INDIA'S FIRST MAGAZINE ON LEGAL AND CORPORATE AFFAIRS

LEX WITNESS

Volume 11 Issue 2 | September 2019

₹65 US $6 UK £4

India's Judicial Brass

34 Judges. Over 50,000 Cases. Do Numbers Matter?

P08

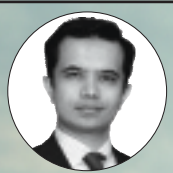
■ipr corner

Daljeet Dabas
Sr. Associate,
S.S. Rana & Co.

Tulip De
Sr. Associate,
S.S. Rana & Co.

P22

■the pondering pill



Krishna Venkat
Co-founding Partner,
Anoma Legal

P26

■let's arbitrate

S. Ravi Shankar
Sr. Partner,
Law Senate

P56

■expert speak

Jayant Saran
Partner,
Deloitte India

Sachin Yadav
Director,
Deloitte India

Ayush Vrat
Manager,
Deloitte India

P38

expert speak

Rajesh Sivaswamy
Sr. Partner,
King Stubb & Kasiva,
Advocates & Attorneys

P14

expert speak

Abhishek Malhotra
Founding Partner, TMT Law Practice

Bagmisikha Puhan
Sr. Associate, TMT Law Practice

P30

expert speak

Varsha Banerjee
Partner, Dhir & Dhir Associates

Stuti Vatsa
Associate, Dhir & Dhir Associates

P18

Business Email Compromise - Delving into the World of a Billion Dollar Scam

Jayant Saran, Sachin Yadav & Ayush Vrat

Email continues to be the top route used by cybercriminals to target victims and business email compromise (BEC) is gaining traction as one of the preferred types of email attacks.

In 2019, a Lithuanian national spent two years posing as a third party who conducted business with two of the world's largest digital platforms. The fraud was complex and the tech giants' money took a round – the – world trip to be laundered before ending up in the impersonator's bank accounts. The victim companies wired funds to bank accounts in Latvia and Cyprus, and quickly these funds were wired to different bank accounts in various locations throughout the world. The impersonator forged invoices, contracts and letters that falsely appeared to have been executed and signed by executives and agents of tech giants and submitted to the banks in support for large volume of funds that were fraudulently transmitted via wire transfer. Collectively, the victim organisations lost about $125 million.[i]

For such a complex fraud, its origins were deceptively simple – a business email sent to victims. According to the US FBI's Internet Complaint Centre, or IC3, BEC-is a sophisticated scam targeting both businesses and individuals performing wire transfer payments. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Scammers and cybercriminals have a variety of tricks up their sleeves to try to obtain financial or personal information from their victims.[ii]

The total value of funds redirected as a result of a BEC scam is now estimated to be $12 billion, according to the recent FBI data. Between December 2016 and May 2018, the world witnessed a 136 percent increase in BEC scam losses with instances of the crime being reported in over 150 countries.

The prerequisite to carry out a BEC fraud is simple. All that cybercriminals need is a computer and an off shore bank account in which the money can be transferred. They usually tend to have bank accounts in countries with less evolved regulatory frameworks and a limited experience of cross border collaboration on tracking the source of funds.

Most of the BEC scams rely solely on social

Deloitte.

Deloitte India
Indiabulls Finance Centre, 27th floor, Tower 3, Senapati Bapat Marg, Elphinstone Mill Compound, Elphinstone (W), Mumbai - 400 013

E: inforensic@deloitte.com
T: 022 6185 4000

engineering. It's the use of trickery, deception, and psychological manipulation rather than malware which results in success. Since most network defence solutions are designed to detect emails containing malware and malicious links, BEC emails often land directly in users' inboxes. And when this happens, the fate of an attempted BEC scam is in the hands of its recipient.

A popular streaming giant with more than 130 million subscribers, film buffs and TV show aficionados – is a hit with cybercriminals. A number of fraud emails were circulated in 2018, urging recipients to update their payment information to avoid having their account suspended. The link in the email lead to a convincing looking website that stole the target's username, password and payment information.[iii]

Since socially engineered attacks such as BEC are designed to exploit human instincts and emotions, human-powered intelligence naturally plays a critical role in defending against these attacks. Unless properly equipped, businesses will have a hard time preventing such attacks.

SAFEGUARDING AGAINST BEC

Preventing BEC scams requires businesses to start with employee security education and training, as user error is the primary reason for the scam

getting activated. While email security solutions will drastically reduce the likelihood of an attack, especially when it starts with a phishing email, having a properly trained group of users will greatly decrease the likelihood of any attack's effectiveness particularly among executives or staff who have authority to release funds or critical information. Some other considerations are listed below:

• Inform employees of how this type of fraud works. They should be alert when payments terms change or the vendor in question asks for funds to be sent to a different bank account than the one registered during the on-boarding process.

• Consider requiring both parties to sign off on all payment transfers rather than leaving authority with an individual.

• The CEO and the board need to be aware of cyber threats. Further, organizations need to perform assessment, design crisis plans and training programmes to reduce susceptibility that will bring down the response time.

• Special protocol arrangements can be made between financial institutes and organizations. Verifying wire transfers can be done by adding additional two factor authentication, such as having secondary sign-off by company personnel.

• Employees can be advised to open emails only from known sources and any suspicious URLs may be opened only after authorising via a pop up window. Further, fraudulent emails may be blocked by deploying Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-Based Message Authentication, Reporting and Conformance (DMARC) capabilities.

• Business fraud, if ascertained, may be

Jayant is a Partner and leads the Forensic Technology area within Deloitte Forensic India. He has over 19 years of experience and has assisted clients with matters related to cybercrime, bribery and corruption investigations, litigation support through e-discovery, dispute resolution and responding to regulatory enquiries.

reported to the respective state's cyber police department and/or the digital police online platform launched by the Ministry of Home Affairs, Government of India[1].

• Lawyers and in house legal counsels would also need to assess other risks arising from BEC scams such as leakage and misuse of sensitive organisational data.

• It is imperative that organizations carefully analyse their service agreements with service providers to be cognizant of the information that may or may not be provided by the service providers in case of an incident investigation.

• Cyber liability insurance may be purchased to recover financial losses due to phishing and other types of socially engineered scams.

BEC scam is a rapidly growing problem that impacts companies of all sizes in all regions of the world. Implementing a best practices approach can help protect your organization from becoming the next headline relating to the fraud.

[1]Source: https://digitalpolice.gov.in/ncr/State_Selection.aspx
[i]https://www.nytimes.com/2019/03/25/business/facebook-google-wire-fraud.html
[ii]https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise
[iii]https://www.consumer.ftc.gov/blog/2018/12/netflix-phishing-scam-dont-take-bait

Sachin is a Director in the Deloitte Forensic practice in India and has over 14 years of work experience in the areas of Digital Forensic, Electronic Discovery and Incident Response. He has worked closely with law firms, forensic professionals and regulators while assisting them in over 200 fraud investigations across industries.

Ayush Vrat is a Manager with the Deloitte forensic practice in India. He has over 8 years of professional experience in the fields of Digital Forensics, Incident Response and forensic investigations. This includes experience in forensics investigation (Cyber & Digital) involving Intellectual Property disputes, cyber security incidents, incident response for domestic and international entities.