CYBERCRIMES IN THE UAE – PHISHING, HACKING AND DATA LEAKS

According to the Economist, the world's most valuable resource is no longer oil, but data. The aim of cybercrimes such as phishing and hacking is essentially to gain access to the data of companies and individuals, including sensitive details like bank accounts and other personal information.

The scale of cybercrimes is increasing each year. 2017 saw some of the biggest hacking incidents with worldwide impact, the most prominent being the Wannacry ransomware attack which shut down governments, hospitals and businesses for days. In the UAE, consumers alone lost USD 1.3 billion to cybercrimes.[1] This does not take into account organisational losses which are likely to be many times more.

In the UAE, there are specific laws that deal with phishing, hacking and data leaks which we discuss in this note. We also discuss some best practices for companies to adopt to prevent and manage cyberattacks and the importance of prioritising cybersecurity as a board agenda item and not simply as a matter for the IT department.

Key issues

- Phishing
- Hacking
- Data Leaks
- Best Practices

1. Phishing

Phishing constitutes a crime under the UAE Cybercrime Law[2] with penalties applied against the fraudster. Under article 11 of the UAE Cybercrime Law, the act of using a fraudulent method, taking a false name or impersonation through an electronic source to capture a movable asset, benefit, document or signature is a crime. Similarly, article 12 of the UAE Cybercrime Law criminalises the act of unlawfully obtaining any means of electronic payment or related information via an electronic source. The fraudster can be imprisoned for at least one year and also fined up to 1 million dirhams. In addition to the

A fraudster posing as a customer's employee (with a minor variation to the email address) requested a UAE company to provide its bank details on the company's official letterhead. The fraudster then issued this letter to the customer after doctoring the bank details with his own account details as a result of which the customer made the payment to the fraudster. This is not an uncommon case and we are seeing increasing phishing incidents of this nature.

1 Norton Cybersecurity Insights Report 2017
2 Federal Law No.5 of 2012

UAE Cybercrime law, the UAE E-commerce Law[3] also imposes penalties for committing a crime by electronic means.

2. Hacking

Hacking is a crime under the UAE Cybercrime Law. Articles 2 to 5 of this law penalise any person who enters without permission an electronic site, information system, information network or an information technology tool and remains in it illegally. The basic penalty is a fine of up to 300,000 dirhams but if the hacking were to damage, destroy, amend or delete any data the penalty increases to imprisonment for at least 6 months and a fine up to 750,000 dirhams against the perpetrator. To the extent the data damaged is personal or the data or website was government related the penalty increases further. As with phishing, the UAE E-commerce Law also imposes penalties against the hacker.

In a public incident, a bank incorporated in the UAE was hacked and the hacker threatened to disclose details of its customers, their bank statements and other bank details on social media and other sites unless a ransom was paid.

3. Data Leaks – a consequence of Hacking/Phishing

Hacking or phishing attacks typically result in leakage of sensitive commercial or private data. Companies who face such data leaks need to consider what data protection laws apply and whether there are any reporting obligations in relation to the breach. While certain free zones in the UAE like the DIFC and ADGM have their own data protections laws, there is no federal data protection law applicable to the rest of the UAE. Instead, provisions relating to privacy and protection of personal data are set out in various federal laws such as the UAE Penal Code[4], the UAE Cybercrime Law and some sector specific laws.

The UAE Penal Code sets out a number of defamation and privacy offences. In particular, the unauthorised disclosure of private data is a crime under Article 378 of the UAE Penal Code which prohibits the recording or publishing of any news, pictures or comments which may reveal the secrets of people's private or family lives, even if the published material is in the public interest and true. A similar prohibition against assaulting the privacy of a person on electronic media also exists in Article 21 of the UAE Cybercrime law.

If any person in the UAE were found to be complicit in the hacking he/she might also be criminally liable under Article 379 of the Penal Code which prohibits the disclosure of a secret that a person is entrusted with by reason of his profession or circumstance without consent, unless permitted by law.

Is there an obligation to report a cybercrime?

Article 274 of the UAE Penal Code requires any individual who has knowledge of a crime to report it to the competent authorities or risk a fine of up to AED 1,000. Therefore, in theory, a UAE company might have to report the crime to the police in the relevant Emirate. However, we understand that such crimes are not always reported in practice. If reported, some Emirates have a designated cybercrimes department who will investigate such crimes and based on whose report the public prosecutor would decide if a criminal case should be filed.

