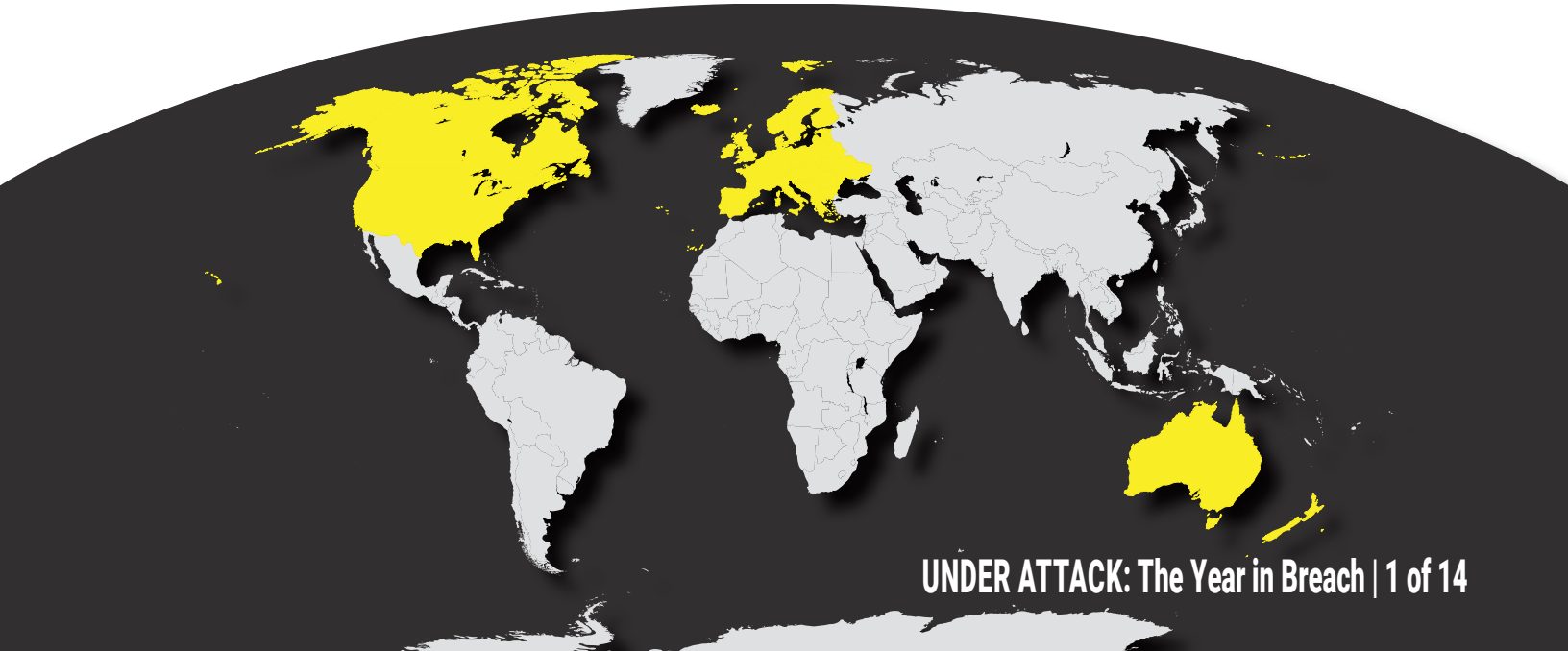
White Paper

UNDER ATTACK:
The Year in Breach

601-427-4185 | sales@bcianswers.com

TABLE OF CONTENTS



SUMMARY

If we were to record a time-lapse of data breaches across the globe in 2018, 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 $3.86B), 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 $141 to $148, with United States, Canada, and Germany leading at $233, $202, and $188, respectively. This means that the more records lost, the greater the cost of the breach.

