Dopkins & Company, LLP
CERTIFIED PUBLIC ACCOUNTANTS AND CONSULTANTS

Is Cyber Fraud Prevention a part of the Internal Controls at your business?

Jim Krupinski jkrupinski@dopkins.com February 2019

Although any employee may be a target for a cyber attack, individuals working in Finance, Human Resources, Information Technology and the Executive Team are considered targets given their roles and access to funds. Unfortunately, recent trends indicate there will continue to be a growing number of companies of all sizes falling victim to cyber fraud through email scams.

The FBI's Internet Crime Report indicates that in 2017, $675 million of losses were attributed to email fraud. In those instances, perpetrators frequently posed as company executives via email or text message to dupe company personnel into wiring large sums of money to fraudulent bank accounts. Another type of fraud involved deceptive emails from a fraudster posing as a vendor with instructions to change bank account information for future wire transfer payments.

These examples signify why it is critical for companies to consider cyber threats when implementing internal accounting controls. Are you comfortable with your responses and overall business preparedness to the following questions?

- Are you and your employees aware of these risks and can spot a fake email?
- Do you know what your employees would do if they received a fake email requesting a wire transfer?
- How do you know if notification regarding changes to vendor banking information is legitimate?

Many organizations approach the management of internal controls on an ad hoc basis, reacting to gaps as they become evident, rather than proactively identifying and mitigating gaps before they lead to problems. A formal internal control assessment process helps ensure that all gaps are identified and mitigated, not just the ones that happen to get noticed. Ultimately, the most important defense against these kinds of scams is awareness – awareness that the threat exists and awareness of the need for vigilance.

The threats are only expected to increase with each passing day, and companies need to remain vigilant by evaluating business processes and implementing technical safeguards within their cybersecurity plans. In particular, they should:

- Develop and implement internal accounting controls that protect assets from cyber-related fraud.
- Ensure appropriate management authorization for employees to conduct transactions and access assets.

Dopkins offers a variety of services to help organizations assess, design, and implement internal control systems tailor made to help prevent your organization from becoming a victim.

For more information, please contact:

James A. Krupinski, CPA
Director
jkrupinski@dopkins.com ▪ 716.634.8800

Jim has 25 years of experience providing audit and consulting services to clients from a diverse range of industries. In addition to his many audit management responsibilities, he currently serves as the leader of the Firm's risk management services group. He has assisted his clients with performing risk assessments, evaluating and improving internal controls, developing fraud prevention programs and complying with the requirements of Sarbanes Oxley's assessment of internal controls over financial reporting requirements.