Simple Tips to Mitigating BEC Risks

Statistics from the 2018 Internet Crime Report issued by the Federal Bureau of Investigation revealed that business email compromise (BEC) scams had between October 2013 and May 2018 amassed more than US$12 billion in domestic and international losses. Over in Singapore, the first seven months of 2019 saw losses arising from BEC scams amounting to S$27.9 million (Singapore Police Force Scam Alert @ https://scamalert.sg/).

There are variations of BEC scams. A common BEC modus operandi involves the scammer impersonating the victim's supplier, using a similar email address. The victim is told the supplier's regular bank account is under audit and provided a different bank account for payment transfer. One variant involves the scammer compromising the email account of the victim, the victim's supplier or business partner. The scammer monitors the email correspondence between them and at an opportune time, strikes with an email to the victim to request for payment to be made to a fraudulent bank account. Another common scheme is impersonating as the CEO or person of authority of the victim's company – also known as spear phishing or whaling, to instruct the victim to arrange urgent payment to a specified bank account for a classified project or investment. In all cases, the spoofed email used by the scammer closely mimics that of the original email address. Sounds familiar?

On hindsight, BEC scams appear simple and straightforward. When an employee unfortunately falls prey to a BEC scam, common immediate responses include 'unbelievable', 'how that person can possibly fall for the scam', 'that person is very experienced', 'where do all the training go'…. Remarks on the employee's intelligence may even pop up.

The truth of the matter is anybody can be scammed. Intentional deceit delivered by professional fraudsters out of routine and ordinary business expectations can catch the victim off-guard. It is a psychological game against the victim who is trying to react fast and carry out the instructions of the supervisor, seal an investment deal for the company, or avoid late payment penalty. A veil of distraction and a moment of lowered level of alertness can therefore enable the scammer to quickly take control. The next salvo of intense urgency and confidentiality pressure tactics compels the victim to 'act now'. The victim, succumbing to pressure, will go 'the extra mile' to facilitate the payment request, likely deviating from the company's established processes and procedures along the way.

Granted that no amount of internal controls can totally curtail fraud, it does not mean that organisations should not take action but wait to be the next victim. With strategic use of a combination of educational training and internal controls, an organisation can mitigate BEC risks, and significantly reduce its exposure.

Here is a practical approach that can help an organisation mitigate the risks of BEC scams.

I. Remove the 'burden' from employees – BEC scams exploit and manipulate a victim's psychology as an employee. It will certainly be helpful if an organisation notifies its employees, especially those remote from the main office and hold certain authority in the payment process, that there are no and never will be, special, urgent, confidential projects that even their direct management are not aware of. This simple communication may appear common-sensical, but it is impactful yet ironically neglected (as it is deemed common-sensical). The firm message removes the burden on employees of any probability of doubt and ambiguity. The ONLY option for any employee who receives special urgent request on payments is to consult and discuss with his/her superior. This is the single, most powerful tool to beat the psychological game played by the scammers.

II Internal controls – They may not totally prevent fraud but have a definite role to play in the fight against fraud. They create hurdles and deterrence to foil fraud attack attempts. Organisations can reduce the number of scam emails from reaching their employees by using analytics to assess the thin differences between clean and infected emails and identify indicators of compromise; system reminders that highlight to employees to be careful of emails from suspicious external sources; segregation of critical duties in the payment process so that there may still be a chance to salvage when the first level is breached; call-back procedures to vendor or supplier main lines to verify payment instructions; payment limits control so that even if there is exposure the damage would be reduced, and so on.

III. Continuous education

a) Scams are here to stay and will not go away any time soon as it is a lucrative business to fraud syndicates. In an ideal situation, all employees must always be alert. However, we are all human and there are bound to be occasions where alertness is less than ideal. To draw an analogy, think of fire drills. Implement a regular simple 'fire drill' training procedure that reinforces the educational message on the steps to take upon receipt of such urgent payment request, such that the reaction to such receipts become a second nature. Organisations can conduct regular simulated phishing attacks that mimic the organisations' activities or employees. This can serve as part of the training and also assess the effectiveness of the 'fire drill'.

b) Each scam, be it attempted or succeeded, must be shared with the populace to inform that the organisation is not immune to such risks. It is also beneficial to share success stories of alert employees who have managed to identify a scam and prevent the organisation from falling prey. This can generate a positive effect on other employees to also want to be the vigilant one who helps the organisation avoid a loss. And in the event that of an unfortunate occurrence (we are talking about mitigation, not absolute prevention of occurrence), the organisation must share the lessons learnt with the populace and rally all to be vigilant to prevent a recurrence.

Scamming has grown both in frequency and impact that one can only conclude that it must be an extremely profitable global business to the fraudster. It is evolving and becoming more sophisticated and will not be going away any time soon. Be vigilant, don't be the next victim. Organisations are left with no choice but to be ready and prepared for the worst-case scenario so that management and employees know how to react appropriately when fraud happens at its doorstep.

Article Contributed By:

Keith Ng, Vice President, Internal Audit, Singapore Airlines Limited and Governor, IIA Singapore

Nadiah Chang, Principal Audit Manager, Group Audit, Deutsche Bank and Member of Technical and Technology Committee for FY18/19, IIA Singapore

Sia Hwee Lay, Head of Business Audit, Internal Audit Department, GIC Pte Ltd and Member of Technical and Technology Committee, IIA Singapore