It was revealed that the loss of highly valuable and sensitive data was the second biggest digital risk for 999 business leaders across Europe, when they were surveyed by Gowling WLG last year.

The risk of losing such data was only second to the threat of an external cyber-attack, which was the number one digital risk for those businesses questioned.

These two risks are somewhat inextricably linked; if your business does fall victim to an external cyber-attack, the data that you handle will be at risk of being compromised.

In addition to these findings, statistics published this week by the Department for Digital, Culture, Media and Sport (DCMS), from its forthcoming Cyber Security Breaches Survey 2018, show that less than half of the organisations surveyed have heard of the General Data Protection Regulation (GDPR) which takes effect on 25 May 2018. The number of organisations who reported having made changes to their operations in response to the GDPR was much smaller still, and less than half of those said they had made changes to cyber security practices.

So, how would a breach of cyber security affect my business?

In the words of Dr Adam Marshall, the Director General of the British Chamber of Commerce (BCC), "Cyber-attacks risk companies' finances, confidence and reputation, with victims reporting not only monetary losses but costs from disruption to their business and productivity".
Keeping a business safe from cyber threats can protect customer data, but it's also invaluable in safeguarding intellectual property, trade secrets, business assets, business continuity and reputation, and preventing downtime as well as to comply with laws and regulations are also all good reasons for doing so.

If that wasn't enough, the need to take action in protecting the data you handle is all the more acute given the GDPR will extend current data protection regulations from May 2018. As indicated in our previous briefing on the GDPR, the GDPR will increase companies' responsibilities and requirements to protect personal data. It will also impose tough penalties for failing to do so - depending on the breach, fines of up to four per cent of global annual turnover for the previous financial year or €20 million, whichever is higher, can be imposed.

In addition, the EU Network and Information Security Directive (NIS Directive) (otherwise known as the Cyber Security Directive), which came into force on 8 August 2016, must be implemented by Member States into their national laws by 9 May 2018. The NIS Directive is the first comprehensive piece of EU legislation on cyber security and will impose minimum harmonisation rules on EU Member States with the aim of preventing and responding to cyber disruptions and attacks.

Requirements on Member States under the NIS Directive include adopting a national strategy and regulatory measures for operators of essential services (within the energy, transport, banking, financial market infrastructure, health, water production and digital infrastructure sectors) and providers of particular digital services (online marketplaces, online search engines and cloud computing service providers) (DSPs). Such operators and DSPs will be required to adopt appropriate measures to manage security risks and to report incidents above certain thresholds to national competent authorities without undue delay. The Member States must enforce those requirements and put in place "effective, proportionate and dissuasive" penalties for non-compliance. There will be an obligation to share information with other affected Member States where an incident has a significant impact on the continuity of essential services in more than one Member State and provisions regarding when it will be necessary to notify the public.

The NIS Directive is not limited to personal data, as is the GDPR, but potentially covers any type of data breach or incident. A data security incident could therefore trigger notification obligations and penalties under both regulations.

The GDPR will be automatically binding and the cyber security directive implemented prior to the UK ceasing to be a member of the EU. The UK has committed to continuing to
adopt their provisions and/or fundamentally similar laws post Brexit. Therefore, they cannot be ignored.

What can I do to keep my business' data safe?

1. Review existing data protection and cyber security policies, procedures and checklists

Does your current security framework provide a level of protection appropriate to the level of the risk? If not then it will need to be refreshed.

Access the Government endorsed Cyber Essentials scheme which sets out basic technical controls across five areas: boundary firewalls and internet gateways, secure configurations, user access controls, malware protection and patch management. Many businesses already have controls in these areas but a report issued by DCMS last year indicates that few have yet applied for certification as having complied with them showing they have met good-practice standards in their cyber security.

Consider the 10 Steps to Cyber Security guidance produced by the National Cyber Security Centre which outlines the practical steps that organisations can take to improve their cyber security and protect their data, some of which are referred to above. Many organisations will already have taken certain technical controls but consideration should also be given to implementing some of the following if not already in place:

- **Managing user privileges** - restricting IT admin and access rights to specific users and placing security controls on devices
- **Monitoring** - monitor user activity and instigate regular health checks to identify cyber risks
- **Removable media controls** - ensure your policy covers what can be stored on removable devices such as USB sticks
- **Home and mobile working** - ensure your policy covers remote or mobile working when additional threats may occur through "free wifi" which may collect potentially sensitive data or be more susceptible to malware attacks.

In any case you will need to plan to ensure that appropriate cyber security measures will be in place to ensure compliance with the GDPR, and also the NIS Directive if relevant, including notifying security incidents. Put in place a breach team and train them to respond to incidents.
2. Incident management and learning from data breaches

Having an effective contingency plan or formal incident management process in place for the most disruptive breaches will help ensure the response to an attack is immediate and disruption and damage (financial and reputational) is kept to a minimum. Reviewing the response after an incident can prompt follow-up action points to raise awareness within the organisation and will help planning (and responses) for future attacks.

3. Raise awareness and train staff

According to the previous DCMS survey, the most common types of breaches can be linked to human factors, such as unwittingly clicking on a malicious link. Staff awareness and vigilance are essential to a business' cyber security alongside any technical and software protections. Raise awareness of the business' policy covering what staff are permitted to do on the business' IT devices and their personally owned devices if they are also used for business purposes. Educating all staff - not just specialist IT staff - on both the policy and potential cyber risk is essential and should be ongoing. Consider including such training as part of the induction process and include it as regular training activity - especially following incidents linked to human factors. It can take just a single, uninformed employee to cause a potentially substantive breach.

4. Engage senior management

It's really important that senior management are engaged. Again, the previous DCMS survey indicates that where designated senior management is engaged then businesses tend to treat cyber security as a higher priority than average.

For example, senior management and security personnel/teams should schedule regular 'sanity check' meetings (as well as with other departments) to allow people to voice their concerns. These meetings are also good opportunities to remind individuals of the cyber threat to your organisation.

5. Consider cyber security risks outside the business
Although many businesses may have concerns about suppliers' cyber security, the surveys mentioned above suggest too few do anything about it. Insist on your suppliers adhering to specific cyber security standards, codes of good practice or appropriate international standards (for example, depending on the circumstances, ISO 27001) which will drive up your own cyber security and potentially prevent a data breach. Suppliers agreeing to such requests demonstrate their reliability to their business clients and their understanding of the need to protect their client's interests.

Take a look at our digital risk calculator to find out if cybersecurity is one of your business' top five digital risks, and calculate your overall digital risk rating.

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.

Related  Cyber Security & Data Protection Law, ThinkHouse

Author(s)

Helen Davenport  
Partner - Birmingham

Email  
helen.davenport@gowlingwlg.com

Phone  
+44 (0)121 393 0174

vCard  
Helen Davenport