Information security: How technology is changing the face of Information security

by Sana Saleem

June 2013

The digital revolution has radically changed commerce, industry and government. Information is no longer stored in rooms full of filing cabinets under lock and key.

Instead it exists in electronic format on computers located on corporate and government networks which can be accessed via the internet. The advent of electronic storage of information has removed the need for people to be physically present to perform transactions; instead they can trade shares or book an airline ticket from their living room over the computer. It has also given rise to an entire generation of computer savvy criminals who have turned hacking into a highly lucrative criminal pursuit. As a result, information security has emerged as a new discipline which serves to ensure the confidentiality, integrity and availability of data, and the availability of technology that enables delivery and processing of that data.

This article presents an overview of the laws impacting information security in the UAE and generally provides tips based on industry standards that may be considered when evaluating an entity's information security regime.

Information security obligations under UAE law

Generally information security breaches result in one or more parties incurring loss or damage that can range from minor to catastrophic. Although the UAE has no consolidated information security law, the following pieces of legislation generally govern information security in the UAE:

Cyber Crimes Law

Federal Law No. 5 of 2012 ("Cyber Crimes Law") provides for a range of offences committed online including issues like hacking into IT networks to steal data, hindering access to an IT system and distributing viruses. Generally, the relevant information security related provisions of the Cyber Crimes Law prohibit the following:

- Unauthorized access to an IT system resulting in access to personal data;
- Unauthorized access to an IT system to obtain government data;
- Hindering access to an IT system;
- Disabling an IT system by introducing spam email and virus programs; and
- Hacking into an IT system.

DIFC Data Protection Law

The DIFC Data Protection Law 2007 and its Regulations (together referred to as the "DIFC Data Protection Law") regulate the processing and transfer of personal data including sensitive personal data located in the Dubai International Financial Centre (a free zone hereinafter referred to as the "DIFC"). Specifically, the DIFC Data Protection Law requires all data controllers (i.e. any person in the DIFC who alone or jointly with others determines the purposes and means of the processing of personal data) to implement appropriate technical and organizational measures to protect personal data.

Additionally, obligations to properly secure information arise in a range of other laws and regulations, including the Dubai Healthcare City ("DHCC") Governing Regulations and the Federal Credit Information Law which require data holders to institute appropriate information security policies to protect health and credit related data.

Government security standards

Meanwhile, the governments of Abu Dhabi and Dubai are in the process of developing their own information security standards in an effort to maintain the security of critical government information.

AD Information Security Policy

The Abu Dhabi Government Information Security Policy and related Abu Dhabi Government Information Security Standards (together referred to as the "AD Information Security Policy") constitute the most comprehensive regulation addressing government data in the Emirate of Abu Dhabi. The AD Information Security Policy defines requirements for ensuring that critical government information is secure regardless of the medium in which the information resides.

Generally, pursuant to the AD Information Security Policy, all Abu Dhabi government entities are required to:

- categorize their information assets (including information systems) based on the importance and critical nature of the relevant asset;
- develop an Information Security Program Plan;
- build the required capabilities to monitor the information systems and manage information security incidents in the entity; and
- regularly report to the Abu Dhabi Systems and Information Center ("ADSIC") – responsible for assisting the government entities in implementing their respective Information Security Program Plans.

All Abu Dhabi government entities must comply with the obligations set out in the AD Information Security Policy to ensure the confidentiality, integrity, and availability of government information. Additionally, Abu Dhabi government entities must ensure that suppliers engaged by them adhere to the applicable obligations of the AD Information Security Policy.

Dubai Information Security Policy

With the passing of the Executive Council Resolution No. 13 of 2012 – Regarding the Information in the Government of Dubai ("Dubai Information Security Resolution"), the Dubai e-Government Department is now set to develop an information security policy for the government of Dubai. Pursuant to the Dubai Information Security Resolution, such policy will include:

- governance of information security;
- incident and risk management;
- access control;
- process, system and communication management;
- development and management of information systems; and
- legislative regulation.

The 2012 Dubai Information Security Resolution is Dubai's first step towards facilitating a further exchange of information between the private sector and government entities in Dubai.

Corporate security standards

There is no uniform standard that may be used as a benchmark against which the adequacy of an information security regime may be assessed. Instead various industry standards have developed which can be used as a basis for implementing 'reasonable' measures in the context of information security.

ISO/IEC 27001

ISO 27001 relates to the development and maintaining of an Information Security Management System ("ISMS") within an organization. The system constitutes an integrated set of documented policies and procedures. The fundamental approach of ISO 27001 can be expressed as follows:

- Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
- Implement and operate the ISMS policy, controls, processes and procedures.
- Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
- Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

The standard does not provide any detailed operational direction as to how to actually implement these processes; that is left up to each organization to work out for itself, on the basis that there can be no "one size fits all" information security management system. However, the standard does provide overall requirements in terms of the approach to be taken when developing and managing an ISMS.

PCI DSS

The Payment Card Industry Data Security Standard ("PCI DSS") is a security standard developed and administered collectively by the leading credit card companies (including American Express, Visa and Mastercard). The PCI DSS is globally applicable, and applies to any person, business or organization that handles credit card data – from the small retailer through to the multinational organization. The PCI DSS standard contains 12 overall requirements which need to be satisfied in order to establish compliance. The PCI DSS standards are significantly more granular than the ISO 27001 standard – for example one of the 12 requirements of the PCI DSS standard is to "Install and maintain a firewall configuration to protect cardholder data".

While PCI DSS is confined in scope to organizations handling credit card transactions, in practice its detailed provisions provide general practical advice on a number of security issues for organizations that are considering their information security regimes (particularly the more technical aspects of those regimes).

Al Tamimi & Company's Technology, Media & Telecommunications team regularly advises clients with respect to information security management policies in a corporate context. For further information please contact Chris Appleby at c.appleby@tamimi.com or Sana Saleem at s.saleem@tamimi.com.