CPA
Practice Advisor

ACCOUNTING & AUDIT

Finance Professionals Offer Powerful Defense Against Cybersecurity Threats

The 2022 AFP Payments Fraud and Control Survey found that 71 percent of organizations were victims of payments fraud attacks or attempts last year.

Sep. 29, 2022

By Christina Quaine.

A recent PwC survey found that rising cybersecurity threats are the number one concern for CEOs around the world. It's not surprising, as malware, ransomware, and phishing scams that provide criminals with access to sensitive customer and financial information can result in hefty financial loss and do irreparable damage to a firm's reputation.

As firms look to better protect themselves, payments remain a key area of concern. The 2022 AFP Payments Fraud and Control Survey found that 71 percent of organizations were victims of payments fraud attacks or attempts last year. Checks, still a primary payment source for many businesses, were the payment method most impacted by fraudulent activity, accounting for 66 percent of attacks.

Firms have powerful allies at their disposal to help protect against the growing threats—the finance and payments team. These professionals can leverage advanced technologies, including artificial intelligence (AI), and security best practices to keep a watchful eye and ward off potential attacks.

Here's a look at just how they can serve as an effective layer of defense, strengthening protection in their organizations from cybercrime that can have devastating effects:

Take a 360-degree view of the threat environment and understand the risks

Understanding cybersecurity risks and generating awareness of them is the first step in training the finance and payments teams to help protect against them.

PwC reports that cybersecurity attacks haven't just multiplied, they've become more sophisticated, and ransom demands steeper. Remote and hybrid work environments have put organizations at increased risk for security breaches, as people are spending more time on their computers and often working on less secure networks and personal devices.

The record high labor shortage, including too few cybersecurity professionals to provide protection, is also to blame for creating a riskier business environment. Eighty-five percent of those finance pros surveyed in a global cybersecurity study by Trellix, said they believe the current workforce shortage is making it difficult to secure increasingly complex information systems and networks.

Which department is most at risk? AFP's 2021 Survey shows that Accounts Payable (AP) departments are among the most susceptible. Fifty-eight percent of respondents report that their AP department was targeted by BEC fraud, a convincing approach where a criminal sends an email to an employee, pretending to be a senior executive

with the company, and instructing the employee to approve a payment or release client data. Employees often fall for the scam, unless they are made aware of them and on guard.

Rely on advanced technology to protect financial information and transactions

The majority of financial institutions surveyed by software provider VMWare plan to protect against the threats by increasing their cybersecurity budget by 20 percent to 30 percent this year.

One powerful place to allocate budget is to the team responsible for managing sensitive customer and financial data and handling mission critical financial transactions, including invoicing and payments—the AP team. Antiquated, error-prone tools and processes like spreadsheets and paper checks expose organizations to greater risk.

Automating risky manual invoicing and payments processes with AI-powered AP solutions can provide the controls and transparency organizations need to better detect fraudulent threats. It also enables organizations to offer vendors e-payments, a far safer payment method than paper checks.

Cloud-based automated AP solutions protect sensitive data by storing it in safe, electronic formations and putting controls in place to assure appropriate access to it. Embedded within the solutions, AI provides 24/7 fraud protection and malware and intrusion detection. It can identify, for instance, important missing invoice details, track unforeseen rises in invoice volumes, trace after-hours logins, and make it difficult to forge documents.

The greater visibility also helps the finance team identify past payment transactions and behavioral patterns to better forecast future transactions.

Establish security protocols and training procedures to support the finance team's protection efforts

In addition to creating awareness of risk and phasing out legacy equipment and processes that are becoming increasingly susceptible, organizations can protect against cybercriminal activity by establishing a strong safety culture.

That means sharing news updates and flagging pervasive issues, so workers are on guard, well prepared, and understand that safety and security are top priorities.

Together, departments can create and share policies and procedures that clarify expectations and define security protocols. Effective safety protocols include requiring remote workers to use company-owned devices, VPNs, and secure internal networks and firewalls to protect sensitive information; regularly updating company-owned software with security patches; and never leaving devices unattended.

Looking ahead

Alarmingly, more than half of respondents in the PwC's 2022 Global Digital Trust Insights survey expect to see an increase in cyberattacks. Undoubtedly, criminals will continue to take advantage of vulnerabilities as they emerge, evolving their methods and targets to outsmart prevention strategies.

While it's impossible to predict what new tactics may emerge, proactive prevention strategies and trusted technology partners, remain the best defense.

======

Christina Quaine is chief information security officer and senior vice president of technology operations for AvidXchange. She is responsible for the company's cyber security program, leading efforts to reduce the risk of unauthorized access to sensitive data and personally identifiable information.

AvidXchange • Accounting & Audit • Backup & Security • Firm Management • Article • Accounting Firms • Cyber security • Data Security • hackers