KFORCE®

How to Prevent Organizational Cyber Fraud

According to a recent survey conducted by the Association of Certified Fraud Examiners (ACFE), the typical organization loses five percent of its annual revenues to fraud. Applied to the estimated 2009 Gross World Product, this figure translates to a potential total fraud loss of more than $2.9 trillion, with nearly one-quarter of fraudulent activities involving losses of at least $1 million.

Included in these fraudulent activities are a number of cyber crimes that have transitioned from targeting personal accounts to now including organizational accounts.

“Cyber crime within the businesses community is out there, and it’s quickly becoming a common and very expensive occurrence,” said Ken Stalcup, CPA, CFE, CFF, manager of the assurance, litigation/valuation and forensic teams of *Somerset CPAs*, a full-service certified public accounting and professional services firm. “These crimes are being committed both internally and externally, and at various levels of complexity.”

Prevalent Forms of Cyber Crime

According to Stalcup, most cases of organizational cyber fraud can be linked to high-tech forms of hacking. Typically performed by outside parties, these schemes involve a transfer of funds from compromised accounts to a third party, who acts as a money mule. The mule receives the funds in a separate bank account and, after taking their percentage, transfers the money to the instigator of the scheme.

More often than not, account information for these types of schemes is obtained through viruses that record key strokes on a compromised computer. The virus records the strokes needed to enter online banking modules and hackers can access accounts with ease.

“Organizations should also be aware of the prevalence of internal fraud which, while I would not necessarily consider it to be cyber fraud, also involves the misappropriation of funds from credit cards and checking accounts using computers and the Internet,” said Stalcup.

According to the ACFE, these types of asset misappropriation schemes are the most common form of fraud, representing 90 percent of cases identified in their study, Report to the Nation on Occupational Fraud and Abuse. Financial statement and corruption fraud were also identified as common and costly forms of organizational fraud.

Prevention Best Practices

According to Stalcup, there are three simple steps that businesses can take to protect themselves from these fraudulent activities:

1. **Stay current with virus protection software:** Ensuring that virus protection is current is one of the best ways to safeguard your organization against cyber crime. These programs can ensure that viruses are detected and removed from your operating system before valuable information is compromised.
2. **Review and reconcile account balances frequently:** The days of paper bank statements are gone. As such, organizations must proactively review and monitor charges to their bank accounts online. Regular monitoring can help ensure that any fraudulent charges will be identified, reported to the bank, and then considered for asset reconciliation.
3. **Create complex passwords:** Choosing passwords that include case sensitive letters, numbers and symbols is also a good practice. The best passwords will be a random string of all three of these characters. The more complex your password is, the harder it will be to crack.

How to Prevent Organizational Cyber Fraud

“Permanent customer names and manually entered passwords still exist. However, several banks now provide a device to electronically produce a new password every 10 minutes or so,” said Stalcup.

These one-time use passwords add an extra layer of protection when making sensitive online transactions. Delivered to account holders via text message, passwords expire as soon as they are used, or 10 minutes after they are issued.

While these best practices can aid organizations in preventing cyber fraud, the best form of prevention is education. Executives should familiarize themselves with the types of fraud being committed in their industry so they will recognize the warning signs should their organization fall prey to cyber fraud.

© 2012 Kforce Inc. All Rights Reserved. Kforce is an EEO/AA Employer.