THE AVERAGE TOTAL COST OF A BREACH INCREASED

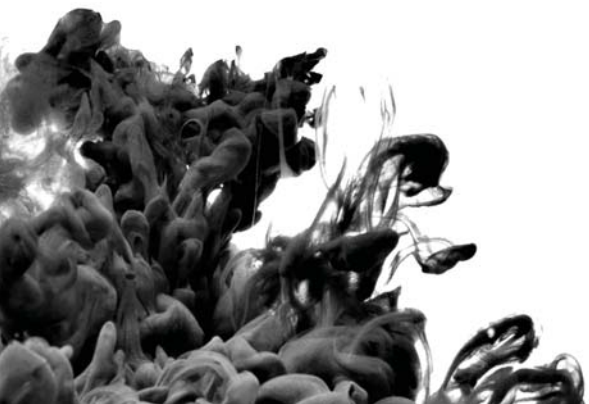
$3.62 Million → 6.4% INCREASE → $3.86 Million

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

$141 per Record → 4.8% INCREASE → $148 per Record



However, a common theme that emerges is the importance of speed in detection and mitigation, which can significantly lower the burden of a breach. Although the mean time to identify (MTTI) and contain (MTTC) rose to record highs of 197 and 69 days, organizations that were able to contain a breach in less than 30 days saved over $1M compared to those who took longer. To put this into perspective, the average cost savings generated from working with an Incident Response (IR) team were as high as $14 per compromised record.

Meanwhile, privacy regulations such as the European Union's General Data Protection Regulation (GDPR) and Australia's Notifiable Data Breach (NDB) are shining a bright beam on the most prevalent breach type: identity theft. Gemalto's Breach Level Index reports that identity theft represented 65% of the breaches that occurred in the first half of 2018, such as Exactis and Firebase. As we've seen in the past, once cyber criminals get their hands on personal information, they will monetize it by selling identity footprints directly on the Dark Web or organizing payment fraud schemes.

Follow along as the ID Agent Team explores the global landscape of data breaches across United States, Canada, Europe, and Australia/New Zealand, providing you with actionable insights for protecting your customers and employees.

BCI

UNITED STATES

A quick glance at recent headlines can characterize most US data breaches in 2018: newsworthy and expensive. At $7.91M, the average total cost in the United States is the highest around the globe. Although this can be largely attributed to organizational spending on post-breach responses, notification costs, and customer churn, it also highlights a cultural phenomenon.

Current American legislation surrounding notification laws creates a domino effect, where the end-user has greater awareness of data breaches, higher expectations for identity protection by companies, and fleeting loyalty caused by the availability of other options. Such insight is illustrated by the $4.2M cost of lost business for US organizations, a number that is nearly twice as high as the next runner-up.

BCI

TIMELINE OF U.S. BREACHES IN 2018

March

FACEBOOK AND CAMBRIDGE ANALYTICA

87M

On March 17, 2018, it was revealed that Cambridge Analytica was responsible for harvesting private information from Facebook profiles on over 50M users without their permission. However, Facebook later confirmed that it affected 87M users, with 70.6M being in the United States.

UNDER ARMOUR

150M

In late March, Under Armour announced that a data breach affected an estimated 150M users of its MyFitnessPal application. Compromised information included usernames, email addresses, and hashed passwords.

May

TWITTER

330M

Twitter urged more than 330M users to change their passwords after reporting that a glitch caused data to be stored in readable text rather than being hashed.

June

EXACTIS

340M

In late June, a security researcher discovered that the database of marketing firm Exactis was being stored on a publicly accessible server with 340M records exposed, including phone numbers, home and email addresses, interests of consumers, the number/age/gender of their children, along with business contacts. This has sparked a class action lawsuit.

September

FACEBOOK

50M

Facebook notified users in late September that yet another massive data breach compromised the accounts of over 50M users. Hackers exploited a security weakness present in the social network's code since July 2017 to steal automated log-in credentials, also known as access tokens.

November

MARRIOTT

500M

Revealed on November 30th, this hack had been continuously compromising data on guests staying at Marriott Starwood properties since 2014, including everything from names, addresses, phone numbers, passport numbers to payment card numbers and expiration dates. Recently, it was discovered that the cyberattack may be part of a Chinese intelligence-gathering effort.

