Cyber security: the new challenge for franchising

By **Mark Abell, Simon Shooter and Joe Jackson**, Bird & Bird

Cyber crime, the use of digital technology by unscrupulous individuals to obtain pecuniary advantages, is already a significant problem for franchisors and costs businesses millions of pounds a year.

It cost the UK retail sector alone over £205m in 2011-12, but this is only the tip of the iceberg and franchisors are very much at risk of being "holed in the side" by it.

They, therefore, need to take action now both to reduce their exposure to it and to get ready to comply with the regime that the government will be introducing to try and stem the flow of electronic crime. The BFA may also want to take steps to try and influence the way proposed legislation will impact on franchisors.

The cost of cyber crime

There is a lack of real information about the current extent of cyber crime in the UK and EU economies, but it is commonly acknowledged by all 28 governments to be a growing threat to the success of European businesses.

The most recent figures are to be found in the British Retail Consortium's recently published report, *Counting the cost of e-crime*. However, as costs of hacking, malware and DDoS (multiple Trojan Horse attacks) are not recorded, an exact value of the loss suffered is unclear. There are also some problems with the uncertain definition of cyber which leads to non-dependable estimates of impact and a black hole as a result of non-reporting by many companies.

The most common type of cyber crime which franchisors will be the victim of is 'card not present fraud', ID-related fraud (including account take over), phishing, hacking and DDoS. It is estimated that 86 per cent of attacks on UK companies originate in this country. After the U.S., UK brands are the second most commonly attacked.

As a result, companies are investing more and more money in preventative technology. This presents a whole new area of cost for franchisors if they are to protect the commercial interests of both themselves and their franchisees.

However, that is not the only challenge presented to franchisors by cyber crime. Compliance with the regulatory regime expected to be introduced is another. A challenge made more difficult by proposed legislation's apparent disregard for the difficulties that are particular to franchising.

Franchisors are also at risk of their trade secrets/know-how being misappropriated electronically. This presents another dimension to the concept of cyber crime.

Proposed European law

As part of its attempt to tackle this problem, earlier this year the EC published its cyber security strategy through which it aims to ensure a common level of network information security across the EU.

The Commission aims at improving Europe's network resilience, which includes raising awareness of the issues surrounding cyber security, developing an internal market for cyber security products and services and fostering R&D investment. Published alongside the strategy, and forming its main action, is a draft directive setting out a number of proposals designed to enhance the EU's resilience to cyber security threats.

Whilst still at an early stage, and with national implementation of any binding rules still some way off, the directive gives an indication of how regulation in this area may develop over the coming years. In particular, it suggests a greater focus on cyber security as part of organisational risk management.

It is important that franchisors are aware of the directive and its likely implications so that they are well placed to manage future regulatory change and the impact it will have on their franchise network. It is also important that the BFA considers how it can best influence the detailed contents of the law in respect of its impact on franchising.

● *The three authors are at international law firm Bird & Bird.*

How is cyber crime regulated?

The current regulatory landscape on cyber security has evolved piecemeal over time and is drawn from a number of sources including the following.

- Data protection rules requiring businesses in the EU to implement appropriate technological and organisational security measures against unauthorised or unlawful processing, accidental loss, and destruction or damage of personal data.
- The Electronic Communications Framework Directive and the Privacy and Electronic Communications Directive requiring public electronic communication service and network providers to ensure the security of their services and networks and report serious network security breaches to their national regulators.
- The Markets in Financial Instruments Directive requiring those in the financial services industry to adopt adequate risk management systems which by implication includes the adoption of network security risk management measures.

Some of these, especially data protection, have already presented challenges to franchisors and resulted in a number of substantial changes to their franchise agreements.

EU directive's aims

At its core the directive has two aims. The first is to ensure that EU countries and those private undertakings providing certain critical infrastructure within the

EU have an adequate strategy, and take appropriate steps, to deal with cyber security threats.

The second is to facilitate information sharing about cyber security threats between the public and private sectors and between EU countries. The directive also sets out in broad terms the obligations that Member States will be expected to impose at industry level.

National strategy

The directive proposes requirements on the establishment of national frameworks for network information security planning. If adopted, these proposals would require EU countries to take the following steps.

