Business Email Compromise (BEC) Attacks – A Rampant Cyber Risk

Social engineering fraud is amongst the top contributors to financial frauds in organisations, today. Business Email Compromise (BEC) (also called Email Account Compromise [EAC]) is one of the most common versions of social engineering exploits to have emerged in recent times – threatening cyber security of businesses**.**

A BEC is a sophisticated scam to cause fraudulent transfer of funds, executed through compromise of legitimate business or personal email accounts through various computer intrusion techniques. Indian organisations, particularly medium and small-scale industries are vulnerable to BEC attacks owing to low awareness and preparedness levels. Unsurprisingly, BEC makes up for a significant part of Cyber and Crime Insurance claims in India.

The cyber-attack of this kind is so elaborate that even before execution, cyber criminals invest time in prospecting specific individuals associated with the fund transfer processes, mostly in finance, payroll and procurement. Techniques like phishing, pharming, vishing, hacking or malwares are used, as also publicly available data from social networking websites to gather information regarding the target executive, especially legitimate email IDs. The Dark Web is the covert marketplace of choice to trade and exchange data collated from various kinds of cyber-crimes. Email IDs of employees used for these scams could have been sourced from dumps of data obtained from data breach incidents of other websites; where an employee (without giving a second thought) would have used their corporate email ID as part of personal details.

The most common kind of BEC scam involves an email from a source that appears to be legitimate or from a known source to a target company's executive. These exploits target companies which are regularly trading or have businesses working with foreign suppliers and/or businesses that very often conduct wire transfer payments to conduct business.

There are various kinds of BEC also known as EAC (Email Account Compromise) attacks and cyber criminals keep enhancing the levels of sophistication.

- CEO Frauds/ Fake President Frauds/ Impersonation Frauds: Once an organisation's systems are infiltrated, the criminal impersonates an executive who has the authority to make funds transfer and uses a spoofed email ID to send instructions (with a tone of urgency) to execute a fund transfer as part of deal or a purchase or an escrow arrangement for a foreign deal. The communications often mirror the official's actual communication styles tricking the receiver into executing the funds transfer.

- Vendor Frauds: Involves impersonating or hacking vendor accounts to trick the victim. Often, the fraudulent email is supported with fake invoices or a request to change bank transfer details to transfer funds for services and products.

There have been cases of 'Man in the Middle Attacks' where invoices from authentic vendors have been altered to include the miscreant's bank account details which are executed through email account takeovers resulting in massive loss of funds.

Though advanced cyber security assessment, monitoring and risk management solutions have improved the technological defence against BEC attacks, the cyber security infrastructure remains as

strong as its weakest link. However, most organisations do not adequately address the fundamental enabler for BEC attacks in their risk management strategy i.e. People Risk.
The trait of 'Optimum Bias' in human psychology which leads people to believe that they are unlikely to be tricked, ironically is one of the key enablers of such attacks. This combined with a culture of following instructions from seniors, creates an ideal environment for malicious actors to exploit cyber security of businesses.

Now, the widely prevalent remote working situation due to the pandemic has had employees connected through even unofficial networks as well. Such unsecure networks coupled with the overwhelming stress that employees are facing under the current circumstances, make them more vulnerable to BEC campaigns. These risks require organisations to optimise steps to address the People and Process risks to mitigate unauthorised transfers.

'People Risk' and 'Process Risk' Management
Managing the People Risk should involve creating awareness among employees through focussed periodic trainings and simulations with employees who are associated with financial transactions. The emphasis should be on process improvements including additional layers of authentication and controls. Companies should also inculcate a risk aware culture of recognising and rewarding vigilant behaviours.

Risk Transfer – A key risk management consideration
With the increased sophistication and frequency of these attacks, enterprises need to acknowledge that a cyber breach incident is a question of 'When' and not 'How'.

To fully understand the severity and possible frequency of the risk, organisations need to assess cyber security postures periodically and also quantify potential cyber loss. They can then consider transferring the financial impact of this risk onto risk transfer mechanisms like insurance. An optimum level of Crime Insurance and Cyber Risk Insurance can help organisations to transfer the high value impact of fraudulent fund transfer losses, investigatory and mitigation costs, data breach liabilities, legal representation and business interruption losses.

In summary – an aware and educated workforce, clear protocols, strong technological defence and a tailored risk management and transfer mechanism is your best chance at beating this phishing net.

This article was first published in ET CIO.

About the Authors:

Sunny Goel
Head of Financial and Executive Risks,
Willis Towers Watson India Insurance Brokers
Sunny.Goel@willistowerswatson.com

Suraj Theruvath
Vice President - Financial and Executive Risks
Willis Towers Watson India Insurance Brokers
Surai.Theruvath@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimise benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.