

Cyber security: New measures for the public sector – A challenge facing us all



**By Rebecca Ford
and Elizabeth Williamson**

The world now spends more than 110 billion minutes on social networks per month. It is estimated that 60 percent of all internet users access some form of social networking site on a daily basis.

With increased use, social media provides unique opportunities. Its content can be republished and can rapidly be seen by a huge audience: globally, Twitter has 200 million active users and Facebook more than 1 billion. Organisations can therefore reach the world's population in a matter of seconds. However, the same speed of communication and dissemination also applies to insignificant, careless or damaging emails or posts. What may look like a small-scale incident can quickly escalate into an issue incurring significant costs and damage to an organisation's reputation.

UAE IT Security Law

New information security laws were issued in August in the UAE (Cabinet Resolution No. 21 of 2013 regarding the regulation of information security) (IT Security Law), which prohibit Government employees from sending, forwarding or responding to email containing confidential information or that may infringe on intellectual property rights. They are due to come into force in November 2013.

The IT Security Law also prohibits sending, copying or forwarding email messages that contain attachments with viruses, spyware, malware or illegal content. Illegal content will include 'disgraceful', slandering or offensive statements, comments on race, sex, colour, disability, age, sexual issues, pornographic images or any material related to religious and political beliefs or practices.

The use of personal email has also been banned and the new IT Security Law imposes an obligation on employees to password protect their phone and include a disclaimer at the bottom of each communication.

The IT Security Law also takes steps to directly address concerns regarding confidentiality; prescribing three categories of confidential information and the purposes for which each may be disclosed, accessed, modified, deleted or copied.

In order to enforce these regulations, Government authorities may periodically check employees' IT and communication systems and employees in violation of the regulations will be subject to disciplinary action and potential criminal liability.

Whilst the new laws are initially only applicable to Government employees, it is likely that, in future, their coverage will extend to semi-governmental organisations. The issues that they are seeking to address are equally applicable to the private sector and consistent with practices adopted by employers globally over the last five years.

Other legal risks

The IT Security Law is the latest addition to the relatively extensive legal framework in the UAE that covers the use of IT and communication systems which employers (and employees) should be aware of. The enforcement of the relevant laws primarily sits with the criminal court, and therefore employees (and their employers) may face criminal sanctions, (including custodial sentences, and fines) for, a number of offences, including the disclosure of confidential information; copyright infringement; and defamation.

Addressing the risks

Many organisations adopt a similar approach to the UAE Government, by banning social media at work and blocking social media sites. However, Smartphones and high-speed mobile networks make this increasingly impractical or ineffective.

It is therefore crucial to develop a social media policy and provide employees and managers with guidance and training on appropriate use.

An employer's openness to social networking sites will of course depend on the sector in which it operates. The key consideration is to set clear standards of behaviour so that an employee knows what is expected of him at the outset and the consequences of getting it wrong. Employees should also be made aware of a common misconception that social networking sites are private and be reminded that their postings will be in the public domain.

Clyde & Co LLP

PO Box 7001, Rolex Tower
 Sheikh Zayed Road, Dubai
 United Arab Emirates

Tel: (971) 4 384 4000

Fax: (971) 4 384 4004

Email: rebecca.ford@clydeco.com

elizabeth.williamson@clydeco.com

www.clydeco.com