Cyber Risks & Liabilities

May/June 2019

Government Releases Annual Data Breach Survey Results

As data breaches remain a rising threat across industry lines and the GDPR celebrates its first anniversary, the past year has seen a continued increase in organisations prioritising cyber-security. And rightfully so—the Department for Digital, Culture, Media & Sport recently released their annual cyber-security breaches survey, complete with robust statistics supporting the importance of implementing risk management measures against data beaches.

Be sure to review the following key statistics from this year's survey and consider what you can do to bolster your organisation's cyber-security practices:

- **Breaches are common**—No establishment is immune to cyber-attacks. In fact, over 30 per cent of businesses and over 20 per cent of charities experienced a breach in the past 12 months. And that's just what we know about. What's more, 30 per cent of businesses and 21 per cent of charities reported suffering negative impacts from a cyber-incident in the last year—including temporary loss of access to files or networks, corrupted or damaged software systems and websites, or online services either taken down or slowed.
- **These forms of attack are deadly**—Of the various ways an organisation can suffer from a data breach, the most disruptive forms included being sent fraudulent emails or links, others impersonating the organisation in emails or online, and viruses or malware.
- **The price tag is significant**—It's no secret that a cyber-attack can entail wasted time and money for an organisation. In terms of their most disruptive breaches, businesses spent an average of three days handling an attack (4.5 days for charities) and paid average costs of £4,180 (£9,470 for charities)—a price tag that has risen by nearly £2,000 in the past two years.
- **Organisations are taking action**—To combat the growing threat of cyber-attacks, organisations have taken considerable strides to bolster their cyber-security efforts. Common risk controls include applying software updates when available, having up-to-date malware protection and using firewalls with appropriate configuration. In addition, 33 per cent of businesses and 36 per cent of charities now have formal policies covering cyber-security risks.
- **The GDPR made a difference**—Since it's implementation, 30 per cent of businesses and 36 per cent of charities have made changes to their cyber-security practices due to the GDPR.
- **Insurance is still lacking—Despite the efforts taken to improve cyber-security, only 11 per cent of businesses and 6 per cent of charities have a cyber-security insurance policy**. Don't miss out on the best protection against a cyber-attack—for more information on cyber-insurance solutions, contact Crendon Insurance Brokers Ltd today.

Crendon Insurance Brokers

Crendon Insurance Brokers Ltd
0121 454 5100

www.crendoninsurance.co.uk
enquries@crendoninsurance.co.uk

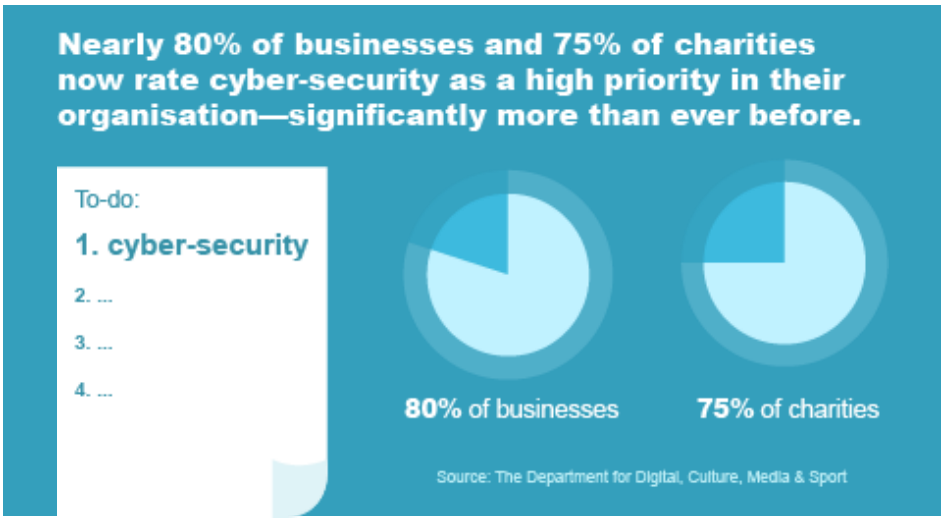
Cyber-exposures to Consider in Your D&O Policy

As a senior-level leader within your organisation, the consequences of a cyber-attack expand even further than that of lost data or resources, and business interruption. Indeed, suffering from a data breach could also place you, as an individual, in a dangerous position regarding directors' and officers' (D&O) liability.

In the event of a cyber-incident, senior-level management members like yourself risk being held accountable if you fail to take adequate steps to prevent a breach or implement proper cyber-security measures. With this in mind, it's crucial now more than over to ensure you have robust D&O cover that takes into consideration the following cyber-exposures:

- **Investigations**—Following a data breach, various regulatory investigations could take place to determine if legal action is needed. It's important to incorporate these investigation costs into your D&O policy.
- **Allocation**—If a cyber-attack occurs, you will want to establish a clear boundary between cover for the organisation as a whole (cyber-cover) and cover for yourself (D&O insurance). Be sure to attribute losses and allocate cover appropriately. In addition, ensure any leaders involved in significant cyber-related decisions are properly insured.
- **Reputational damage**—As the leader of an organisation that suffered a breach, you could face reputational injury for years to come. Consider including the costs of limiting reputational downfall within your policy.

For more guidance on finding the right D&O policy for your cyber-risks, contact ***Crendon Insurance Brokers Ltd*** today.



GDPR Compliance Is Paying Off: Here Are the Numbers to Prove It

In the year since the GDPR was officially implemented, recent reports from Cisco revealed the wide range of benefits that compliant organisations have experienced in the last 12 months.

While ensuring GDPR compliance may have felt like a tedious or unrewarding process within your workplace, the following statistics emphasise how these efforts have truly paid off:

- **Shorter sales delays**—GDPR-ready organisations experienced significantly shorter sales delays due to customer privacy concerns. While non-compliant businesses suffered from average delays of 5.4 weeks, those that were prepared for the GDPR dealt with average delays of just 3.4 weeks—totalling a 14-day difference.
- **Fewer data breaches**—Although a large majority of organisations reported that they had experienced a data breach within the past year, a closer look at compliance numbers revealed that GDPR-ready establishments still reaped some benefits. Indeed, compliant organisations were 15 per cent less likely to have experienced a data breach when compared to unprepared businesses.
- **Better data security**—One of the most difficult aspects of a data breach is dealing with the consequences of stolen, missing or deleted data records. But with the help of GDPR compliance, prepared organisations suffered from far less impacted data records during a breach—an average of 79,000 impacted records compared to 212,000 for non-compliant establishments.
- **Decreased downtime**—It's no secret that time is of the essence during a cyber-attack. And fortunately, for compliant organisations, GDPR-preparedness saved them an average of three hours in system downtime following a breach. While these businesses took an average of 6.4 hours to recover, unprepared organisations required 9.4 hours to get their systems up and running again—longer than the span of an average working day.
- **Lower costs**—More than anything, the financial burden of a data breach can be significant. But in the case of GDPR-ready organisations, only 37 per cent had losses of over £500,000 after a cyber-attack, whereas 64 per cent of the least prepared establishments suffered such losses.