Cyber resilience testing for email fraud attacks

Risk Consulting

Rise in Business Email Compromise (BEC) incidents

The Internet Crime Complaint Center (IC3), a multi-agency task force set up by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) of USA, has made an announcement about the BEC incidents, which it has been tracking. These sophisticated scams target businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.[1]

Email cyber fraud

Also known as, 'Man-in-the-Email' scam, email cyber fraud is typically an improvised attack wherein organisations are defrauded of huge sums by effecting fraudulent wire transfers to designated bank accounts across the globe.

These attacks generally involve targeting either end of the supply chain and effecting fraudulent transfer of funds in one of the three ways described below:

Targeting business suppliers

Business suppliers especially overseas suppliers, are asked to wire funds for outstanding payments to an alternate, fraudulent account. This attack is typically carried out using a spoofed email id of an employee who corresponds with the suppliers.

Compromised business email

The e-mail accounts of CXO level business executives are targeted using spoofed or hacked accounts. A wire transfer request using the compromised account is sent to the employee who is normally responsible for processing these requests.

Compromised personal email

Personal email accounts of employees are hacked. Using the compromised email account requests for payments to a fraudulent bank account are sent to multiple suppliers identified from employees' contact lists.

Characteristics of email cyber fraud

While businesses and personnel using open-source email are more likely to be targeted/hacked in such type of attacks, businesses running their own email systems are also frequently targeted. Fraudsters tend to gather sufficient information in advance to target individuals specifically responsible for handling wire transfers within the business. Fraudulent e-mail requests for a wire transfer are observed to be genuinely toned and customised to the business environment of the target, and typically do not raise suspicions in reference to the legitimacy of the request, unless closely scrutinised.

The frequency and scale of such email cyber attacks are expected to rise in proportion with the increased usage of business email.

Service overview

KPMG offers a two-pronged approach for assessing the robustness of an organisation's security posture towards withstanding email cyber attacks to provide a holistic management process:

Email cyber attack simulation

Simulating email cyber attacks to test the control effectiveness from outside would include researching and preparing imitation domain and designing rouge emails so as to avoid suspicions and incite fraudulent wire transfers.

Email cyber security infrastructure review

Reviewing the email infrastructure controls such as: email security gateway, anti-spam filtering, AV scanning, SPF records, email log analysis, etc.

Business email compromise statistics[2]

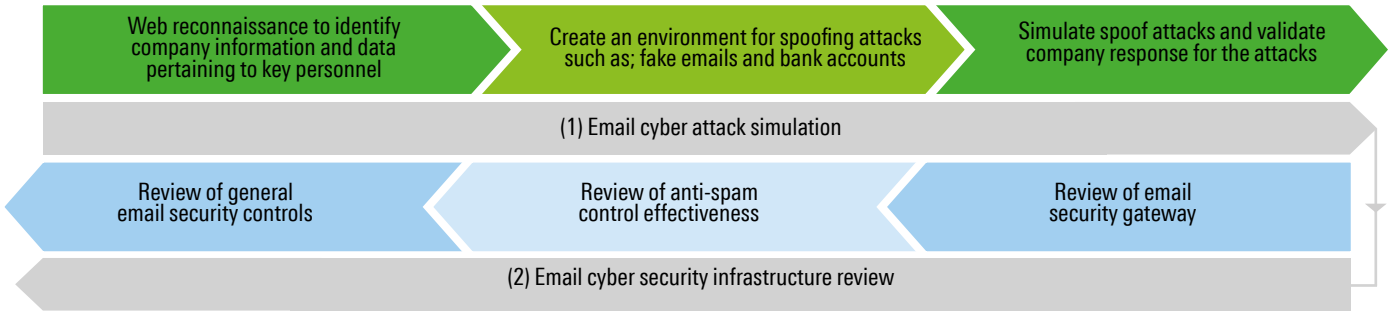
BEC incidents have been reported across the globe, with significant financial losses. The highlights of statistics reported by IC3, for the year 2016, are as below:

- Total number of worldwide victims: Over 22000
- Total financial loss: Over USD3 Billion;

As per the IC3 Data, during 2013-16, the number of victims of the BEC fraud increased by 11 times, while the estimated financial loss went up by 14 times.

1. https://www.ic3.gov/media/2016/160614.aspx
2. https://www.ic3.gov/media/2015/150122.aspx dated 22 January 2015 and https://www.ic3.gov/media/2016/160614.aspx dated 14 June 2016

Our approach to Cyber Resilience Testing



Source: KPMG in India, approach to cyber resilience testing, 2015

What we can deliver: Key reporting areas

The outcome of our assessment is typically reportable aspects from the email infrastructure security analysis which would include aspects as mentioned below.

#	Key activities/areas covered
1	Review of the overall email network infrastructure architecture
2	Review of anti-spam controls and spam filtering parameters
3	Review of email security gateway configuration
4	Review of mailbox configuration settings for display of mails from outside the organisation
5	Review of organisational SPF records for authentication of outbound emails to third parties
6	Review of anti-malware scanning controls at the email security gateway and/or end points
7	Simulation of email spoofing/domain imitation attacks to evaluate awareness levels and effectiveness of the technical control deployed
8	Analysis of email gateway logs to identify any past incidents

KPMG's business email cyber fraud assessment service: Our value proposition

- Provides an assessment on effectiveness of the current email security systems and controls in the organisation
- Provides valuable insights about email incidents in the past
- Can predict whether such email cyber attacks would be successful
- Provides a view on the level of employee awareness and adherence to the organisational processes followed
- Offers a flexible solution tailored to the client's business environment.

KPMG in India contacts:

Mritunjay Kapur
Partner and National Head
Strategy and Markets;
Leader - Technology, Media and Telecom
T: +91 124 307 4797
E: mritunjay@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
T: +91 124 428 7098
E: atuteja@kpmg.com

Mohit Bahl
Partner and Head
Forensic Services
T: +91 124 307 4703
E: mbahl@kpmg.com

Sudesh Anand Shetty
Partner
Forensic Services
T: +91 22 6134 9703
E: sashetty@kpmg.com

KPMG.com/in

Follow us on:
kpmg.com/in/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This document is meant for e-circulation only.