News 27 Jan, 2016

Wire Transfer Fraud

Beware wire transfer fraud! Business email addresses are being intercepted in order fraudulently to divert funds

The International Chamber of Commerce's Commercial Crime Services has reported a 270% increase since January 2015 in the number of victims reporting losses caused by internet hacking of business email addresses, a phenomenon known as business email compromise ("BEC") - see https://icc-ccs.org/news/1123-millions-lost-due-to-wire-transfer-fraud

Some of these victims include Club members who have received an apparently legitimate request (often where the payment needs to be made urgently) to change the beneficiary bank details for a payment but where the funds have not been received by the claimant/beneficiary. Members affected have not to date been able to recover the sums diverted.

Precautions that the ICC recommend include:

To avoid your own email system from being intercepted:

- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, the system would flag up if the e-mail address of "abc_company.com" is changed to "abc-company.com" (ie the subtle change from underscore to hyphen in the email addresses);
- Ensure that you have up to date malware protection to prevent infiltration of networks which would enable fraudsters to access your organisation's emails and to steal information from which convincing fraudulent emails can be crafted;
- Improve the security awareness of all employees in your organisation, for example, not to click on any link in an email or text message unless it has been confirmed that it is legitimate and never to use a password from their business accounts on a non-business account. (This will ensure that if an employee's personal email address is compromised their business email is still protected.) Employee awareness is key. As the Financial Times reported on 20 November 2015, in an attempt to raise awareness by its employees about vulnerability to cyber threats the Bank of England launched fake attacks on its own employees and has warned employees against revealing their roles on social media, particularly those employees who have privileged access to information who could be a target for hackers, stating that "*Significant progress had been made in applying controls, but at the same time external threats had been increasing …. No technical fix could guarantee security 100 per cent, so at the same time significant effort had been made to improve security awareness among all staff.*"

To avoid falling victim to fraud where you are due to receive or make a payment:

- Where you are making a payment, ask yourself whether the change to the beneficiary's bank account "makes sense"? Does the beneficiary have links with the country in which the new bank account is based?;
- Where you are making a payment, telephone the beneficiary/payee to check whether the new banking details are legitimate (use a previously known telephone number);
- Where you are due to receive a payment, advise those who are due to pay you to check that the new account details are legitimate. For example you may wish to include a provision in your contracts that those who are due to pay you must not to make payments to any newly-advised account details unless they have followed a designated procedure, such as telephoning (using a specific telephone number) or faxing you in order to verify the new account details. You may wish to include a provision in your terms and conditions that failure to follow this procedure in making payment to any newly-advised bank account will be deemed to constitute an invalid payment and that the counterparty will still be liable to pay the full invoice value to you.

This note is for general guidance and information purposes only and should not be relied upon. If in doubt, queries should be raised via the usual and established channels. Should you require specific advice on a particular situation please contact the Managers or ICC directly.

This article was written by Nicola Cox, FD&D Deputy Director, with input from Tony Surkovic, Chief Information Officer and ICC's Commercial Crime Services.