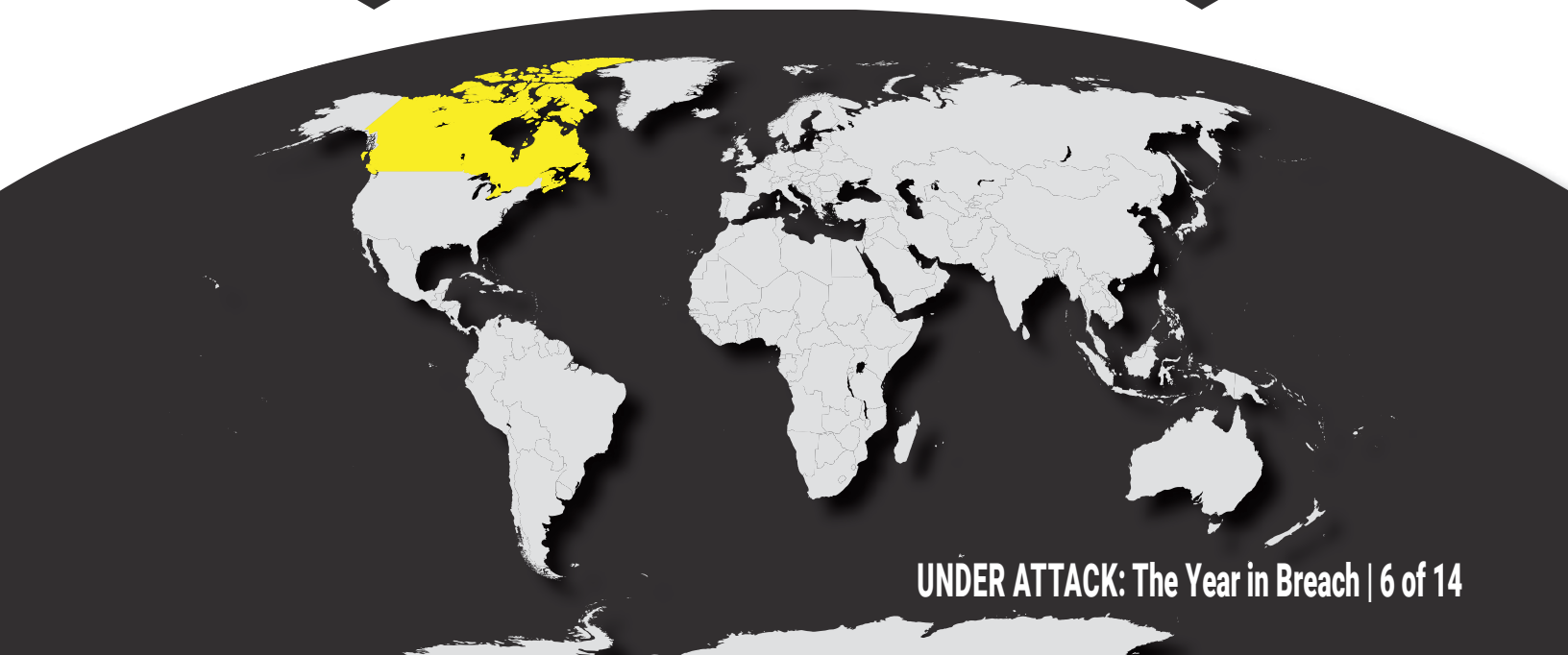
CANADA

As mentioned earlier, Canada ranks second for highest average per capita costs, at $202 per record, with an average number of 22,275 records compromised in a single breach. Within the first half of 2018 alone, Canada experienced 19 security incidents, resulting in the exposure of 6,295,443 breached records. A closer look at the data reveals that the numbers are driven by three key factors:

THE SEVERITY OF MALICIOUS OR CRIMINAL ATTACKS

DIRECT COSTS

DETECTION AND ESCALATION COSTS



At $86 per compromised record, Canada commands the highest direct costs, which refers to expenses related to "engaging forensic experts, hiring a law firm, or offering victims identity protection services." Additionally, detection and escalation costs are the largest in Canada, at $1.78M. Along with breach identification and mitigation, these costs include assessment and audit services, crisis team management, and employee/investor communications. However, Canada also spent the second most to resolve a criminal cyber attack, costing companies $213 per record, compared to the global average of just $128 per record.

