CYBERRISKS+LIABILITIES

January/February 2016

IN THIS ISSUE

Common Applications May Expose Companies to Data Breaches

Common applications—such as Word and Excel—could unintentionally contribute to a data breach.

EU General Data Protection Regulation Takes Shape

The General Data Protection Regulation will affect each of the 28 European Union (EU) member states and introduce significant data protection changes.

Recent Cyber Security News and Prosecutions

Read about how the average cyber criminal is most likely under the age of 20 and how an HIV patient support service was fined after exposing sensitive patient information.

Crendon Insurance Brokers

Common Applications May Expose Companies to Data Breaches

It may seem that common applications such as Word and Excel are intuitive enough not to generate a data breach by inadvertently hiding sensitive data. Yet, the government’s 2015 Information Breaches Survey revealed that 50 per cent of all data breaches were caused by inadvertent human errors. Each of these breaches cost those companies, on average, between £75,000 and £311,000 due to business disruptions, reputational damage and time spent fixing the breach.

To prevent an application from causing a breach by inadvertently hiding information, be on the lookout for these four sources of hidden data:

1. **Hidden columns:** Hiding sensitive data in a spreadsheet is not as secure as you might think. For example, setting a column to hidden leaves obvious clues as to how to retrieve that information—such as a gap in numerical or alphabetical sequencing. To ensure that you share only the data you want, check for hidden columns or export the spreadsheet to a comma separated value (CSV) format.

2. **Pivot tables:** A pivot table is an optional function of a spreadsheet application and is capable of summarising a large set of data. Yet, a separate spreadsheet of the original, raw data may still exist and be hidden from view. To ensure that only the information displayed in the table is shared, you can either export it to a CSV format, or copy the table and paste only the values into a new workbook.

3. **Ineffective redaction:** When you want to redact or irreversibly remove data, it should only be redacted from a copy of the document—not the original. Also, highlighting the text in black does not permanently hide the obstructed text as a user could simply copy and paste the information in a new document, revealing the text obscured in black. For best results, use a specific redaction software.

4. **Meta data:** Meta data refers to the ‘data about data’ which is embedded within files, such as when and where a photo was taken or the comments of a document’s previous author. As you may not want to share all of this data, use bespoke redaction software to remove it.

By adhering to the guidance outlined above, you can help ensure that you and your employees only share the information that you want to.

Recent Cyber Security News and Prosecutions

Teenage cyber criminals becoming the norm

According to the National Crime Agency (NCA), the average age of suspected cyber attackers has dropped to 17. Investigators attribute this to youths being swayed by the allure of validation from others in the cyber community. Experts also predict that this praise has contributed to these youths joining organised cyber-crime groups.

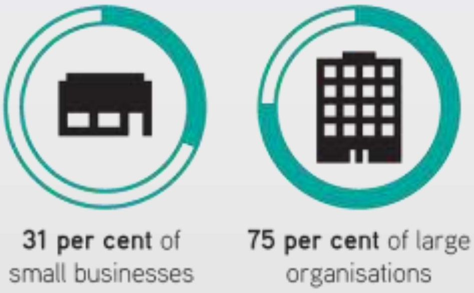
To address the potential allure of cyber crime, the NCA has launched the Cyber Choices campaign. The purpose of the campaign is to help parents of boys ages 12 to 15 educate and persuade their children to not be swayed by the allure of cyber crime.

HIV patient support service fined after accidentally exposing its patient list

The Bloomsbury Patient Network was fined £250 after it inadvertently revealed the identities of HIV patients through an email error. In a newsletter offering support and guidance for HIV patients, the organisation included the email address of 200 patients in the 'To' field rather than the 'Bcc' field—revealing 56 full or partial names. This is the second incident of this type in three months for the organisation.

In its investigation, the ICO found that the incident had occurred before it had provided the organisation with guidance on how to mitigate these types of cyber risks. While the issued fine was relatively small, the ICO had the authority to issue a fine of up to £500,000. The incident emphasises that all organisations, even if they are an unincorporated association, will be held financially responsible.

In 2015, a staff-related security breach affected:



SOURCE: GOV.UK

EU General Data Protection Regulation Takes Shape

In December, the European Parliament and Council agreed upon the final structure for the General Data Protection Regulation (GDPR) proposed by the European Commission in January 2012. The regulation was designed to unify data protection legislation across all 28 EU member states, and it requires all foreign companies to adhere to its statutes if they want to conduct business with a company in the EU. In addition, the regulation is expected to strengthen data protection for EU citizens, set clear and modern rules for businesses, and bolster data protection legislation. These objectives are expected to be met through the introduction of significant changes to the following two areas:

3. Data subjects

A data subject refers to any individual who is the subject of personal data—which includes all information that can identify and refer to that living individual. The regulation will create the following:

- A new right to 'data portability', which will enable data subjects to transfer their personal data between service providers
- A clarified 'right to be forgotten', which will guarantee that if subjects do not want their data to be processed any longer and if there are no legitimate grounds for retaining it, then their data will be deleted
- The possibility of contesting targeted online advertising
- Specific protection for vulnerable data subjects
- Methods of facilitating action against non-compliant data controllers

4. Businesses

Under the GDPR, businesses will be required to do the following:

- Establish a principle of accountability for the personal data that they are responsible for managing
- Ensure that data protection safeguards are built into products and services
- Complete data protection impact assessments which outline their procedures to effectively protect personal data
- Appoint a data protection officer, who will advise on situations involving data protection law, and will develop a business' privacy and data protection policies
- Report data breaches that would likely harm data subjects to the national authorities within 72 hours

In addition, businesses will no longer be required to notify the local data protection authorities, which is expected to save an estimated £100 million. However, if a business fails to follow any obligations outlined by the GDPR, the data protection authorities have the capability to issue a fine of up to 4 per cent of its total turnover.

Although the GDPR has not yet been formally adopted, the European Parliament and Council expects to do so in the coming weeks. After formal adoption, the GDPR will come into force in 2018. Your business should utilise this time in between to implement the required practices listed above.

Crendon Insurance Brokers Ltd

0121 45 45 100

www.crendoninsurance.co.uk

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.