telecoms world PLC

White Paper

# UNDER ATTACK:

## The Year in Breach

# SUMMARY

If we were to record a time-lapse of data breaches across the globe in 2019, it would reveal consistent increases in four key categories:

**COST** **SIZE** **IMPACT** **TIME**

**According to the 2018 Cost of Data Breach by the Ponemon Institute, aside from a 6.4% year-over-year lift on the average total price tag of a single breach (now £2.26B), the number of records lost or stolen has climbed by 2.2% this year alone.**

**To make matters worse, the consequences of each record compromised continue to skyrocket. The global average per capita cost went from £107 to £112, with United States and Germany leading at £177, £153 respectively. This means that the more records lost, the greater the cost of the breach.**

### THE AVERAGE TOTAL COST OF A BREACH INCREASED

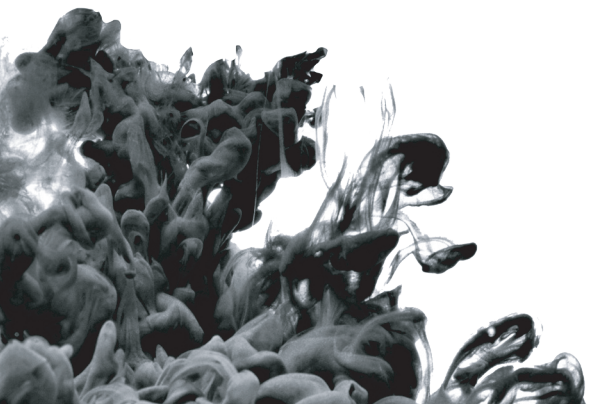
£2.75 Million → *6.4% INCREASE* → £2.93 Million

### THE AVERAGE SIZE OF A DATA BREACH HAS INCREASED

*2.2% INCREASE*

### THE AVERAGE TOTAL COST OF A RECORD LOST DUE TO A BREACH INCREASED

£107 per Record → *4.8% INCREASE* → £112 per Record



# GDPR

Introduced in May, the privacy regulation applies to any organization that collects or processes data about EU citizens. The business implications are stringent, ranging from a 72-hour window for notifying authorities to fines of up to 4% of annual global revenue. Companies across the world are taking notice, doubling down on investments in cybersecurity governance and risk mitigation. It should be noted that with the GDPR in full effect, the number of breaches reported is likely to increase due to strict notification requirements.

Regardless, privacy regulations are far from a catch-all solution for preventing data breaches. Although there were plenty of security incidents recorded in 2018 for Europe, the next page shows some of the most significant.

## KEY GDPR CHANGES:

BREACH NOTIFICATION

INCREASED TERRITORIAL SCOPE

PENALTIES

CONSENT

RIGHT TO ACCESS

RIGHT TO BE FORGOTTEN

PRIVACY BY DESIGN

DATA PROTECTION OFFICERS

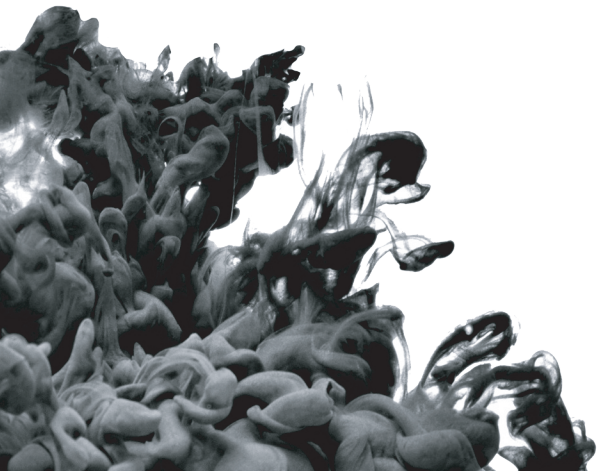

UK supermarket Morrisons will face a massive payout to staff after losing an appeal for a class action decision. The lawsuit stems back to a data leak from 2014 involving Andrew Skelton, a senior internal auditor, who posted personal and payroll details of more than 100,000 employees. The High Court ruling determined that the firm was liable for Skelton's actions, setting precedents for increased scrutiny, more class action lawsuits surrounding data breaches, and yet another cost that must be factored into corporate risk assessments.

During a 2-week online hack back in August, credit card details for almost 250,000 customers of British Airways was stolen and sold for up to $12.2M on the Dark Web. Cybersecurity intelligence firms Flashpoint and Risk IQ demonstrated how payment information went for sale between £8 to £45 per card, and was linked to a Russian hacking group known as Magecart.

