DS NEWSLETTER savoir faire

NEWSLETTER – LEGAL INFORMATIONS

PROPOSED BY DS AVOCATS

The IT Charter - an important tool for the security of business IT systems

ASIA

There are many articles describing cybercrime and the cost it represents for businesses (risk of the loss of data, harm to their knowledge base, risk in terms of image and reputation, and perhaps even a risk for the continuation of business and survival of the firm). Businesses have been aware of the importance of securing their IT systems for several years and sometimes gain little comfort from practises of their subcontractors or even sub-subcontractors (whose security failings are sometimes also the reason behind athe success of certain attacks); they are also the object of statutory and regulatory provisions requiring them to implement detailed, and sometimes restrictive, security measures.

Consequently, since the entry into force of the Chinese Cyber-Security law on 1st June 2017, businesses have come under increasing obligation to ensure the security of their IT systems and that of the information and personal data passing through or stored in them: implementation of internal procedures to both prevent and resolve security incidents, notification of incidents to the authorities and even to those affected, in the event of an incident affecting personal data, storage of personal data and «important data» in Chinese territory etc.

The implementation of a politique de sécurité du système d'information [IT system security policy (PSSI)] is therefore essential to determine the cyber-security framework to be set up in a business and, most importantly, the monitoring thereof. The PSSI describes the goals and general measures taken by the firm in matters of IT system security. It aims to strike a compromise between the strategic objectives of the business and the supervision required to protect its IT system.

What would happen, however, if a security incident were to originate from inside the firm? For example, if a video surveillance system detected actions by an employee for which they were sanctioned by the employer, but the surveillance system had not been set up in compliance with the labour law formalities and/or personal data protection requirements. In such event, the evidence would be deemed inadmissible before the courts and the unduly-sanctioned employee would be entitled to compensation. It should also be borne in mind that a PSSI relates exclusively to the internal organisation of a firm and it cannot lay out rules that are binding directly on employees and external service providers. And this is where the IT charter comes into play...

WHAT IS AN IT CHARTER? WHAT IS IT FOR?

An IT charter is a legal document the purpose of which is to (i) determine the rules for use of the IT resources and communication tools of a business and (ii) set out the rights and obligations of users (employees and external service providers who may need to gain access to the IT system of a business) in order the ensure the security thereof. The goal is to protect the knowledge base of the business. In this respect, the charter enables the procedures for the cyber-surveillance and cyber-protection of employees to be approved and compliant, as well as for electronic evidence required in the event of a dispute to be collected lawfully.

A charter must be prepared in draft stages and requires the intervention of several departments: IT security, legal, HR etc. The document should be based on and be coherent with the existing PSSI.

An employer may include the charter as a schedule to the employment agreement but most often the IT charter will be annexed to the internal regulations of the business which is given to the employee together with their employment agreement. This obviates the need to negotiate the employment agreement with each employee or to enter into an amendment thereto each time the charter is updated.

WHAT SHOULD AN IT CHARTER PROVIDE?

The content of an IT charter shall vary in accordance with the context, constraints, aims and requirements of the business applying it. It should also be pointed out that there are no main principles or interpretations to be drawn from judgments of the Chinese courts where such matters are analysed on a case-by-case basis. Consequently, we strongly advise businesses to set out the conditions whereby their IT resources may be used and the procedures for the supervision of their employees in the charter. In any event, the charter should take into account the existing balance between the interests of the business (security requirements, management power of the employer etc.) and those of the employees. The content of the charter should not contravene statutory and regulatory provisions in force or impose obligations that are too restrictive and would infringe certain rights or liberties enjoyed by employees, such as the right to their private lives.

The charter should contain the following elements at least:

1. the scope of application of the charter (employees,temporary staff, interns, external service providers, entities concerned etc.) as well as the procedures for intervention of the teams in charge of the management of the IT resources of the business;

2. the means of authentication used by the business (logins/passwords, badges, thumbprints, facial recognition, hand outline etc.);

3. the security rules with which users must comply, such as notably the requirement to notify the internal IT department of any suspected breach or attempted breach of one's IT account and, in a general manner, of any malfunction; to never give one's login/password to a third party; to never install, copy, modify or destroy software without authorisation; to not install any VPN; to lock one's computer on leaving one's desk; to not access or delete information that is not relevant to the user's task in hand; to comply with the procedures defined beforehand by the business for copying data on removable media (USB keys, external hard drives etc.); not to view certain websites etc.;

4. the procedures for the use of IT and telecommunications tools provided such as:
- the workstation (personal storage area, whether or not the employee may store personal files on their workstation, the conditions under which the employer may access files stored on an employee's workstation etc.);
- nomadic equipment (notably in relation to teleworking);
- the terms of use of personal equipment;
- Internet (e.g. tolerated use if it does not affect an employee's productivity, prohibition from viewing certain websites, prohibition from downloading films, video games etc.);
- the use of certain social networks (WeChat, Weibo etc.) and rules in matters of communication;
- electronic messaging (rules for separating professional and personal e-mails; reminder of the rules in matters of communication through the firm's professional messaging service and the management of evidence; whether the employee's use of their professional e-mail for personal purposes will be tolerated; the conditions under which the employer may access the content of messages sent and received by an employee, e.g. where the employee is on holiday, etc.);
- use of telephones (are they to be used exclusively for professional purposes or is personal use tolerated? May an employer read the SMSs sent or received by an employee on a mobile telephone?);

5. the conditions under which an IT system is managed and the existence, if any, of supervision and surveillance mechanisms (traceability, geolocation, video-surveillance, telephone tapping etc.); and

6. the liabilities and sanctions incurred in the event of non-compliance with the charter (disciplinary sanctions or even criminal proceedings under certain circumstances).

HOW SHOULD THE CHARTER BE MADE BINDING ON EMPLOYEES AND SERVICE PROVIDERS, AND GIVEN BINDING FORCE?

In order to be binding on employees, certain formalities must be complied with when setting up an IT charter. Failing this, it will not have binding force.

In firms which do not have a trade union or employee representative body, the draft charter should be submitted for opinion and discussion to all the employees. The employer should take into account the comments made but is not obliged to accept them all. The final version of the charter is then sent to all the employees by e-mail with a read receipt, or handed to them against signature (for evidential purposes).

In firms that do have an employee representative body and/or a trade union, the draft charter should be submitted first to the body or trade union for opinion and discussion. The final version of the charter is then sent to all the employees by e-mail with a read receipt, or handed to them against signature (here again for evidential purposes).

In order for the IT charter to be binding on service providers, it should be attached as a schedule to the agreement for the provision of services entered into between them and the firm.