- Adopt a national strategy and cooperation plan regarding network and information security.
- Establish a national competent authority (NCA) tasked with monitoring the application of the directive. NCAs will also be required to contribute to [the directive's] consistent application across EU countries, though it is unclear what this will require NCAs to do in practice.
- Establish a Computer Emergency Response Team ('CERT') to work under the supervision of its NCA. The role of CERTs appears to be more hands-on than that of the NCAs and includes monitoring and responding to cyber security incidents, raising public awareness of cyber risks and forging co-operative relationships with the private sector.

The UK already has a national strategy on cyber security, published in 2011. More recently, the Home Affairs Committee issued a report on e-crime in July. The committee's report followed a ten-month inquiry and makes various recommendations for tackling cyber crime. Looking forward, it may be that the national strategy will be updated to reflect the requirements of the directive and the recommendations' stemming from the committees' report.

Information sharing

The directive also sets out plans for establishing a communication network, aimed at providing permanent communication between NCAs and the Commission. It is intended that the communication network will be used to as follows.

- Circulate early warnings of cyber risks and incidents. The directive would oblige NCAs to report risks and incidents that affect multiple EU countries, as well as those that exceed national response capacity or could grow rapidly in scale. There is a risk that in practice, EU countries might apply differing thresholds as to what sort of incident would trigger notification.
- Facilitate a co-ordinated response to cyber threats. The directive simply states that NCAs must agree on a response, though it does not make clear what would happen in the event that agreement cannot be reached. Furthermore, the effectiveness of any response could be undermined if delays are caused by having to get each EU country's approval.
- Exchange information and best practices. The directive envisages non-confidential information being made available through a common website and sensitive information being exchanged via a secure infrastructure.

How will franchising be affected?

Chapter IV of the directive sets out the minimum obligations that EU countries will be expected to impose on businesses. Franchisors will be regulated on the basis of either the sector they work in or the services they provide.

The Directive requires that EU countries impose the chapter IV obligations on certain market operators who provide the following.

- Critical infrastructure. This will include franchisors in the health, transport, education and financial services sectors for example.
- Information society services which enable the provision of other information society services, including e-commerce platforms, online payment gateways, social networks, search engines, cloud services and app stores. The directive is therefore unlikely to impact on all franchisors who provide online services to their franchisees.

Exemptions

The directive envisages that the chapter IV obligations will not be placed on so called micro-enterprises, or in other words, businesses with fewer than 10 employees and with an annual turnover of 2m Euros or less.

Whilst at first sight it is tempting to imagine that this will therefore exclude many smaller franchisors from the scope of the directive, there is much uncertainty around the definition of micro-enterprises and whether franchisees would be included in the franchisors' business for these purposes. Likewise, it is uncertain whether franchisees will be aggregated together for the purposes of the definition.

Scope of the directive

The inclusion of certain information society service providers suggests recognition of the importance of certain online functions in society today. Perhaps however the scope of market operators has been drawn too wide.

For example, whilst a case could be made for placing enhanced security requirements on internet payment gateway operators, social network providers might well wonder why they are being asked to comply with the same standards being placed on those in the energy, healthcare, education and financial services sectors.

It is unlikely to be a one-size-fits-all law and so there may be an opportunity for trade bodies, such as the BFA to set self-relevant standards.

Another concern for franchising is the lack of certainty over which businesses will be affected. The examples of market operators under the directive are described as non-exhaustive and EU countries may have different interpretations of these terms in practice.

This lack of clarity creates an uncertain outlook for businesses and carries a real risk that the directive will be applied inconsistently across the EU, making life still more complicated for franchisors doing business in a number of different member states.

The further risk is that even if the franchisor is not expressly caught by the provisions of the directive, but does business with organisations that are, those organisations may take the view that they will impose the directive's obligations on the franchisor and its franchisees as a condition of doing business. It is likely to lead to the government focusing on the most exposed and most affected, therefore includes retail.

Too onerous?

One cause for concern is that chapter IV requires EU countries to impose requirements that guarantee a level of security appropriate to the risk presented. ⮑

The impact this has on franchising could potentially be quite significant. It poses the question what level of investment and organisational effort would a franchisor need to undertake to guarantee its cyber security? In short, it is too early to say exactly.

