LOPATA, FLEGEL & COMPANY LLP
Accountants and Management Consultants

600 Mason Ridge Center Drive
Suite 100
St. Louis, Missouri 63141
314-514-8881
314-514-8872 Fax

July 2019

Unfortunately, we have seen a substantial increase in cyber-related frauds affecting numerous businesses. These frauds can be expensive and very disruptive to the companies effected. Some of the more common frauds are as follows:

1. Vendor payment changes: Emails come to management or accounting staff that appear to come from company vendors that request electronic payments are sent to a new or different bank or bank account. They may also direct checks be mailed to a new address or PO Box. Many are frauds and the result of someone's email being hacked either at the Company or at the vendor. For your protection, we recommend that no payment directives be changed without verbal confirmation initiated at your company to the contact and phone number on file.

2. Wire transfer or gift card frauds: Emails come to company personnel that appear to come from someone of authority within the organization requesting an employee either:

   a. Buy store (e.g. Walmart, Target, etc.) gift cards, scan the cards and send the scanned image to the email address requesting the cards; or,

   b. Wire funds to a new vendor for a deposit for consulting or other services or product purchases.

   Fraudulent instructions appear genuine but are likely from a hacked email account. Once the action(s) are completed, they are difficult, if not impossible to reverse. We recommend that any email payment instructions are confirmed verbally with the sender.

3. Ransomware: We are hearing more and more about hackers taking over computer systems and requesting large sums (some in excess of $100,000) payable in bitcoins. We recommend that every company hire experts to evaluate susceptibility to ransomware and take all reasonable actions available to minimize these horrible situations.

We also recommend that every company purchase full-coverage cyber insurance. Many policies will cover ransomware and other cyber-fraud schemes including providing IT consultants to assist in data recovery and restoring systems. These insurance carriers know how best to deal with these situations and can cover the ransom payment in the event that it is the best solution. You should work with your insurance broker to assess the coverages available to ensure that your policy is right for your business and its risks.

We are always happy to discuss better ways to improve internal controls over your physical and intangible assets.