New IT Security Threat Targeting Finance Departments On the Rise

By Stan Reiff, Partner

Imagine this scenario:

Someone outside your nonprofit organization hacks your colleague's email account. Once he has access, the perpetrator identifies your executive director and monitors her activity. He analyzes her email communication style, activities, travel, and even your organization's culture.

The executive director leaves on a scheduled trip and the perpetrator emails the chief financial officer from her account. Posing as the executive director, the perpetrator requests that the CFO wire funds to a particular "ministry partner" for an urgent need or incredible ministry opportunity that has arisen and must be acted on immediately. According to the email, the executive director has the supporting documentation with her and will provide it when she returns. The email provides instructions for wiring the funds in the meantime. The CFO sends thousands of dollars to the fraudulent account, and the money is never recovered.

The Nature of the Threat

This may sound like a movie plot, but unfortunately, it is a reality we see playing out more and more. There is an increased incidence of white-collar financial crime through breaches in IT security made by individuals outside an organization, and we're aware of several nonprofits that have experienced a financial loss this way.

Because the fraudulent email looks like it's coming from a leader within the organization, many times the accounting department head is reluctant to question it or request additional information. And because many organizations do not have sufficient internal controls over electronic funds transfers, the transfer is initiated and completed before the leader returns and the breach is detected.

In one case, this fraudulent activity occurred more than once, and was only detected after the senior leader postponed a scheduled trip at the last minute and was in the office when the fake email was sent. This organization suffered significant financial loss.

In a case at a church, a security breach was uncovered when the perpetrator provided an incomplete wire transfer account number and the director of finance contacted the senior pastor directly for the correct number. This case had a happier ending, with financial loss averted.

Preventing Loss at Your Organization

Most, if not all, nonprofits use email and calendaring programs, and that's just one example, albeit a common one, of how an IT security breach can occur. But there are steps you can take to reduce your organization's risk.

Here are four recommendations for preventing this type of IT security breach at your organization:

1. **Conduct an IT security risk assessment for intrusion vulnerabilities**. This can include user names and passwords, firewall protection, update and patch management, and security policies on encryption. It's important to note that IT security is not just the responsibility of the IT staff — it's the responsibility of all employees.
2. **Review and strengthen your organization's electronic funds transfer policies and procedures to help reduce the risk of theft in this area**. There are several options to consider, depending on the size of your organization. We recommend that you establish policies that allow you to maintain your fiduciary responsibilities but remain flexible and responsive to needs that arise. Your CPA and bank can help you assess the specific options that would be a good fit for your organization.
3. **Educate accounting and finance staff members about the risk**. Make sure they understand how this fraud is being committed so they can be vigilant and flag suspicious activity.
4. **Build extra precautions into enhanced policies and procedures.** One simple but effective control is to have employees double-check the actual email address used in any messages requesting a funds transfer. This is often masked because only the executive's name is visible. We recommend that the

email be printed and signed as part of the documentation process. Many times the fraudulent email address will print out, making it easier to detect. Even if it's still not visible, however, the required step of printing out the email, inspecting it, and then authenticating the inspection with a signature is a great way to ensure that this simple step is completed. The few extra seconds this takes could save thousands of dollars in unrecoverable funds.

Another option is to consider implementing a policy that no wire transfers can be authorized or authenticated through a single means of communication. For example, an authentic initial email with instructions for an electronic funds transfer should be followed up with a phone call or text from the email recipient to the person requesting the funds transfer. This call or text message should be made to a known phone number, not one provided in the email.

You can also establish additional protocols such as including code words for transfers. If your organization makes frequent or large electronic funds transfers, you may want to use more advanced random number or confirmation code generators.

While these steps won't completely eliminate your risk, they can help reduce it. We can also assist you through services such as an IT security risk and intrusion testing assessment or a fraud risk assessment. Please contact us to learn more.

About the Author

Stan Reiff, Partner
National Consulting Practice Leader
sreiff@capincrouse.com
o 678.518.5301, ext. 260
c 678.521.0182

Stan's professional experience includes over 30 years in ministry operations, public accounting, government accounting, and missions. He provides strategic leadership of the firm's professional advisory and consulting services and serves as National Director of Church and Denominational Services.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving not-for-profit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served mission-focused not-for-profit organizations, churches, and higher education institutions by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

.