PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Protecting Your Business from Cyber Fraud During a Financial Crisis

By Thomas J. DeMayo, Partner

The recent events that have rocked the banking industry on Friday with the collapse of Silicon Valley Bank have caused anxiety and uncertainty for a number of businesses and their clients across the globe. How this will impact other financial institutions and the broader technology sector, inclusive of private equity and venture capital, has yet to be seen. There are a significant number of questions that still have to be answered; however, there is one certainty – cybercriminals are opportunists and will leverage the recent banking collapse to their advantage.

Social Engineering and Fraud

Events like this that trigger emotional distress or curiosity give cybercriminals the platform of legitimacy they need for creating social engineering campaigns. A social engineering campaign is an act through a social mechanism – be it email, phone calls, text messages, etc. designed to manipulate the victim into performing an action (e.g., clicking on a link/attachment, disclosing information, or making a change that shouldn't be made). For these types of attacks to be successful, they must trigger an emotional response with the target. The recent banking failure is the perfect mechanism for cyber criminals to leverage and trigger that response through social engineering and deception.

The following scenarios provide examples of how current events could be leveraged to manipulate you or your employees:

- An email from a legal partner, FDIC or financial institution stating they have (or need) new information that is time sensitive and can help recover deposits or similarly related matters. A link is supplied and the victim unknowingly clicks to get further information or to enter information on a fraudulent site. While the act of clicking alone seems benign, that is enough for the cyber criminals to infect your systems, compromise credentials, steal, or hold your data hostage with ransomware.

- An email claiming to be from an executive in the C suite, or external business partner stating urgency in performing an action, such as changing ACH wire or payment instructions. The end user unknowingly updates the system with the new payment instructions thereby sending money to an illegitimate source.

Time to Increase Employee Awareness

Now is the time to remind your employees to be aware of these types of fraud. Reiterate the importance of approaching emails with links or attachments cautiously, especially those that reference the recent financial crisis, FDIC or requesting payments. Educate employees to ***Pause, Inspect and Think*** (PIT) before taking action to emails, text messages, or phone calls. It's equally important to pay close attention to messages flagged as "urgent" or "time-sensitive" that reference matters pertaining to the recent banking failure. You may find it beneficial to mandate refresher training for social engineering techniques such as phishing and business email compromise in response to this event. Remember, it only takes one mistake (or click) that could have far-reaching implications.

Disbursement Safeguards

The attempted redirection of funds is a likely scenario. Remind your finance team that any request to change wire or ACH instructions must include a call back to a known good number of the requestor, no exceptions. One of the common themes we witnessed during the Pandemic was that many companies had established this control; however, procedures were not always followed.

Going Forward

Operational stability of your business has been brought to the forefront with the recent events that began unfolding just this past week. While critics are quick to point out the negligence on strategy from an asset diversification, treasury management, or perhaps ineffective governance perspective, there are several tangential risks that have emerged as a result, including cybersecurity risks and the fraud that follows.

Contact Us

Whether your organization needs assistance in establishing a comprehensive cybersecurity program or just needs a phishing training refresher for your employees, we are here to help your business be cyber safe. Please reach out to your engagement team or to our Cybersecurity and Privacy Advisory specialists:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353