Cyber Risks & Liabilities

January/February 2019

Brexit is Coming: Prepare Your Data and Technology

Time is limited for the UK and the EU to craft a proper withdrawal agreement before Brexit takes place on 29th March 2019, leaving room for a range of possible outcomes. Despite the uncertainty, however, it's crucial for your business to be prepared for anything—especially in the realm of data and technology.

No-deal or not, ensure your organisation remains successful and compliant during the Brexit process with these top technology tips:

- **Transferring data**—Regardless of Brexit's impact, the GDPR is here to stay. But in terms of data transfers, it's important for your organisation to review its current export practices. Businesses that transfer data between the UK and EU should keep in mind that this could be considered an international practice post-Brexit. This means your organisation must comply with the GDPR's restrictions on international data transfers by creating a contractual clause.
- **Protecting your database**—Currently, an EU right known as the Sui Generis right protects all EU databases. In a no-deal, UK businesses established by UK nationals may lose this right. Protect your database in this scenario by including developers with EU connections in your workforce.
- **Securing your supply chain**—In the event of a no-deal, any arrangements your business has involving the circulation of technology or hardware with the EU may suffer at the hands of customs delays and potential border regulations. Be sure to revisit your supply chain and develop methods to limit your risk.
- **Reviewing your workforce**—Many UK organisations employ EU nationals within their workforce. This practice could be problematic if a no-deal takes place and changes current immigration requirements. Make sure all EU nationals have applied for 'settled status' to ensure they can continue working for your organisation post-Brexit.
- **Updating agreements**—Finally, your business should review all contracts and agreements for material technology with Brexit in mind. Pay close attention to elements such as the territorial scope of licences, the location of personal data, rights in databases and currency changes.

In addition, ensure ultimate peace of mind during Brexit by securing proper cover, such as trade credit insurance. For more information, contact Blackfriars Insurance Brokers Ltd today.

Blackfriars Group Insurance

Blackfriars Insurance Brokers Ltd
92 Irish Town
Gibraltar, GX11 1AA
200 77076
www.blackfriarsinsurance.gi

ICO Releases Top Tips for Passwords and Encryption Under the GDPR

While the GDPR has been in place for several months, the ICO kicked off the new year by updating their data protection guidance with more details in the realm of encryption and password practices. Here are the highlights:

- All organisations should possess a **proper encryption policy**, detailing the use of encryption and outlining associated staff training protocol. The policy should include these standards:
    - Encryption must be included in company risk assessments.
    - The planned encryption method should meet standards such as FIPS 140-2 and FIPS 197.
    - Personal data should be transmitted within an encrypted communication channel over any untrusted networks.
- The ICO emphasises that businesses with an **effective password system** possess these qualities:
    - The system needs a proper hashing algorithm. Never store passwords in plaintext.
    - All login pages require HTTPS protection. Limit available login attempts.
    - Users must create a password with more than 10 characters.
    - Two-factor or multifactor authentication should be available as needed.

Here's Why Cyber-Criminals Want To Attack Your Organisation

Regardless of size or industry, attackers often target companies for control of these assets:

Business plans or bids

Employee or customer personal data

Contracts with customers or suppliers

Source: Internet Security Alliance

Cyber and D&O Liability Go Hand in Hand: Principles for Handling Risk

In recent years, UK organisations have experienced a dramatic increase in the prevalence of cyber-attacks, increasing the need for cyber-security risk management. **Recent industry research found that there were as many cyber-claims in 2018 as there were in the past four years combined.**

And while this alarming statistic emphasises the importance of implementing initiatives to protect your organisation's data, doing so can also help limit your directors' and officers' (D&O) liability concerns.

Under the GDPR, directors and officers are largely responsible for prioritising cyber-security throughout their organisation. With this in mind, senior leadership could face serious consequences if your business suffers from a data breach. Consider the following tips to reduce cyber-risk and protect your senior leadership:

- **More than IT**—Many organisations fail to understand that cyber-security should be considered a companywide risk management concern—not just something for IT to handle. Break this stigma among your directors by incorporating cyber-security into routine senior-level discussions. These conversations should pertain to your most critical data assets, including where data is located and who has access to it. In addition, discuss what security controls you have in place and how often they are tested.
- **Legal concerns**—Your leaders should know what is legally required of them in terms of establishing proper cyber-security measures. In addition, they must document evidence of compliance.
- **Access to expertise**—As well as discussing cyber-security in senior meetings on a routine basis, directors should also receive input from cyber-security experts during these conversations.
- **Company culture**—Directors need to help generate a culture that prioritises cyber-security by setting standards for management, training staff members and providing a proper budget.

Apart from risk management, protect your organisation with robust cyber and D&O cover. For more information, contact Blackfriars Insurance Brokers Ltd today.

This publication is for informational purposes only. It is not intended to be exhaustive nor should any discussion or opinions be construed as compliance or legal advice. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.