BYOD and social media in the workplace — managing the risks

Robert Bond, Partner at Bristows, explores the challenges surrounding BYOD in the workplace, and advises on the some of measures organisations can take to mitigate the risks. Robert is a Member of the Examination Board of the Practitioner Certificate in Data Protection ***www.dataprotectionqualification.ie***

The days of spending long hours at work sitting at a desktop computer are steadily diminishing — great for work/life balance, but more problematic for workplace data protection. Individuals now use multiple devices for both work and pleasure, bringing opportunities and risks in equal measure. Whilst for some employers, there may be a temptation to ban the use of devices other than the corporate networked desktop, this is impracticable in an age where individuals expect to work remotely. The rise of BYOD (Bring Your Own Device, also known as Bring Your Own Disaster) coupled with the increase of the use of social media for work related matters, are bringing challenges that organisations are only beginning to address.

The key challenges concerning BYOD in the workplace are how to manage legal compliance and ethical issues, and in particular the risk of personal data incidents. In addition, there are the risks of the breach of confidentiality and the loss of commercial confidential information and trade secrets. This article explores the benefits and opportunities of BYOD, as well as the risks and responsibilities.

The BYOD policy

If BYOD is to be permitted (and really that is an inevitability), then controller organisations need to have a policy dedicated to setting out what is and isn't permitted. The policy can form a part of the organisation's broader data protection policy, or it can stand alone. Many organisations chose to deal with BYOD in a stand alone policy.

It is essential to remember that liability for any mishaps around BOYD will always fall on the employer. Or as the UK Information Commissioner has in the past put it: "it is important to remember that the controller must remain in control of the personal data for which he is responsible, regardless of the ownership of the device used to carry out the processing."

In deciding what needs to be addressed in a BYOD policy, the controller will need to assess:

- what type of data are processed;
- where those data may be stored;
- how they are transferred;
- the potential for data incidents;
- the blurring of personal and business use;
- the device security capabilities;
- the control of the device both during and after employment;
- the means with which to deal with loss or compromise of the device; and
- how to manage reputational brand and ethics issues.

The policy should address all of the above points in the depth required.

The benefit of the BYOD policy is that it can improve staff satisfaction and increase job efficiency since staff will not need to be tied to their desk in order to be productive. A good BYOD policy will set staff expectations and standards and ensure compliance with data protection and other relevant laws. The policy and training on the policy should help employees to be aware of confidentiality and data incident risks which will be of value for the protection of the organisation as well as employees themselves.

On the other hand, the challenges in rolling out a BYOD policy include balancing the employers governance needs with the rights of the employees. Since the employer is likely to require access to the personal device and will reserve the right to monitor compliance with the policy, then this may be regarded as a change to the terms of employment, and consultation will be required as well as a Data Protection Impact Assessment. Whether or not the device is supplied by the controller, or is the personal property of the employee, it will be important to guide employees as to how they should segregate business information used on the device from their own domestic and household communications.

The policy will need to cover access to the device in and out of the workplace, as well as managing platforms and apps used on the device, whether supplied by the business or downloaded by the employee. In implementing a suitable BYOD policy, regard will need to be had to how it interfaces with other policies and practices within the organisa-

tion. If the organisation has implemented an overarching data protection code or policy, then the BYOD policy will need to be integrated into that. To the extent that there will be parallel policies, again consideration will need to be given to how that BYOD policy sits alongside the information security policy, the incident response plan, the acceptable use policy and the social media policy (for example).

Finally, for any policy to be effective, it needs to be appropriately drawn to the attention of employees and so consideration will need to be given as to where the policy sits within the Staff Handbook, how it is communicated to existing staff and as part of the job applicant process and training will need to be given on how to adhere to the policy.

The risks of social media in the workplace

In addition to the risks of BYOD, there is an increasing risk from the use of social media, both by the organisation and by its employees individually. The shift from post and email as traditional methods of communication to the use of social media and related apps means that the instantaneous nature of the method of communication creates risks for the organisation in terms of loss of control, risk of breaches of confidentiality and trade secrets as well as the possibility, if not likelihood of, reputational and brand damage and financial harm.

More and more organisations are creating social media accounts as a method of marketing, sales and brand awareness, but there are many examples of where inadvertent postings or even mischievous postings by employees can cause irreparable damage.

There is no doubt that social media platforms enable the development of professional networking, knowledge building, strengthening of reputation, positioning of brand presence in the marketplace and as a recruitment tool.

On the flip side, the corporate risks are that staff may also be recruited through social apps, and the organisation will remain liable for the acts or statements of employees which has reputational risk and potential for financial loss. Other corporate risks include breaches of confidentiality and infringement of intellectual property, as well as a general failure to comply with information security duties. In much the same way as a balance has to be struck between the rights of the employer to monitor and enforce social media policies, the human dignity and data protection rights of employees need also to be adhered to.

Intellectual Property and trade secrets

The increasing use of devices to instantaneously share impressions and experiences through social media means that employers must recognise the risks that employees may post statements, materials and pictures such as 'selfies' which whilst intended to identify an event and individuals at that event, may also pick up in the background information that might otherwise be confidential to the business (for example, master plans on white boards).

The instantaneous nature of digital media and the speed at which a message of an image can spread means that organisations must not only protect the personal data of parties whose information is processed in the course of the use of social media, but also protect the businesses' intellectual property including trade secrets and/or the intellectual property and trade secrets of third parties for which the employer is also responsible.

Protecting trade secrets in the workplace

The Trade Secrets Directive (2016/943) aims to harmonise protection of trade secrets across the EU, rectifying issues caused by the lack of a consistently used definition. The Directive defines a trade secret as information which is:

- secret;
- valuable because of its secrecy; and
- subject to reasonable steps by the person in control of the information to keep its secret.

For the owner of a trade secret to be able to enforce the right to protect it, or to enforce that right against those that have unlawfully acquired the trade secret, the owner will need to show that sufficient steps have been taken to keeps its secret. Organisations will therefore need to:

- review their non-disclosure agreements and confidentiality clauses in their business contracts;
- review their technical and organisational security policies and procedures;
- ensure that contracts of employment and service contracts adequately address the protection of trade secrets;
- assess the use of BYOD in the workplace as well as web based applications, social media and other hosted solutions;
- increase risk management and monitoring in the workplace; and
- train staff on the need to be vigilant in terms of the security of trade secrets during their creation and then use.

Given the above, it is essential that in terms of the use of BYOD and social media in the workplace, attention is drawn to the protection of trade secrets as well as other intellectual property. If a trade secret is misappropriated or disclosed, it will be difficult for the owner to show that they treated the trade secret as secret if they cannot demonstrate appropriate policies and procedures, particularly around the use of BYOD and social media.

Robert Bond
Bristows
robert.bond@bristows.com