Wire Transfer Fraud

In a continually evolving global financial landscape, where banking networks are shrinking, volumes of digital payments are increasing and payments are being processed in seconds, fraudsters are creatively finding new ways to steal from organizations.

Cyber related fraud risk is emerging as one of the primary threats to today's organizations. In response, organizations need to be agile to respond to cyber threats and embrace new approaches and technologies to detect, predict and prevent wire transfer fraud.

Understanding Wire Transfer Fraud

Wire transfer fraud refers to a scenario in which a fraudster defrauds or obtains money based on false representations. In today's technical world, fraudsters are attempting to infiltrate organizations through electronic communications such as email, text messaging or social media messaging, among others. Based on recent investigative experience, KPMG has seen an increase in the use of phishing attacks as a mechanism through which fraudsters are able to gain access to corporate financial information.

A phishing attack refers to a scenario in which an individual sends an email pretending to be someone they are not in order to obtain information from the target of their attack. Phishing commonly involves the recipient clicking on a link contained within the email and entering their password, after which the fraudster is able to gain sufficient information to obtain access to the victim's account or mailbox. From there, the fraudster is able to extract financial information that they can use in an attempt to complete fraudulent wire transfers or alternatively to impersonate the individual and complete fraudulent wire transfers through impersonation.

The goal of a phishing attack focused on obtaining financial information is usually one of the following:

- A situation through which the fraudster gains unauthorized access to an employee's email account containing an organizations financial information which is then leveraged by a fraudster to gain access to an organizations bank accounts; and
- A situation through which an employee is coerced into transferring money to an account controlled by the fraudster.

As an example, consider a situation in which an employee receives an email from a vendor regarding payment of a recent invoice. The tone of the email is welcoming, congratulates the employee on their recent promotion and mentions that the vendor's financial year end is approaching and that expedited payment associated with the outstanding invoice would be appreciated. The employee remembers that the vendor recently completed work for the organization, recognizes the account executives name and submits the invoice for payment. However, the employee was unaware that the email they responded to was actually from w.white@abcc0rp.com instead of w.white@abccorp.com – the account executives actual email account.

However, actions are not just external. Consideration should be given to the potential harm of insider fraud that can be as great, if not greater, than external fraud, given the ability of employees to exploit weaknesses in an organizations controls to target the organizations financial assets.

Artificial Intelligence

As data volumes increase and security mechanisms become more complex, Fraudsters are turning to Artificial Intelligence (AI) to compromise data and its security. As an example, Fraudsters are leveraging AI to automate cyberattacks, to increase the efficiency and effectiveness of exploiting vulnerabilities and to develop malicious code that can evolve and change to disguise its existence. To combat AI adoption by Fraudsters, organizations are turning to AI to detect, predict and prevent security incidents. The role that AI has to play in relation to cyber security will continue to evolve on both sides of the fence.

How Do Financial Institutions Fit into the Puzzle?

From the perspective of a financial institution, the difficulty in detecting wire transfer fraud is that, in most cases, it appears that a customer is legitimately accessing their own account or providing legitimate instructions regarding fund transfers. Financial institutions are continually evaluating their controls and several institutions now have dedicated teams that operate to address these risks.

Measures to Detect, Predict and Prevent Wire Transfer Fraud

There is a growing need for organizations to ensure a balance between operational efficiency and the protection of one of its most valuable assets, its financial assets. Ineffective controls and systems within an organization can lead to the mismanagement of fraudulent incidents which in turn negatively impacts an organization's ability to make appropriate resource allocation and investment decisions.

Effective wire transfer fraud controls leverage both technology solutions and human expertise. One of the primary technical protection mechanisms is the implementation of access or control rights to information. Access or control rights are mechanisms that govern access (and revocation) rights to information, usage limitations and security. Similarly, access rights can be used by organizations to create a standardized or customized set of management protocols that define the manner in which information is shared with third parties. In this respect, access controls provide organizations with the ability to securely and confidentially link their financial information with key personnel.

With respect to human expertise, organizations should implement one or more of the following mechanisms in an attempt to combat wire transfer fraud:

- Organizations should consider the adoption of formal processes to validate any changes to the pre-determined invoice payment policy, specifically payment details that are requested via email. Particular attention should be paid to internal payment detail requests that deviate from standard processes. Consideration should always be given to the fact that internal accounts may have been hacked or "spoofed".
- With respect to external payment requests, should the standard payment process not be followed, a call back mechanism should be implemented to confirm the changes with the requestor through a known phone number (not the phone number outlined in the email associated with the payment instructions) or a specifically designated contact person.
- Unusual payment requests should be carefully reviewed to ensure that they are legitimate requests, including:
  - Foreign currency / bank payments for local vendors
  - Urgent requests for payment
  - Payment to other beneficiaries
  - Large value payments
- Organizations should develop procedures for recovery / reversal of wire transfer / electronic payments. Time is of the essence to recover from wire fraud. According to the US Secret Service "Within 72 hours, if the wire hasn't been recalled, you have less than a 9% chance of recovering funds".

Contact us

Hartaj Nijjar
National Leader
Cyber Security
hnijjar@kpmg.ca
416-228-7007

John Heaton
Partner
Cyber Security
johnheaton@kpmg.ca
416-476-2758

Chris Walker
Sr. Manager
Forensic Technology
chriswalker2@kpmg.ca
416-777-8139