With such data in mind, it is clear that data breaches are becoming a growing concern for Canada. This is further evidenced by legislation just put into place, mandating that companies must report breaches to the Office of the Privacy Commissioner (OPC) of Canada. Known as the Personal Information Protection and Electronic Documents Act (PIPEDA), it requires companies to alert their customers any time there is a risk of "significant harm to an individual," among other stipulations.

However, similar to the plight of EMV (Europay, Mastercard and Visa) adoption in America, there is a lag in awareness and adoption by business owners. As Monique Moreau, VP at the Canadian Federation of Independent Business, puts it: "the vast majority of business owners don't know that this is happening. Among all the changes and government regulations, data breach reporting requirements are not going to be top of the list." It remains to be seen how the law will be enforced, along with the response companies will have when their bottom line is threatened.

AVERAGE PER CAPITA COST = $202 PER RECORD

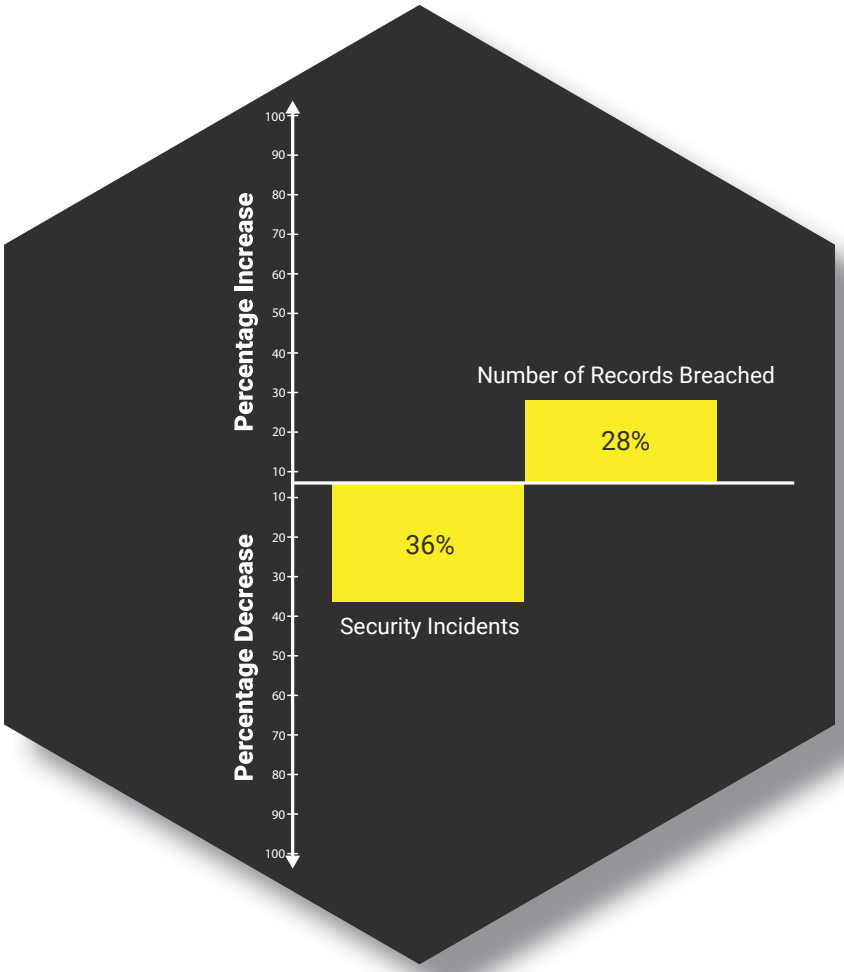
SPENDING ON CRIMINAL CYBER ATTACK RESOLUTION = $213 PER RECORD

