction in recent years and succeeds by focusing on the weakest link in a company's security arsenal – its personnel.

These kinds of attacks, which can range from vendor impersonation to spoofing to fraudulent urgent requests, have wide-ranging consequences – from huge monetary losses for an organization, to career-ending mistakes for the employee in charge. Yet, according to PaymentWorks, Inc. customer data, 99% of organizations rely on a manual process for managing supplier identity. To protect a company's assets, both material and otherwise, security measures beyond demanding your staff to 'be careful' are crucial.

With its reliance on manual processes, ultimately, stopping fraud is not just a technology problem, it is a people process problem that opens the door for this kind of fraud to succeed. Either employees unintentionally break the policies in place (is it really a process if it's never followed?), or organizations (universities, colleges, healthcare entities, federal agencies, etc.) retain stagnant processes for social engineering, and fail to keep pace with ever-evolving sophisticated attack methods.

This threat comes into play most often in two ways:

1. Enterprise resource planning (ERP) system conversions. When an organization converts to a new ERP system, it needs to alter payment processes and adopt a new vendor management module. With data in flux, the information is increasingly vulnerable. The team is often asked to do more, leading to more points of failure. With this in mind, it is important for leaders to

automate processes before a system conversion and set up layered approaches to protect the vendor master file, a complete repository of data and intel on an organization's vendors.

2. Changes to the vendor master. By far the most targeted entry point for these scams is the door to the vendor master. When supplier identity information is changed, there is an opportunity for fraud.

Guarding the vendor master file

When a person in procurement oversees gatekeeping the vendor master – especially in a distributed procurement model – there is naturally more room for error, something cybersecurity or cyber insurance cannot protect or insure against.

As the repository of all data collected from vendors and business partners, the vendor master file requires near constant updates and vigilance. A digital front door that serves as the gateway to the ERP and the identity information it stores is a wraparound security approach that protects both the payee and the payer. PaymentWorks, a business identity platform, and a Huron partner, serves as that digital front door – providing a platform to collect and verify information, before it's entered into the ERP, with a workflow that provides an auditable onboarding and approval trail to guard against attack. The platform offers a way to get a consistent process in place and provides automated validation to prevent personnel from being tricked.

This doesn't necessarily mean that an organization's ERP is no longer the system of record. The ERP must be updated with the information, which will then update PaymentWorks. The onboarding process with automated validation and verification checks ensures that nothing gets changed within the ERP without passing its tests. Protecting against fraud is certainly the goal, but with clean vendor master data, data that is up-to-date and trustworthy, compliance issues are solved for as well! Huron can help with this in getting the most out of PaymentWorks and all the capabilities available.

For PaymentWorks to ensure full protection against fraud, the platform also checks out any information that is leaving the ERP to be used for bank transactions. This payment security check protects against any process failure by processing a final risk assessment and vetting the payment credential information from the ERP before it goes to the bank, protecting both the front and the back door on each vendor transaction.

Protecting personnel from risk

Fraudsters typically operate like they are playing a game of chess – patient bad actors that play a long game waiting for casual human errors. While strong cybersecurity measures protect your organization from internally generated scams, they cannot detect hacks at the vendor level. Without a guard in place, any kind of information can flow into the system and result in fraud. You need to win the defensive game at the point of entry, not just at the time of payment.

For this to be successful, an important shift needs to occur. Right now, far too many organizations are relying on personnel to spot and stop fraud, with the same rigor and risk assessment being applied to every interaction. The scope of the job is enormous, and it's likely not even the person doing its primary responsibility. People can make honest mistakes, and while it is one thing to not follow the process and encounter fraud, it's increasingly likely that your person will follow your process and still be tricked. The human toll can be huge. A vendor desk contact of PaymentWorks at a large state school in the Southeast described the stress like this: "I feel as if I am holding a hand grenade with the pin pulled every time, I input a bank account change to our ERP."

It is a balance between empowering and educating employees and employing the right technology to create optimal security measures.

Policies, processes, and training are all important and can help influence human behaviors, however, establishing rigorous policies and processes that are constantly updated based on sophisticated attack methods requires constant vigilance. Giving your personnel tools which remove the guesswork from their jobs and protect the vendor master from hijacking, will not only bolster your defenses, but will create room for your staff do to their actual full-time jobs and foster less stress in work environment. The more elements that you can layer, the better the opportunity to continually protect against attacks.

HURON

huronconsultinggroup.com

About Huron
Huron is a global consultancy that collaborates with clients to drive strategic growth, ignite innovation and navigate constant change. Through a combination of strategy, expertise and creativity, we help clients accelerate operational, digital and cultural transformation, enabling the change they need to own their future.

About PaymentWorks
PaymentWorks provides digital onboarding for secure, compliant, and optimized business payments. Featuring the industry's only payments security platform and a network of tier one partners, PaymentWorks enables customers across healthcare, higher education, state and local government and enterprise and more to capitalize on the opportunity to digitize the payments process while minimizing costs, ensuring compliance, and reducing the overall risk of fraud.