Practical Guidelines to Minimize Risks from Cyber Attacks

Omar Khodeir

June – July 2017

With this type of software, a victim could be locked out of his computer or other electronic devices until a certain ransom is paid to the hacker. The victim receives a request to pay a sum of money, in order to be able to access their locked data. The device remains blocked pending the payment of the specified ransom, hence the name “ransomware”. Even if the victims pay the requested amount, this does not guarantee that access will be restored.

Global Cyber Attacks

Last month, the world witnessed one of the biggest global cyber attacks ever recorded. “WannaCry”, a ransomware, affected numerous international services. Sources argue that it affected 100,000 entities over 150 countries, including Taiwan, Ukraine, United Kingdom, Russia, India, China, Romania, Italy, Brazil, Egypt and others. The entities affected included FedEx, Spain’s Telefonica, Renault, and some NHS hospitals whose services were slowed down and patients’ appointments had to be canceled.

Recent cases in the Middle East

In less sophisticated fraudulent acts, criminals simply impersonate others and request payment of money from third parties in lieu of offering a service or a commodity. Many of other cyber crimes commence by a simple email or even a private message on social media platforms.

In one case, a customer received a fraudulent email from a business’ head of office requesting the customer to transfer funds to a specific bank account. The customer, unaware of the fraudulent scheme, transferred the funds to the specified bank account and received nothing in return.

In another case, a branch manager received an email purporting to be from the CEO of the company, requesting the branch manager to connect the CEO to the local travel agency so that he could book tickets for business trips. The branch manager complied with the request and unknowingly connected the fraudster via email to the travel agency who then booked 35 plane tickets for various people. Later on, the branch manager and the travel agency discovered that the real CEO never made such requests and that the previous correspondence was made with someone who impersonated the CEO’s identity. A total of 35 passengers flew between two countries with the business and the travel agency left to pick up the costs.

There have also been a number of other incidents where criminals attempted fraud by establishing websites and emails almost identical to those of legitimate businesses, with the aim of impersonating them and deceiving third parties.

Minimizing Risks

In the UAE, the relevant authorities, including the public prosecution offices, are very effective in deterring cyber crimes. Moreover, a new department, the Federal Public Prosecution for Information Technology Crimes, specialised in information technology crimes, was established earlier this year. In a previous Law Update Articles, we explained how this signifies the UAE’s determination to safeguard individuals, the community and the Emirates from these types of crimes.

Given the difficulty in locating and identifying cyber criminals, the key is to have in place protective measures against cyber attacks, particularly ransomwares and other viruses that reach devices through the internet or when downloaded mistakenly through a malicious file. It is thus recommended to:

- Check the validity of requests received via email or text messages. This could be done by contacting the entity who sent the email by phone or even paying them a visit to meet in person;
- Do not click on internet links that you do not recognise;
- Do not download files from sources you are not sure of their credibility;
- Do not open attachments or any files sent to you through emails you do not recognise;
- Make it a regular habit to install software updates and anti-virus programs;
- Be doubtful and suspicious towards any requests you receive through technological platforms;
- Establishments and all corporations should provide regular training to ensure that they undertake the necessary actions;
- Specialised IT systems should be in place to increase cyber security.

In the unfortunate event your company is impacted by cyber crime, report it as soon as possible to the authorities. Cyber incidents and viruses that may seem insignificant to you (if for example it affected an old PC) are nevertheless worth reporting to the authorities as every piece of information helps authorities to assess the magnitude of the attack and can assist in tracking and combating the virus before it spreads further.

Al Tamimi & Company’s Litigation and TMT teams regularly advise on cyber security issues. For further information please contact Nick O’Connell (n.oconnell@tamimi.com) or Omar Khodeir (o.khodeir@tamimi.com).