CYBERCRIME IN THE UAE

Presented by

Omar M. A Obeidat
Partner & Head of Intellectual Property

January 2016
INTRODUCTION- Rise of Cybercrimes in the UAE

- In 2014, more than 1500 cybercrime cases were reported to Dubai police; (The National).
• These key offenses are committed by the use of the internet or any information technology tool such as gaining unauthorized access to:
  – a website,
  – an electronic information system,
  – a computer network or information technology

Basically any offense using computer data and systems and the like
• The UAE Cyber Crime Law ‘s "key offenses”:
  – Unauthorized access to IT system, website, IT tool or Information network/Hacking,
  – Deletion, destruction, amending, copying or disclosing data
  – Tampering with / Changing the design or layout of a site
  – Credit Card fraud,
  – Forging official documents
  – Wrongful impersonation
  – inciting criminal and terrorist acts;
  – threatening state security;
  – disclosure of confidential information;
  – defamation;
  – publishing "illegal content".
Correlated UAE Laws

• The Cybercrime Law correlates with other UAE Laws which are usually cited in the complaints to complement and strengthen the causes of action depending on the nature of the attack, namely:
  – Federal Law no. (15) of 1980 on Publications,
  – Federal Law no. (3) of 1987 on the Issuance of the Penal Code and the amending laws thereof,
  – Federal Law no. (7) of 2002 on the Copyright and related rights and the amending laws thereof,
  – Federal Law no. (1) of 2006 on Electronic Transactions and Commerce,
  – Federal Law no. (37) of 1992 on Trademarks and the amending laws thereof,
  – Federal Law no. (4) of 2002 on Criminalizing Money Laundering
  – Federal Law no. (35) of 1993 on Criminal Procedures
Examples of cybercrimes we have encountered

• Hacking the social media pages of a high profile media company based in the UAE and posting defamatory political statements!

• Hacking on the network systems of customers for UAE based company and sending emails impersonating certain individuals to defraud customers to remit invoices to a different bank account!

• Hacking into the network systems of a UAE based health care clinic/hospital and sending emails impersonating certain individuals from HR with offers of employment!

• Hacking into the personal laptop of an employee and gaining access to company data!

• Finding cybercrime from illegal broadcast of content through the internet
Steps to file a criminal complaint - Police department

• Criminal complaint is filed before the police station unit ("Unit"); filling out forms prescribed by Dubai Police including inserting IP Address

• The Unit obtains statement and refers matter to investigations to the Cyber Criminal Evidences Forensic within CID lab and Cybercrime Departments ("Cyber Departments")

• The Cyber Departments hands out the investigation reports to the Unit;

• The Unit then prepares a report to the Public Prosecutor to continue investigations and take it forward;

• Public prosecutor may issue arrest warrants, transfer the matter to the court depending on the evidence available.
Required documents and evidences

- **Requisite evidences to be presented upon submittal of complaint**
  - **Screen shots:** If the hacker hacked into social media pages of the victim, then immediate screen shots must be submitted; but Lab must record screen shot in order to include in report.
  - **Relevant documents:** All emails, letters, correspondences showing that the hacking has resulted in a wrongful impersonation of the victim.
  - **Information on bank:** which the fraudulent account was used to open.
  - Presence of the complaint or victim
Technical Evidences/Bank cooperation

• The Victim must be prepared to assist the police with all technical aspects namely:

  – Having readily available the relevant computer/lap top subject matter of the crime;
  – IT report on how the crime occurred. Usually, if victim is a company, the IT team must be ready to cooperate with police to gather all necessary evidence;
  – Crucial that the hard disk is NOT removed to safeguard the evidence;
  – Cooperation of the banks is crucial to assist in investigating the criminal who opened the suspicious account.
Challenges in the UAE

- In cases of automatic transfers for money forwarded outside the UAE, public prosecution may not be interested to pursue case.

- Where offenders are outside UAE, either judicial cooperation agreements would allow for PP to refer investigation to foreign judicial authority, but foreign judicial authorities are not bound to act without a court judgment.

- Slowness in responding to nature of cybercrimes (e.g. blocking of bank account).

- Where part of crimes are outside UAE, PP are reluctant to pursue case.
Challenges in the UAE.......continued

Jurisdictional issues and multiple victims (example)

• The hacker hacked into the computer systems of Victim No. 1 (a customer placed overseas) with the intention of impersonating Victim 2 based in UAE to defraud its customers who are Victim 1;

• Victim No. 1 (based overseas) is the customer of Victim No. 2 (based in UAE);

• The fraudulent bank account used to receive funds is in the UAE.

