Cyber-Security

As we all know, cyber-security is rarely out of the news, and this won't change given estimates that by 2019, an additional 4.5 million cyber-security experts will be needed worldwide*.

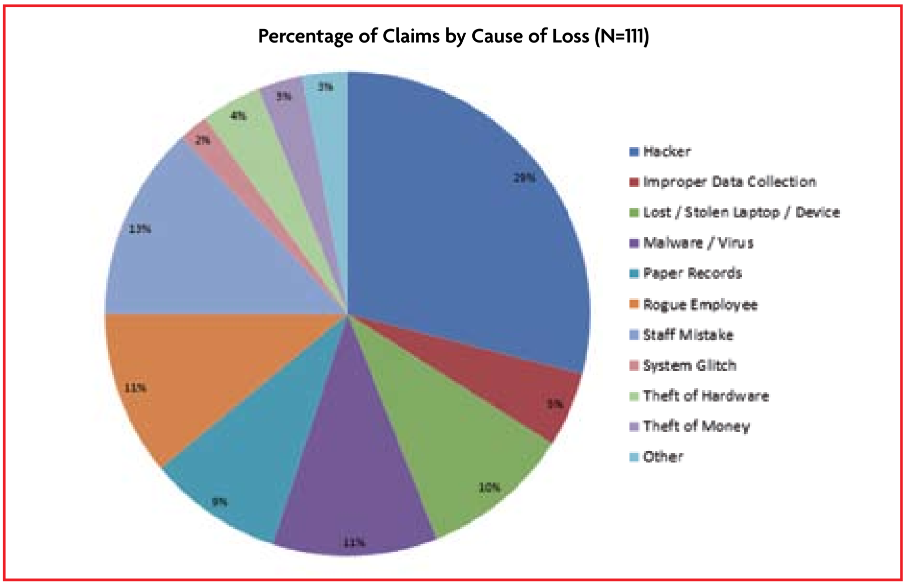
A study by PwC reported that in 2015, 38% more security incidents were detected than in 2014.** The recruitment industry has seen the impact of this increase in cyber security threats, with job postings in the US alone increasing 74% over the past five years, according to research conducted by the Bureau of Labor Statistics cybersecurity***.

And, understandably, companies are worried about the threat of an attack. In our own research amongst SMEs, we found that 76% of the companies are concerned about cyber-security, with 17% having experienced a cyber-attack.

Whilst HR Law might differ from country to country, the Web has no real international boundaries per se. With this in mind, this article will cover generic best practice with regard to HR policies and social media and what procedures need to be put in place to combat cyber crime and protect your business and customers, wherever you are in the world.

Our biggest observation when we discuss 'cyber-security' is often not 'computer security' but 'people security'. Whilst companies can have the very best tech in place and invest heavily in new systems, the fact is that around a third of data security issues are people-based.

Data is scarce but, in 2014, a cyber claims study conducted in the US found that over a third (34%) of claims for data loss was down to people security, with 11% of the dataset being rogue employees; 10% for lost or stolen laptop devices; and 13% for staff mistakes. Add to this a further 5% for improper data collection, and almost 4 out of 10 (39%) of the claims are because of the user.


Percentage of Claims by Cause of Loss (N=111)

Many organisations protect themselves from the usual business-critical blunders by having any potential issues covered off in the employee's employment contract and the company's policies and procedures. However, this is often not the case with data loss, as it is often not given the same priority as other 'serious' employment issues, such as inappropriate sexual or racial behaviour or financial misconduct. Organisations do need to make sure they have robust policies covering cyber/data security, data protection and IT and communications - policies which are communicated to employees who are made fully familiar with the rules and processes they are required to follow. Failure to ensure that data security is protected can put individuals at risk, cause them harm and distress, and result in a loss of reputation and prosperity to organisations. In the UK, the Information Commissioner has the right to levy fines of up to £500,000 for a serious breach of the data protection principles. The corporate fallout and financial implications can often be much more severe and broader in nature when cyber or data issues are involved. As the data controller, the organisation is responsible for making sure the confidentiality of the data they process is preserved.

> *In the UK, the Information Commissioner has the right to levy fines of up to £500,000.*

A business should also ensure that it has a social media policy in place which receives equal prominence within an organisation to other HR policies. Companies should put the social media policy in place, to provide employees with enforceable guidelines on:

- The company's level of tolerance for personal use of social networking services
- Details of what constitutes business damaging social media which is not illegal
- How the company will handle situations where employees post inappropriate and potentially business damaging, but not unlawful, posts such as illicit photos, profanity or other potentially derogatory content
- How the company will monitor compliance with the policy; and
- The sanctions imposed for any breach of the policy and the procedure through which those sanctions will be enforced.

The social media policy is in addition to having HR policies covering cyber/data security and a data protection policy that will cover the myriad of issues that a company might face, such as data handling, storage, transportation etc.

The key is that employees must understand that they are required to comply with these policies and that a breach of any of the policies is an HR issue that could ultimately lead to dismissal.

This is critical for any business, as although the legal framework is still being developed, it is clear that businesses can face public and private claims for breach of cyber-security. The security provisions in the Data Protection Act 1998 in the UK, for example, have been interpreted by the Information Commissioner's Office (ICO) to include cyberspace and to contain a duty for cyber-security to protect personal data from cybercrime. Complying with the seventh data protection principle requires an organisation to have appropriate technological and organisational measures in place to prevent personal data being lost, damaged or stolen. The ICO has heavily fined companies that have been hacked, and a failure to protect confidential information due to a lack of adequate cyber-security can also be a breach of the common law duty of care, therefore amounting to negligence.

Despite the fact that the legal framework is currently unclear, the standard that the law will apply is the consensus of opinion in the professions and industry about what constitutes good practice. For example, laptop computers holding sensitive personal data should be encrypted. Mobile telephones containing confidential data should also be passcode protected.

ISO 27001: 2013, which sets a standard for security management systems, is regularly cited by the ICO in enforcement decisions and regulatory guidance, and deals with such matters as Human Resource security.

The responsibility for monitoring and reviewing the operation of all cyber-security policies and making recommendations for change to minimise risks should lie jointly with HR and the Head of the IT Department, or someone in a similar position. In addition, according to the UK's Data Protection Act, any data controller must take reasonable steps to ensure the reliability of any employees who have access to personal data. Policies should be reviewed regularly to ensure that they meet legal requirements and reflect best practice in this ever changing and evolving area.

However, IT and human resources management need to be trained thoroughly on the appropriate and effective monitoring of employees, and enforcement of the various company policies, restrictions, guidelines and contract provisions relating to social media and cyber and data security. This should be done in compliance with employees' privacy rights. This is important as employees who breach any of the policies may be subject to disciplinary action up to and including termination of employment.

(source: BBC and Wales Online - http://www.bbc.co.uk/news/uk-wales-south-east-wales-35840428)

*** (source: PwC - http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html*

**** (source: Forbes - http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#1ca3749c7d27)*

KATHERINE MAXWELL
Partner and Head of Employment,
Moore Blatch
katherine.maxwell@mooreblatch.com

Katherine Maxwell is a partner and head of the Moore Blatch employment law team, based in their offices in Richmond and Southampton. She has been with the firm for 16 years and handles all aspects of employment law, acting for clients ranging from large corporations to small companies, both in the UK and internationally. Katherine is a member of the Employment Lawyer's Association.