FIFA admitted to suffering a hack via phishing campaign, where UEFA staff was tricked into sharing password-protected login details. The revelations are based on information accessed by the Football Leaks organization, which sent over 70M documents and 3.4 terabytes of data to German magazine Der Spiegel for analysis. Keep in mind that this the second large-scale cyber attack that FIFA has experienced in recent years, immediately following the 'Fancy Bear' hack originating from Russia in 2017. It is reported that the threat of cyber attack has become so important that UK's National Cyber Security Centre (NCSC) briefed the England national football team on how to avoid cybercrime during the World Cup.

# CONCLUSION

When we reflect on data breaches in 2019, it will be important to account for the good with the bad. Even though cyber attacks are growing in cost, size, and impact, there is an enhanced sense of global awareness and vigilance that will serve as the foundation for better cybersecurity. With privacy regulations taking shape in countries that are most affected, we can predict that identification, escalation, and mitigation will be the focus of many organizations going forward. As we've all heard before, it's no longer a question of "if," but "when" a company will get breached. In order to future-proof ourselves, our employees, and our customers, it will become paramount to invest in solutions that can pinpoint threats proactively, contain compromises quickly, and empower parties that are affected so that they can take action.



# SOURCES


- https://www.ibm.com/security/data-breach
- https://breachlevelindex.com/
- https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline
- https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html
- https://www.reuters.com/article/us-twitter-passwords/twitter-urges-all-users-to-change-passwords-after-glitchidUSKBN1I42JG
- https://securingtomorrow.mcafee.com/consumer/consumer-threat-notices/exactis-data-breach/
- https://www.pymnts.com/legal/2018/exactis-data-breach-class-action-lawsuit/
- https://www.wired.com/story/exactis-database-leak-340-million-records/
- https://www.cnet.com/news/exactis-340-million-people-may-have-been-exposed-in-bigger-breach-than-equifax/
- https://www.cpomagazine.com/2018/10/04/facebook-data-breach-resulted-in-50-million-compromised-accounts/
- https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html
- https://www.wired.com/story/facebook-security-breach-50-million-accounts/
- https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-databreach
- https://www.wired.com/story/under-armour-myfitnesspal-hack-password-hashing/
- https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html
- https://www.fastcompany.com/90274708/500m-marriott-customers-data-hacked-heres-what-we-know
- https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018
- https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach
- https://www.washingtonpost.com/technology/2018/12/12/us-investigators-point-china-marriott-hack-affectingmillion-travelers/?noredirect=on&utm_term=.3ebd451168ba
- https://duo.com/blog/canada-breach-reporting-law-goes-into-effect-november-2018
- https://www.cbc.ca/news/business/pipeda-privacy-data-1.4886061
- http://www.mondaq.com/canada/x/729560/data+protection/Craft+Beer+Industry+Incentives+Deemed+Unconstitutional
- https://www.mcinnescooper.com/publications/the-digital-privacy-act-5-faqs-about-the-new-mandatory-breachresponse-obligations-effective-november-1-2018/
- https://www.forbes.com/sites/kateoflahertyuk/2018/10/22/this-is-what-the-morrisons-data-leak-class-action-meansfor-future-breaches/#10f0c5072328
- https://www.bbc.com/news/business-45943735
- https://www.itpro.co.uk/security/32275/fifa-discloses-massive-hack-as-internal-documents-are-leaked-to-press
- https://www.computerworlduk.com/security/fifa-hack-threatens-further-embarrassment-footballs-governingbody-3686106/
- https://www.securitynewspaper.com/2018/11/10/fifa-is-hacked-once-again/
- https://www.telegraph.co.uk/business/2018/09/06/british-airways-hacked-380000-sets-payment-details-stolen/
- https://www.theweek.co.uk/96327/british-airways-data-breach-how-to-check-if-you-re-affected
- https://www.cnbc.com/2018/10/16/facebook-hack-affected-3-million-in-europe-first-big-test-for-gdpr.html
- https://www.forbes.com/sites/kateoflahertyuk/2018/10/22/this-is-what-the-morrisons-data-leak-class-action-meansfor-future-breaches/#45ce84b92328
- https://www.stuff.co.nz/business/better-business/105264055/mandatory-data-breach-law--what-this-means-for-yourbusiness
- https://www.reseller.co.nz/article/643820/assessing-top-nz-security-breaches-2018/
- https://www.kennedyslaw.com/thought-leadership/article/australias-new-data-breach-notification-laws-take-effecttoday
- https://www.zdnet.com/article/notifiable-data-breaches-scheme-getting-ready-to-disclose-a-data-breach-in-australia/
- http://www.legislation.govt.nz/bill/government/2018/0034/latest/LMS23223.html
- https://www.darkreading.com/vulnerabilities---threats/2018-on-track-to-be-one-of-the-worst-ever-for-data-breaches/d/d-id/1333252