Managing cyber risks

Rebecca Kelly and David McDonald of Morgan Lewis examine key cyber laws throughout the GCC. Although the states have their own laws to punish cyber-related crimes, the GCC lacks a regulatory framework for data protection.

Cyber security has emerged as a key concern for companies and institutions operating in virtually every industry sector in the world, with no country immune from potential cyber-attacks. Recent cyber-attacks have exposed cyber security as one of the most significant threats affecting national security and economic stability. In order to mitigate potential risks associated with cyber-related crimes Middle Eastern businesses must manage and implement their own prevention and protection measures to limit their exposure to cyber criminals.

THE IMPACT OF CYBER CRIME IN THE GCC

The impact of a cyber attack on an organisation can be devastating with consequences that include, among others, financial loss (due to fraud or business disruption), loss of key client and employee data, regulatory investigations, reputational damage and ultimately the loss of customers. There are no official statistics about the prevalence of cybercrime in the region, however, the larger GCC countries such as Saudi Arabia and the United Arab Emirates (the "UAE") are seen as targets for cyber criminals due to their economic, political and geographical positions in the Middle East. In 2012, a vicious malware attack on Saudi Aramco managed to partially wipe or destroy 35,000 computers within the Aramco network, one of the world's largest oil suppliers. In 2012, RAK Bank in the UAE and Bank of Muscat in Oman were hacked by criminals who were able to manipulate pre-paid debit cards

and withdraw USD45 million from cash machines in 27 countries. In the absence of regulatory guidance of what companies must do to take protective measures companies must adopt their own processes and more often these processes are developed on best international practice.

CYBER CRIME REGULATORY FRAMEWORK

Over the past five years, GCC countries have implemented a number of cybercrime which have sought to mitigate the potential for cybercrime attacks by criminalising cyber attacks. However, there is not one overarching regulatory body or legislative framework that applies unilaterally across all the member states of the GCC and each jurisdiction has a slightly different mechanism for detecting and criminalising cybercrime.

We set out below a short summary of key provisions of the cybercrime laws in each of the GCC states:

UAE: UAE Federal Law Decree No. 5 of 2012 on Combatting Cyber Crimes criminalises hacking and unauthorised access of websites, electronic systems, computer networks or information technology with the intent of causing a change its design, or deleting and destroying information (amongst others). Breaches of the law can lead to imprisonment and fines of up to AED3,000,000 depending on the severity of the crime.

Saudi Arabia: Royal Decree No. M/16/2007 Anti-Cyber Crime Law aims to combat cybercrimes by identifying such crimes and determining their punishments in order to enhance information security, protect rights pertaining to the legitimate use of computers and information networks, protect public interests, morals and common values, and protect the national economy. The law introduces a wide number of offences with penalties ranging from imprisonment for a term of one to ten years and/or a fine of up to SAR3 million.

Qatar: Qatar Anti-Cyber Crime Law No. 14 of 2014 sets a range offences relating to infringement upon information systems, information programs, information networks and websites with punishments including imprisonment for a term of not more than three years and/or a fine of 500,000 Qatari Riyals. More serious offences involving fraud or forgery are punishable by imprisonment of up to ten years and a fine of up to 200,000 Qatari Riyals.

Oman: Royal Decree No. 12 of 2011 Cyber Crime Law contains similar provisions in respect of offences relating to unauthorised access of data, electronic information and information systems. Penalties include imprisonment and fines, and in very extreme cases, the death penalty.

Kuwait: Kuwait Law No. 63 of 2016 Cyber Crimes Law states that anyone who obtains illegal access to computers and information systems or networks shall be jailed for up to six months and/or fines up to KD2,000. Illegally acquiring confidential personal/government data or information is punishable by imprisonment of up to three years and/or a fine of KD3,000 to KD10,000.

Bahrain: Bahrain Law No. 60 of 2014 concerning Information Technology Crimes contains penalties for a range of offences relating to the misuse of information technology.

The above mentioned laws set out punishments for the respective crimes but they do not specifically obligate companies to implement protective measures against cybercrime. Therefore, companies must implement policies and processes that will address cyber-related issues to avoid being a victim of a cyber-attack.

LACK OF DATA PROTECTION REGULATION IN GCC STATES

There is an intrinsic link between data protection and cybercrime. Companies must take steps to ensure their data is adequately protected from a cyber-attack. Attackers are often motivated by the desire to steal valuable data such as customer details, financial information and health records which can be used in other crimes such as identity theft in the cyber sphere. Notably, there are no specific data protection laws in the majority of the

GCC countries (Qatar issued legislation by way of Law No. 13 of 2016 on Personal Data Privacy) and there are certainly no GCC-wide regulations. In contrast, the European Union has introduced the General Data Protection Regulations, which comes into force in May 2018, and will place stricter obligations on those handling data on EU citizens.

The lack of specific data protection laws framework in the GCC means that companies operating in the GCC must take the initiative to introduce international best practice policies with respect to data protection and cyber security.

HOW CAN COMPANIES IN THE GCC PROTECT THEMSELVES?

Often it is the employees who perpetrate cybercrimes[1]. Many of these employees accidentally compromise data through targeting phishing schemes or through loss of devices rather than carrying out malicious attacks. Former employees are also a major contributor to cyber attacks and the results of a recent PwC survey show that 30 per cent of "insider" security incidents are attributable to former employees[2]. This suggests the need for better processes to be put in place for both training and monitoring current employees but also ensuring that former employees, and particularly those employees that move to a competitor, are properly shut out of the IT systems and denied access. Employment contracts and policies should also contain appropriately-drafted confidentiality and intellectual property provisions.

Common steps a company can take to prevent and protect against cyber-attacks include:

» purchasing up-to-date cyber security software and operating systems. This is one of the simplest strategies to defend against attacks;

» providing employees with detailed internal policies on cyber security requiring authentication and strong passwords which are regularly changed;

» increasing employee awareness training and implementing a tailored and risk-based approach to safeguarding information and systems. This training and awareness must be updated on a regular basis so that employees are, for example, aware of the most recent email scams;

» setting out a clear, tried and tested incident response plan that the company can deploy to ensure that it can quickly implement appropriate steps to recover in the event of a cyber-attack[3]. Such a plan should include the requirement to alert an appropriate cyber security solutions firm as well as the relevant national authorities in order to deter further attacks; and

» employing a cyber security consultant and obtaining legal advice to evaluate holes and security risks in the company infrastructure. Although this can be an expensive option these services can assist to reduce the risks of cyber-attacks.

CONCLUSION

Whilst the GCC states have their own respective laws to recognise and punish cybercrimes, there is no developed regulatory framework for data protection in the GCC. Companies operating in the GCC countries should seek specialist legal advice and employ a cyber security consultant if they are unsure of the steps they should take to limit their exposure to cybercrime. Companies should ensure that their internal governance and policies are aligned with international standards even where it is not prescribed by domestic legislation.

Text by:
1.REBECCA KELLY, *partner, Morgan Lewis*
2. DAVID MCDONALD, *associate, Morgan Lewis*

[1] http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf
[2] Ibid.
[3] According to a 2017 survey published by PWC, the majority of UAE companies that took part in the survey do not currently have a fully implemented and operational incident response plan.