Other bodies in the UAE with cyber security responsibilities include the (a) National Electronic Security Authority, a federal authority; (b)Telecommunications Regulatory Authority (TRA); (c) UAE Computer

3 Federal Law No.1 of 2006
4 Federal Law No.3 of 1987

Emergency Response Team (aeCert), a subsidiary of the TRA; and (d) Dubai Electronic Security Centre. One of aeCert's stated goals is to provide a central trusted point of contact for cyber security incident reporting in the UAE and there is a form on its website to report a cyber incident. Though not mandatory, a company could also report the incident to aeCert who might assist with recovery.

In the case of data leaks, a UAE company having operations outside the UAE might also have reporting obligations under the laws of those other jurisdictions.

Cybercrimes are not restricted by physical borders and can impact data held across many countries thereby invoking the laws and regulators of multiple jurisdictions.

If the data subject become aware of the leak of his/her data, they might themselves lodge a criminal complaint with the police in the relevant Emirate. Such complaint might be against both the hacker and the company itself given hackers rarely ever operate in the same jurisdiction. The customer might also bring parallel civil proceedings in the UAE Courts against the UAE company if they can prove that the UAE company's actions or inactions caused them damage. As part of managing data leaks, companies should have holistic customer management strategies to avoid losing control of the process.

Does UAE law penalise a company for failing to protect itself?

The UAE Cybercrime Law and the UAE E-commerce law do not require individuals or entities to protect themselves from cybercrimes or penalise them for lack of such protection. However, UAE law does require government bodies and employees to take various measures to prevent cybercrimes.[5]

Moreover, UAE Company Law requires directors and employees to act in their organisation's best interests and with reasonable skill and care. Failure to maintain adequate cyber security or to prevent unauthorised disclosure of data may, in certain circumstances, constitute a breach of those duties, opening the doors to liability against such persons. If the directors or employees of UAE companies were found guilty of cybercrimes or data privacy breaches while performing their duties it might also expose the company to vicarious liability under UAE law. It is therefore advisable for companies to adopt international best practices in relation to cyber security and data protection systems and provide adequate training for its personnel.

4. Best Practices

The cyber landscape is shifting in the UAE as it is across the globe and as technology advances, and we become increasingly reliant on it, so do the risks and consequences of cybercrime. Outstanding cyber risk management can put businesses at a significant advantage and open opportunities for them.

To adopt a colloquial phrase "Cyber Sec_rity is incomplete without U".

We recommend that businesses take the following steps in order to maximise cyber security:

1. Make cyber security a board level priority – it is not simply a technology issue but one that can result in serious reputational and financial impact, so ensure that your board is always alert to cyber risk issues and is able to react quickly. Core policies (HR/data collection/confidentiality/business continuity/insurance/training) must be designed with cyber in mind.
2. Address the cyber risk profile of suppliers –valuable data should only be transferred to vendors and suppliers who have been cyber-vetted. To back this up, new cyber protection clauses should be integrated into agreements

[5] Cabinet Resolution No.21 of 2013.

to ensure that your suppliers will tell you about a cyber attack before your customers read about on the internet and will help you manage the impact of any such attack and compensate you for your losses.

3. Create a cyber disaster response plan – an hour-by-hour cyber-attack response plan, which is regularly tested and reviewed, is needed across the organisation with collaboration between business leaders, legal, IT, HR and PR teams.
4. Know your notifications – in the event of a data loss incident one or more regulators may need to be notified following a data loss incident and in these circumstances you will want your legal adviser to have intimate knowledge of your risk mitigation strategy to put forward your best case. You may also need to tell customers – this legal communication process needs careful management.
5. Prioritise cyber in M&A due diligence - when buying any business, cyber due diligence needs to be at the top of your list. Consideration needs to be given to whether the target has fallen victim to a cyber attack, the risk mitigation measures in place and whether the valuation reflects any cyber weaknesses.

When a company's cyber systems are breached there can be serious ramifications for the organisation, its employees and its customers from a legal, reputational and commercial perspective.

CLIFFORD
CHANCE

CONTACTS

James Abbott
Partner

T +971 4503 2608

M +971 506450677

E james.abbott@cliffordchance.com

Arun Visweswaran
Senior Associate

T +971 4503 2748

M +971 504559270

E arun.visweswaran@cliffordchance.com

Djamela Magid
Associate

T +971 4503 2696

M +971 5668 40410

E djamela.magid@cliffordchance.com