• While technically in this case, the hacking most likely occurred only overseas, Victim 2 is still based in UAE and there are many elements of the crimes that happened in the UAE (i.e. opening of fraudulent bank account, impersonation, attempted fraud...etc).

• This cross border element makes enforcement of a complain in the UAE challenging.
Challenges in the UAE……..continued

• Not knowing who the offender is a main challenge. How to identify whereabouts of a criminal?

• If offender is outside UAE, there should be cooperation with countries for extradition to the UAE. There should be a number of international agreements to regulate such issues;

• Thresholds of evidence must be adapted to less stringent measures. For instance, screen shots of a Facebook page detailing the illegal incident may not be sufficient for police investigation purposes.

• PP sometimes neglects issuing the memo of accusation solely on Criminal Law although may also be subject to Cybercrime Law which include penalty of deportation
• National Council is studying legislative amendments to elevate the cybercrimes from misdemeanor to felony thereby increasing the penalties to reach AED 2 Million and increasing the jail term.
CYBERCRIME: PROTECTING AGAINST AND RESPONDING TO A NEW AND HIGH-PROFILE THREAT

HERBERT SMITH FREEHILLS

JANUARY 25TH, 2016

Alexandra Neri, Head of IP/TMT, Paris, T +33 (1) 53 57 78 30, Alexandra.Neri@hsf.com
INTRODUCTION

Cybercrime, a high-profile menace

What is cybercrime?

Why does it matter?

How to mitigate the risks of cybercrime?

Prevention

Incident management
PART 1:

CYBERCRIME: A HIGH-PROFILE MENACE

JANUARY 25TH, 2016

Alexandra Neri, Head of IP/TMT, Paris, T +33 (1) 53 57 78 30, Alexandra.Neri@hsf.com
WHAT IS CYBERCRIME?

Perpetrators
- Organised criminals
- Employees
- Governments
- Competitors
- Hackers
- Terrorists / Activists

Methodology
- Malicious code
- Malicious networks
- Social engineering

Goals
- Financial gain
- Disruption of operations
- Theft of customer data
- Espionage
- Political / Ideological agenda (hacktivism)
WHY DOES IT MATTER?

OPERATIONAL RISKS

CYBERCRIME

LEGAL RISKS

REPUTATION-RELATED RISKS
WHY DOES IT MATTER?

OPERATIONAL RISKS: sources of risk and consequences

STAKEHOLDERS

ACCIDENTAL EVENTS

UNINTENTIONAL ACTS

INTENTIONAL ACTS

IT CONSEQUENCES

BUSINESS CONSEQUENCES
WHY DOES IT MATTER?

OPERATIONAL RISKS: case study

 ✓ An employee wishes to work on a data file at home
 ✓ Mass extraction of information from the system (Excel file)
 ✓ Connection to a personal webmail client such as Yahoo Mail, Gmail
 ✓ Email with unsecured attachment sent
 ✓ Synchronisation of the email account with a personal terminal (iPhone, etc.)
 ✓ File downloaded to terminal
 ✓ Loss of terminal on public transport
 ✓ Third party accesses terminal data
 ✓ Publication of data online
 ✓ Identity theft
WHY DOES IT MATTER?

LEGAL RISKS: financial / criminal sanctions for failure to take appropriate measures

- **Zurich Insurance**: fined £2.275 million by FSA for loss of 46,000 customer records in 2010. Unencrypted back up tape lost

- **HSBC**: fined £3.175 million by FSA for a series of data breaches, including losing 180,000 records in 2009. Unencrypted CD lost in post

- **Norwich Union**: fined £1.26 million by FSA in 2007, after £3.3 million stolen from policyholders (including Aviva’s directors) through “social engineering” of the NU call centre staff
WHY DOES IT MATTER?

**LEGAL RISKS:** financial / criminal sanctions for failure to take appropriate measures

Both applicable to foreign companies doing business in the EU:

- **Data Protection:** General Data Protection Regulation (into force in 2018)
- **Cybersecurity directive** (expected early 2017)
WHY DOES IT MATTER?

REPUTATION-RELATED RISKS: case study

An American software company, inventor of Photoshop, the PDF, Adobe Creative Suite…
WHY DOES IT MATTER?