One of the aims of the directive is to facilitate the exchange of information and early warnings amongst EU countries. In parallel, the directive asks the countries to impose notification and audit requirements at industry level. This raises the following issues.

- Market operators will be required to notify the NCA of any incidents that have a significant impact on its core services. No further guidance has been offered on what sort of incident would trigger mandatory notification and this could lead to uncertainty in practice.
- In turn, the NCA may make such information publicly available where it decides that it is in the public interest to do so. The chapter III provisions in the directive suggest that such information could also be exchanged between NCAs at a European level. Businesses may be reluctant to notify their NCA of any incidents through fear that the information will be shared further or made publicly available, particularly where its disclosure could result in bad publicity or breach of any confidentiality obligations that they owe to third parties or adversely impact on share prices.
- The directive proposes that NCAs are given broad powers to audit market operators and public administrations. As well as confidentiality concerns, businesses may also need to consider whether their commercial contracts allow them the freedom to facilitate such audits.

Possible sanctions

Failure to comply with the law could expose franchisors to penalties. The directive requires EU countries to adopt effective, proportionate and dissuasive sanctions for non-compliance. It does not prescribe the form of such sanctions, though it seems likely that they will be similar to existing regulatory punishments (e.g. fine, name-and-shame type notice, etc).

What does all this mean for franchise agreements?

We are in fear of the unknown. When adopted, the directive could have a significant impact on all of a franchisor's existing commercial contracts not just its franchise agreement. Franchisors should ensure that their franchise agreement is amended as follows.

- Tailoring confidentiality clauses accordingly.
- Ensuring sufficient audit rights are in place.
- Including appropriate change of law provisions (i.e. requiring the supplier to comply with all current and future laws).
- Obliging the franchisees and suppliers to comply with your reasonable internal cyber security standards, as may be updated.
- Making sure that a sufficiently robust contract change procedure has been included.
- Including appropriate indemnities from the franchisees, such as an indemnity against losses arising from breach of the cyber security law and payment of regulatory fines.

Headache for franchisors?

Franchisors, like all other businesses are becoming increasingly vulnerable to cyber crime. The interconnected nature of our networks means that individual EU countries cannot assess their cyber security in isolation from the rest of the digital marketplace.

The overarching purpose of the directive – to establish a common minimum standard of network security across Europe – should therefore be viewed as a legitimate aim.

In its current form (as is the case with most directives), the directive contains a number of flaws, the foremost being that key concepts are left open to interpretation by EU countries (such as the meaning of public administrations and significant impact).

These grey areas could lead to the directive being adopted inconsistently, causing a real headache for franchisors and other businesses that operate in multiple jurisdictions. It remains to be seen whether these issues will be resolved before the directive is adopted.

It also takes no account of the particular needs of franchising This adds still further uncertainty to both franchisors and franchisees.

It will also be of interest to franchisors to see how the directive is implemented at a national level. EU countries should be careful not to place unnecessary burdens on the businesses when introducing their own cyber regulations.

Role for the BFA?

Importantly, franchisors should be alert to the requirements that they could potentially face in the future, particularly with regards to notification and information sharing.

It may be that the BFA should start monitoring developments so that it can try to assert some influence on how the directive develops as regards its impact on franchisors.

Franchise agreements today typically include terms on data protection and other regulatory requirements, and with the directive in mind, express contractual provisions on cyber security may become more common.

Before entering into any long-term franchise agreements, franchisors should ask themselves: could my organisation be caught by the scope of the directive?

If the answer is yes, appropriate steps should be taken to future-proof their franchise agreements.

www.twobirds.com

New venue for BFA Manchester exhibition

The British Franchise Exhibition, held annually in the North, is moving from its traditional venue in central Manchester to Event City in Greater Manchester next to Trafford Shopping Centre at Salford, near the M60. It will take place on June 20 and 21.

The new site will make it easier for visitors from the whole of the North, particularly in the North-East, as the M60 adjoins both the M61 to the North, and the M62 to the West and across the Pennines to the East into Yorkshire. The site also offers over 3,000 free parking spaces.

Andrew Goodsell, of the show's organisers, Venture Marketing Group points out that the new venue by attracting visitors from the across the North will particularly attract franchise exhibitors offering territories across the whole region.

The show is exclusively supported by the BFA and all the exhibitors will be checked by the association that they meet its ethical trading standards.