Grant Thornton

23 June 2020

HALT - **PLAN** - REFRESH

COVID-19: Mitigating risk of current rise in cyber frauds

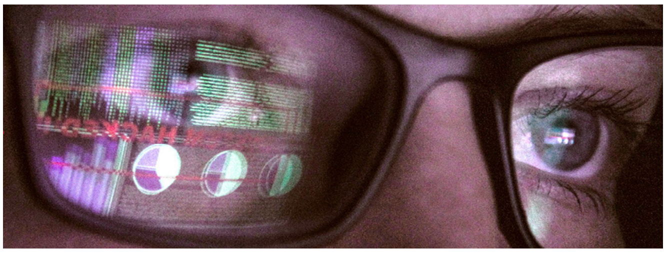
The current crisis has forced employees of most businesses to work remotely. Consequently, there is an extensive use of personal mobile networks and WiFi to check official emails or connect to official laptops, instead of the much safer office LAN connections. Cybercriminals are using these vulnerabilities to their advantage, giving rise to email frauds, phishing and ransomware attacks on organisations.

Cybercriminals launch these frauds for gaining unauthorised access to individual electronic devices. Currently, business email compromise (BEC) incidents are on the rise and a prominent method of attack. According to the FBI's 2019 Internet Crime Report, BEC related frauds alone accounted for 23,775 complaints amounting to losses of over USD 1.7 billion[1].

How do cyber frauds, such as, BEC work?

A BEC fraud is a form of phishing that occurs when a malicious user compromises legitimate business email accounts to facilitate fraudulent and illegal activity. It is done by implementing one or more tactics, including:

- Gaining access to IT systems using social engineering attacks, such as, phishing, spear-phishing and computer intrusion techniques, including, dropping trojan, remote administration tools etc.
- Carrying out extensive reconnaissance to understand the nature of business and critical roles inside the company
- Gaining access and further tampering the victim's mailbox by creating new rules to divert relevant emails into a different folder, which is not commonly used by the victim
- Monitoring the mailbox over a period to understand and gain a grip on the business process, financial approval processes and identify the key stakeholders in the approval process
- Sending fraudulent emails in line with the process using a lookalike domain and request for money transfer to a different bank account



Common BEC frauds

Based on recent incidents, fraudsters have used various modus operandi for committing such crimes. In their methods, they identified key employees, suppliers, business associates, including law firms and used their conversations for creating their plan. Following are some of the known techniques:

CXO fraud

- Cybercriminals pose as a senior executive of a firm by hacking into their account and send a flagged email requesting a transfer of funds.

Bogus invoice scheme

- The business receives an email from what appears to be one of their current suppliers asking them to change the payment destination. It is common in companies that use more overseas suppliers.

Account compromise

- The employee's email account is hacked and any emails, which contain an invoice, are intercepted to change the amount and bank details. This is mostly carried out against smaller businesses where billing is managed directly through email and not via any defined payment process or any enterprise resource planning (ERP), where vendor onboarding is required.

Lawyer or attorney impersonation

- Hackers impersonate a company's law firm and request an urgent transfer of funds to deal with a legal dispute or unpaid bill.

Data theft

- When a cybercriminal compromises a senior executive's email account and requests for sensitive corporate information.

[1] 2019 Internet Crime Report, FBI

How can businesses be cautious?

Businesses should be alert when any of the following is noticed:

- Large funds transfer to a recipient with whom the company has never dealt previously
- Transfers initiated towards the end of the day or at unusual times
- Emails that contain urgent language and are perceived to be confidential in nature
- Small changes to an email address that resembles a legitimate business address
- Usage of an unusual style of English/ communication and sentence construction
- Recipient account has no history of receiving large money transfers in the past
- Recipient account is a personal account instead of a registered business account

Here’s what business leaders should ensure as they PLAN to minimise BEC and other cyber frauds

- Increase awareness among employees of these fraud incidents and phishing attacks
- Conduct spear-phishing campaign within organisations to check the awareness quotient
- Identify gaps and design controls around payment processes
- Build robust controls for IT systems including patches, access, change management and incorporate other endpoint security aspects including anti-virus, data loss prevention (DLP), mobile device management (MDM), etc
- Conduct periodic assessments to identify security loopholes within the organisation
- Create a culture of compliance

Prevention

Awareness and mitigation

- Provide employees with adequate training on current fraud incidents
- Conduct campaigns related to spear-phishing to raise employee awareness
- Equip employees with understanding spear-phishing risk, its implications and response

Process and control

- Review and improve current processes and controls to reflect emerging risks arising from cyber-related frauds and incorporate new controls to prevent frauds

Detection

Investigation

- Conduct a thorough investigation into a fraud
- Provide support to legal counsel to take steps against fraudsters

In-depth analysis

- Conduct an in-depth analysis of IT systems, including review of overall email network infrastructure, anti-spam controls, security gateway configuration, mailbox configuration setting and analysis of email gateway logs to identify any past incidents

Respond

Incident response mechanism

- Identify compromised critical assets and stakeholders from the organisation
- Segregate and isolate the infected systems, as applicable
- Investigate procedures to identify evidence of malicious activities

How Grant Thornton can help

Grant Thornton's Forensic Investigation Services team can help you effectively brainstorm fraud risk areas across organisation and identify potential areas of activities and priorities that might help prevent integrity breakdowns.

Our cross functional team comprises forensic investigators, sector experts and cybersecurity professionals. We leverage our competencies and multidisciplinary approach to help businesses tackle such frauds, from prevention to detection and response.

For further details, please contact

Dinesh Anand
National Managing Partner, Risk
E: dinesh.anand@in.gt.com

Samir Paranjpe
Partner and Leader Forensic
Investigation Services
E: samir.paranjpe@in.gt.com

Akshay Garkel
Partner, Cybersecurity and
IT Risk Advisory
E: akshay.garkel@in.gt.com

Nitin Talwar
Associate Partner, Forensic
Investigation services
E: nitin.talwar@in.gt.com

Click here to download the recently released Grant Thornton Halt-Plan-Refresh Guide on revisiting business priorities and plans

For more insights on the COVID-19 crisis, scan this barcode to see continuous updates on our website