

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

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.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

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

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

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.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

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.

Accounting • Artificial Intelligence • Firm Management • Security

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.

© 2024 Firmworks, LLC. All rights reserved