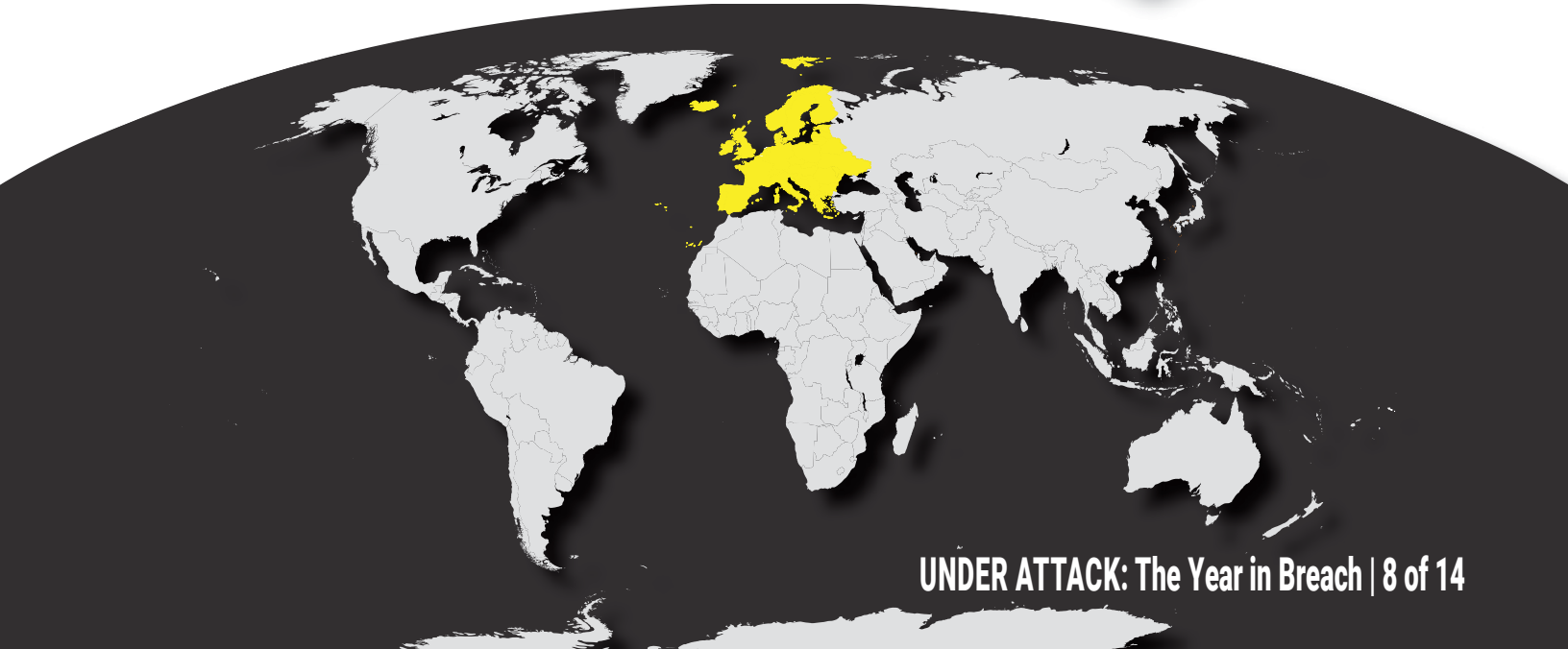
AVERAGE NUMBER OF RECORDS COMPROMISED IN A BREACH = 22,275

AVERAGE DETECTION AND ESCALATION COSTS = $1.78M

EUROPE

During the first half of 2018, Europe saw a 36% decrease in security incidents but surged by 28% in the number of records breached, signaling a rise in the severity of cyber attacks. Nevertheless, Europe represented just 4% of all breaches globally, with the United Kingdom accounting for 22 of 36 incidents. However, any discussion encompassing the state of European data breaches in 2018 would be remiss without mentioning the impact of the General Data Protection Regulation(GDPR).



