The Fight Against Cybercrime

by Andrew Hudson - a.hudson@tamimi.com - Dubai, UAE

September 2016

Criminals will generally not commit armed robbery at a branch of a bank these days, when they can hack into emails and access bank accounts from the relative comfort, safety and anonymity of their computer. Law enforcement agencies and consultancy companies around the world report that incidents of cybercrime are on the rise. Although statistics are not readily available, there is no reason to think that the UAE is an exception to this trend and this is borne out by our own experience of acting for clients in such matters.

This article considers an interesting example of a case that our Financial Crime team handled, which highlights that financial institutions are especially vulnerable to attacks from cyber criminals, and asks what can be done to minimise the risk of a cyber attack.

Background

Our client is a global bank. An employee in the bank's Dubai branch (in the interests of anonymity for our client, we will refer to the culprit as "TC") was able to commit acts amounting to cybercrime despite the bank's security procedures. The discovery of the employee's acts led the bank to file a criminal complaint with the Public Prosecutor in Dubai and the initiation of criminal court proceedings against TC, resulting in his conviction.

TC accessed confidential client information through the bank's information system. Although he could legitimately access the system, he had no work-related purpose to access the information relating to these particular clients. He searched for high net worth individuals, including apparently famous footballers, and used his personal iPhone to take pictures of the data on the screen. The information that he copied included names, internal customer numbers, personal telephone numbers, email addresses and total assets of each client under management. He then offered this information to third parties on the 'Dark Web' to use for illegal means such as fraud, in return for payment. Dark Web is a term used to describe a portion of the Internet that is accessible only by using networking software that makes it difficult to trace the users, and which allows anonymous online activity, for both legitimate and illegitimate purposes.

As is common among major financial institutions, the bank gathers and shares intelligence from the Dark Web. Intelligence gatherers acting on behalf of the bank saw the information that TC had copied being discussed and offered for sale in a Dark Web marketplace called AlphaBay. The internal investigations and compliance team at the bank was able to use the bank's internal audit logs to determine the identity of the employee who had searched for these customers. They traced the searches to TC's unique user ID in the Dubai branch. Several interviews were conducted with TC, during which, and faced with the evidence against him, he admitted that he had accessed the bank's information system beyond his authority and then offered the copied information for sale to third parties who he knew intended to use it for fraudulent purposes.

The bank duly reported the incident to the relevant authorities in the various jurisdictions in which it is regulated. This included a report to the UAE Central Bank, which instructed the bank to file a complaint with the Dubai Police.

Criminal complaint

The role of Al Tamimi's Financial Crime Team was to draft and file the criminal complaint on behalf of the bank. We relied on Article 379 of UAE Federal Law No. 3 of 1987 as amended ("Penal Code") and Article 2 of UAE Federal Law No. 5 of 2012 ("Cybercrime Law").

Under Article 379 of the Penal Code, where a person is entrusted with confidential information due to his employment or other circumstances and he discloses or uses that information for his or another's advantage, he will be guilty of an offence and subject to a penalty of imprisonment for at least one year and a fine of at least AED20,000.

Article 2(1) of the Cybercrime Law provides that, if a person enters any electronic system without permission or exceeds his authorised limits, he will be sentenced to imprisonment and a fine of between AED100,000 and AED300,000. The penalty is increased if, whilst accessing the system, the person deletes, discloses, damages, changes, copies or publishes any information in or from the system. In such aggravating circumstances, the punishment will be imprisonment for at least six months and a fine of between AED150,000 and AED750,000. The offence is further aggravated if the subject matter of these actions was personal information, with the punishment being elevated to imprisonment for at least one year and a fine of between AED250,000 and AED1,000,000. Additionally, per Article 42 of the Cybercrime Law, if a non-UAE citizen commits any offence under the Cybercrime Law, the court must impose an order for the person to be deported after the punishment has been completed.

Judgment

The public prosecution and the court were convinced with the evidence provided and the criminal complaint drafted by Al Tamimi & Co. The evidence in this case illustrated that TC had exceeded his authority when he used the bank's information system to copy and disclose personal information with the intent to receive money in return for the provision of such information. TC was indicted and, at the first Court hearing, sentenced to imprisonment for one year along with a fine of AED500,000, which will be followed by deportation. He immediately appealed this decision and the matter is currently ongoing.

The fight against cyber crime

Cybercrime is a real phenomenon with very real consequences. In this case, the bank was able to prevent the frauds that inevitably would have been committed by the eventual recipients of the confidential information that TC copied and disclosed. However, this was due to the sighting of the information by intelligence gatherers infiltrating the Dark Web on behalf of the bank and this information could easily have been missed. It is likely that the bank would then have faced claims from its customers as well as potentially suffering from negative publicity, on top of regulatory enforcement action.

In a world where the number of of cyber attacks is increasing and, due to the sophistication of organised criminal gangs and the rapid evolution of technological tools, a 100% security record is unachievable, what can financial institutions and others do to minimise the risk that they will be the next victim of cybercrime?

Take the threat seriously

Cybercrime should be a boardroom issue. The board should be engaged in the issue and sufficient resources should be allocated for a dedicated team to strategise and implement programmes that are relevant for the activities and profile of the business and its exposure. Continuous investment in and development of defence systems should be encouraged and these systems should be tested to ensure that they stand up to the latest known technical threats.

KYE – Know your employee

Anyone familiar with anti-money laundering processes is well-aware of the term ‘Know Your Customer’ (KYC) as part of the risk-based approach to doing business and preventing money laundering. As the major source of cyber compromises are reportedly insiders or former staff members, it is suggested that a new term should become just as familiar to boards, compliance officers and IT staff. The concept of ‘Know Your Employee’ (KYE) would require businesses to undertake a risk assessment of their workforce in the context of cyber security.

Train your staff

Although employees may be cited as the weak link in a company’s data system, it is certainly not always the case that employees are knowingly involved in violations of information security. It is important that adequate and ongoing training is given to relevant members of the workforce, so that they can consciously and defensively act in the best interests of the business.

What can government do?

Respond

The relevant authorities must be capable, technically and financially, of responding to reports of cybercrime. They should then use these capabilities to respond effectively, so as to deter cybercriminals from operating in the jurisdiction. If there is evidence of the authorities acting, cybercriminals may well look elsewhere for a lower risk option.

Share Information

Given the global nature of cybercrime, it is vital that governments share information with each other, which also means obtaining information from the private sector. In doing so, it should be made clear that no civil or criminal action will result against information providers, if done in accordance with established criteria and standards.