REPUTATION-RELATED RISKS: case study

- October 2013: **data breach**, 10GB of data - 150,000,000 user records
- Unencrypted email addresses, password hints, expiry dates
- Passwords not “salted and hashed”
- In its initial statement, Adobe only admitted that 2.9 million users were affected

Adobe allowed “the data to be stolen” and made serious errors

Adobe “did not reveal the full scale of the issue”

“Adobe never should have stored passwords in a reversibly encrypted format”

“The company needs to take a long, hard look in the mirror”
PART 2:
HOW TO MITIGATE THE RISKS OF CYBERCRIME?

JANUARY 25TH, 2016

Alexandra Neri, Head of IP/TMT, Paris, T +33 (1) 53 57 78 30, Alexandra.Neri@hsf.com
HOW TO MITIGATE THE RISKS OF CYBERCRIME?

**PREVENTION**

- Developing rules for information security
- Defining who is responsible for implementing the rules
- Ensuring rules are enforceable and effectively applied

**INCIDENT MANAGEMENT**

- Identifying / limiting leaks and preserving evidence
- Liability actions and litigation strategy
- Informing affected persons / Notifications / Disclosure
PREVENTION

DEVELOPING RULES FOR INFORMATION SECURITY

Group level
An overall framework for information security

Operational level
Practical tools for company operations

Employee level
Clear rules for all employees
Key considerations for cybersecurity policies

- **Proactive prevention** of cyber-attacks
- **Board-level** involvement
- Compliance with applicable **standards** and **regulations**
- **Data storage and transmission** methods
- **IT security of external suppliers**
- **Personal data protection** obligations
- Ensure compliance across all **stages of the supply chain**
PREVENTION

DEFINING WHO IS RESPONSIBLE FOR IMPLEMENTING THE RULES

A system for delegating assignments is a sign of sound company management

The reality and scope of a delegation of authority is subject to assessment by the courts
PREVENTION

ENSURING RULES ARE ENFORCEABLE AND EFFECTIVELY APPLIED

- Internal Regulations: Incorporating information security rules into company internal Regulations
- Employment contracts: Ensuring employees give individual consent to security rules
- Relationships with service providers: Ensuring service providers abide by security rules
INCIDENT MANAGEMENT

IDENTIFYING / LIMITING LEAKS AND PRESERVING EVIDENCE

Treating IT environment as a “crime scene”

Employees

Loss of data caused by employees

Tech intermediaries

Breach/negligence caused by intermediaries (hosts)

Third parties

Breach caused by third parties
INCIDENT MANAGEMENT

LIABILITY ACTIONS AND LITIGATION STRATEGY: who can be liable? On what ground?

- **EMPLOYEES**
  - Holding employees responsible for a data breach

- **SERVICE PROVIDERS**
  - Holding service providers liable in contract

- **THIRD PARTIES**
  - Holding third parties responsible for a data breach
### INCIDENT MANAGEMENT

#### LIABILITY ACTIONS AND LITIGATION STRATEGY: risks of taking criminal action against perpetrators

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Investigating judge has broad powers</td>
<td>• Long and often unfruitful proceedings</td>
</tr>
<tr>
<td>• Certain incidents may be connected to other similar incidents</td>
<td>• Acts must correspond exactly to criteria defining the offence</td>
</tr>
<tr>
<td>• Procedural costs</td>
<td>• No compensation</td>
</tr>
<tr>
<td>• Strong message</td>
<td>• Potential damage to the company’s reputation</td>
</tr>
<tr>
<td></td>
<td>• Jurisdictional challenges</td>
</tr>
</tbody>
</table>
INCIDENT MANAGEMENT

INFORMING AFFECTED PERSONS / NOTIFICATIONS / DISCLOSURE

Informing affected persons

Informing people affected by data breach

Notification of regulatory authorities

Obligations to report data breaches

Reputation management

Developing a litigation and public relations strategy
CONCLUSION

• No one is safe.

• Losses are hard to assess, especially in terms of damage to reputation

• Reducing risk means clear and enforceable rules for all

• If you want a peaceful company, prepare for a cyber war

• Inform affected persons, report the breach to the authorities in due time

• Preserve evidence + use all the legal instruments available in case of litigation
Legal services are provided in Indonesia, in Jakarta, through Herbert Smith Freehills LLP's ("HSF") association with Hiresa & Partners ("HBT"). HSF and HBT are two independent firms which have a formal association in Indonesia.