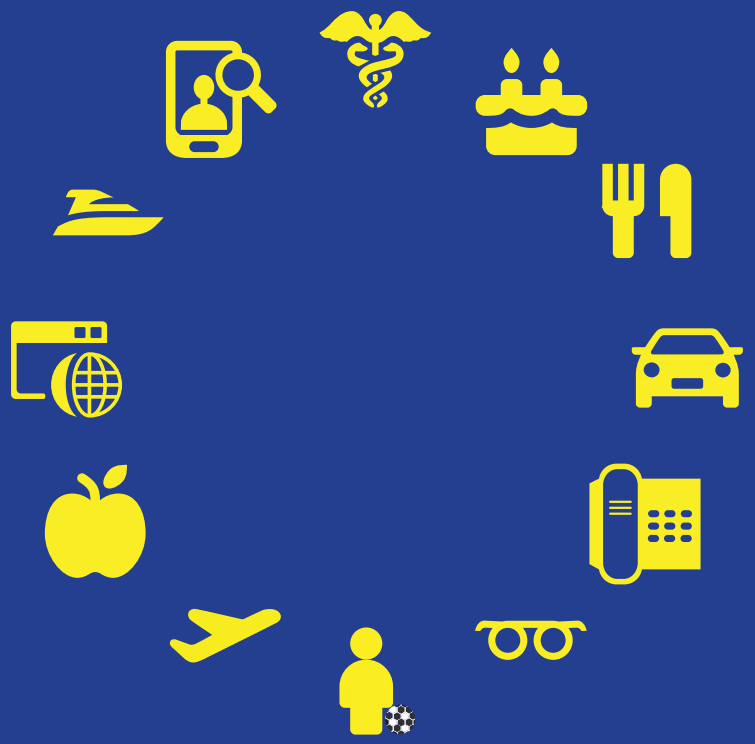


GDPR

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.

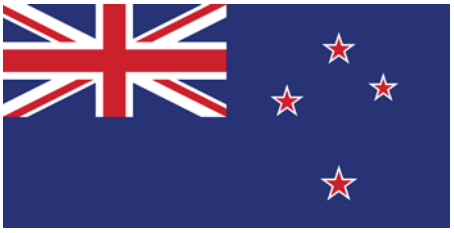
KEY GDPR CHANGES:



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 $9 to $50 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.



AUSTRALIA AND NEW ZEALAND

With the implementation of Australia's Notifiable Data Breach (NDB) scheme early in the year, companies were required to disclose all data breaches to the Office of the Australian Information Commissioner (OAIC), similar in principle to the GDPR. In the first three weeks, 31 data breach reports were received, but by the end of Q2 2018, this number had increased by almost tenfold, reaching 305. Among the incidents reported was that of PageUp, an Australian-based software company which announced that its IT systems were breached in late May, compromising personal data of over 2M customers worldwide.

New Zealand is also in the process of establishing privacy regulations, with the Privacy Act bill introduced to Parliament in March, replacing the Privacy Act of 1993 in order to "promote people's confidence that their personal information is secure and will be treated properly." In the past, companies were not legally required to notify their customers of any data breach activities, or even tell the Privacy Commission. Once again, such change is a reflection of the emerging landscape, which now consists of sophisticated cybercrimes, precious personal information, and glaring vulnerabilities.

