The increasing threat of business email compromise to organisations in Hong Kong and the APAC region – How to manage the risks and respond to a breach

July 23, 2020

In brief

We have recently observed a surge in incidents where cybercriminals attempt to defraud organisations by hacking into their email accounts and impersonating employees and third parties. This common type of scam is called Business Email Compromise (**BEC**), where intruders spend a prolonged time period spying on victims' email communications with internal colleagues and third parties outside of the organisation. The aim of these criminals is to convince staff members of the victim organisation to transfer significant sums to a bank account that they control.

In March 2020, a financial services firm in Hong Kong lost HK$41 million in a BEC scam. Such a sum highlights the significant scale of the problem; this is not just low value fraud. The US Federal Bureau of Investigation revealed that BEC cost victims more than US$1.7 billion in 2019 alone, and it affected victims in 177 countries. We have seen this first-hand too. PwC's Cyber Incident Response team in Hong Kong, which helps organisations respond to and recover from cyber attacks, has seen a spike in such cybercriminal fraud affecting Hong Kong and other locations in the APAC region in recent months. While traditional BEC targets just one organisation, recent scams have shown a focus on hijacking communications among two or more partner companies. Organisations have been more vulnerable to such risks recently because most employees are working from home. This means that criminals are likely to succeed at capitalising on their victims' limited coordination capability in relation to legitimacy checks.

In detail

Common type of cyber fraud - BEC scams

BEC scams have been a significant issue for many organisations in Hong Kong and the APAC region even before the current pandemic. In the last two years, the majority of hacking incidents that PwC responded to were BEC-related. There are different groups and individuals allegedly perpetrating such scams, ranging

pwc

Tiang & Partners
程偉賓律師事務所

from Nigerian gangs[1] to middle-aged US citizens[2]. The popularity of this type of cyber attack among cybercriminals is likely due to its perceived profitability and the low level of technical knowledge required to pull it off.

There are two main ways that criminals impersonate their victim organisations' employees or third parties: they can spoof the email addresses of their victims or a third party; or hack into the email accounts of their victims. The former is the easiest, and is often enabled by companies' lack of security policies over who can send emails on behalf of their domain (i.e. the part after the @ in an email address).

Accessing a company's email account is also relatively simple for a cybercriminal with access to a sprawling underground economy of hacking tools and stolen data. Companies' migration to cloud environments have further provided new attack opportunities to cybercriminals. Login portals to cloud-based email systems often need to be accessible from the open internet to allow remote working and employee mobility. Criminals can simply attempt to login to such exposed parts of companies' IT infrastructures. Large data breaches can provide email and password combinations that employees may have re-used as corporate access credentials. Automatic tools that attempt hundreds of login combinations per second (so-called bruteforcing) are also freely available online.

Practical tips to avoid being the next victim

Despite the significant threat that BEC poses to all organisations, some simple security controls can help prevent most of these attacks. For example, companies:

- Should ensure that they have complete visibility over their IT infrastructure. A common mistake is to forget a server without having been security hardened that is connected to the internet, or a login portal that is accessible from the open internet. Foreknowledge of such vulnerable systems means they can be secured before a criminal finds and exploits them.

- Should consider implementing multifactor authentication company-wide. This would help prevent criminals from logging in to companies' remote access systems or systems with highly sensitive and confidential data.

- Should verify that the principle of least privilege is correctly implemented for all users. Staff should only have access to digital resources they need to perform their jobs. This would hinder criminals' attempts to access sensitive resources when they breach your external defences.

- Should set up internal procedures, including call-back procedures, to verify that changes to recipients' bank account details and requests for bank transfers have been authorised by legitimate parties.

- Should make sure they have established and implemented (through training and communication) procedures to deal with such an incident, including cyber incident response and obtaining legal advice.

What to do after suffering a cyber attack?

You must act quickly in order to maximise the chance of recovery and improve your prospects of not being the victim of further attacks. For example:

- Contact your bank – put them on notice of the suspicious transaction and ask them if they can prevent or reverse the payment and/or request that the respondent bank freezes the recipient's account.

- Make a suspicious transaction report to the Joint Financial Intelligence Unit (**JFIU**) – they could choose to issue a letter of non-consent to the recipient's bank which will put the bank on notice that they do not have consent to deal with the monies under suspicion. This will put the bank on notice of potential money-laundering concerns and effectively freeze the account.

[1] https://www.cyberscoop.com/silverterrier-email-scam-nigeria/
[2] https://www.justice.gov/usao-sdtx/pr/man-admits-spoof-email-fraud-scheme-and-more

- Engage cyber incident response specialists to investigate – it is important to understand what has happened, who is involved, what has been compromised (e.g. data, money, systems, etc.) and what steps need to be taken to remediate. Indeed, insurers may require an investigation report before they agree to compensate for breaches.

- Instruct legal advisors – they can advise on the strategy for the recovery of misappropriated funds and how the courts and the police could assist as well as helping to mitigate wider legal and regulatory risks.

- Learn from your mistakes – roll out staff training and enhance IT systems which might have been compromised, or if any weakness have been identified as part of the investigation into the breach.

- Consider disclosure obligations – there are not just financial losses to consider, but also regulatory risks both locally and internationally. This is where an investigation is important and legal advice should be sought. For example, what data has been compromised – are there data privacy risks?

Conclusion

We at Tiang & Partners and PwC expect BEC to continue being one of the most significant cyber threats to companies in Hong Kong and the APAC region, especially in the era where companies continue to adjust to the COVID-19 crisis and the new normal which may follow. Nonetheless, adoption of good cyber security hygiene and an internal due diligence process can significantly help to reduce the impact of such global cyber-enabled scams, and initiating a rapid response when a breach is identified can help mitigate any losses.

Let's talk

For a deeper discussion of how this impacts your business, please contact:

David Tiang
Partner, Tiang & Partners
Tel: +852 2833 4928
Fax: +852 2833 4902
david.wp.tiang@tiangandpartners.com

Chris Cartmell
Counsel, Tiang & Partners
Tel: +852 2833 4913
Fax: +852 2833 4902
chris.c.cartmell@tiangandpartners.com

Kok Tin Gan
Partner, PwC Hong Kong
Tel: +852 2289 1935
Fax: +852 2289 8888
kok.t.gan@hk.pwc.com

Kenneth Wong
Partner, PwC Hong Kong
Tel: +852 2289 2719
Fax: +852 2810 9888
kenneth.ks.wong@hk.pwc.com

www.pwchk.com

www.tiangandpartners.com

pwc

Tiang & Partners
程偉賓律師事務所