NOTIFIABLE DATA BREACHES SCHEME

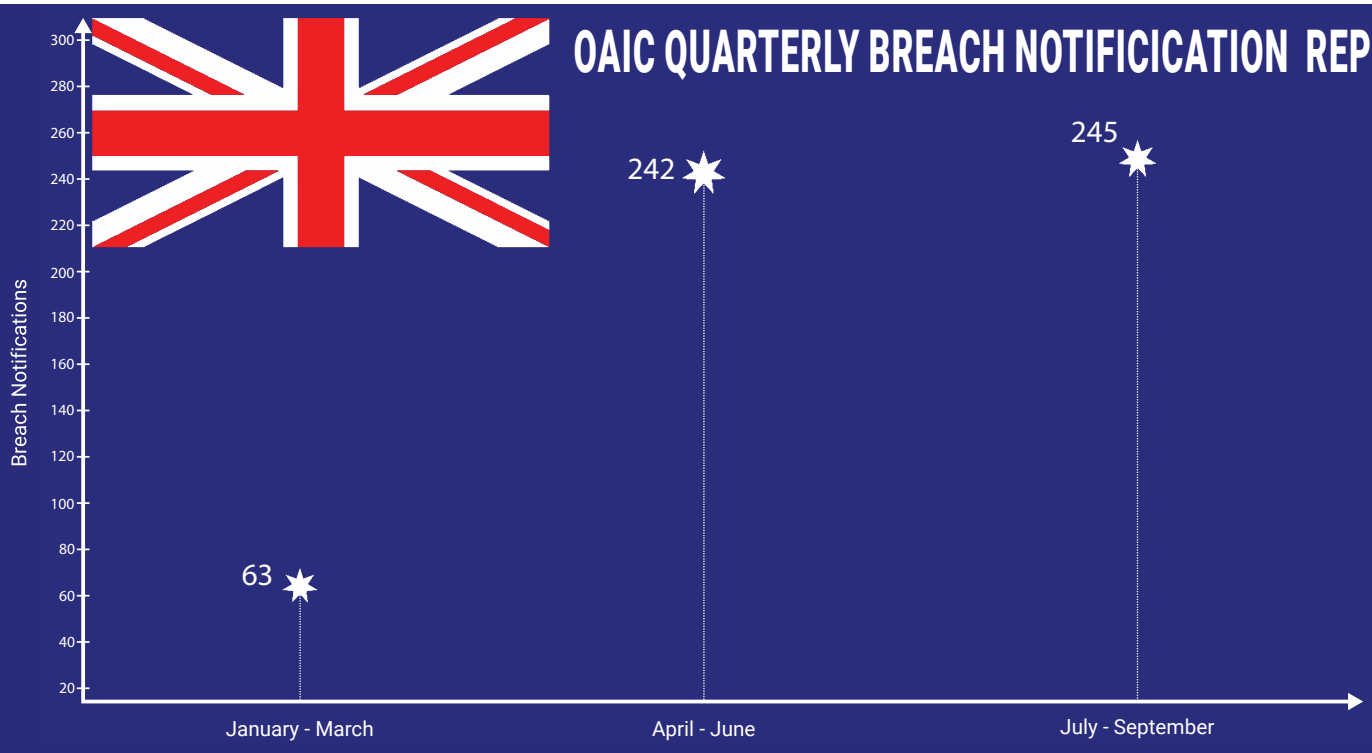
WHO NEEDS TO COMPLY WITH NDB?

- Australian Government agencies
- All businesses and not-for-profit organizations with an annual turnover of $3M or more
- Some small business operators, including:
  - All private sector health service providers;
  - Those that trade in personal information;
  - Tax file number (TFN) recipients (if annual turnover is below $3M, the NDB scheme will apply only in relation to TFN information);
  - Those that hold personal information in relation to certain activities, for example; providing services to the Commonwealth under a contract.

WHAT IS CONSIDERED AN ELIGIBLE BREACH?

- An eligible data breach occurs when three criteria are met:
  - There is unauthorized access to, or unauthorized disclosure of personal information, or a loss of personal information, that an entity holds;
  - This is likely to result in serious harm to one or more individuals;
  - The entity has not been able to prevent the likely risk of serious harm with remedial action.
- 'Serious harm' can be psychological, emotional, physical, reputational, or other forms of harm,
- Understanding whether serious harm is likely or not requires an evaluation of the context of the data breach.

OAIC QUARTERLY BREACH NOTIFICATION REPORT:



CONCLUSION

When we reflect on data breaches in 2018, 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-glitch-idUSKBN1I42JG
- 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-data-breach
- 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-affecting-million-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-breach-response-obligations-effective-november-1-2018/
- https://www.forbes.com/sites/kateoflahertyuk/2018/10/22/this-is-what-the-morrisons-data-leak-class-action-means-for-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-governing-body-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-means-for-future-breaches/#45ce84b92328
- https://www.stuff.co.nz/business/better-business/105264055/mandatory-data-breach-law--what-this-means-for-your-business
- 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-effect-today
- 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