IDC Security Conference

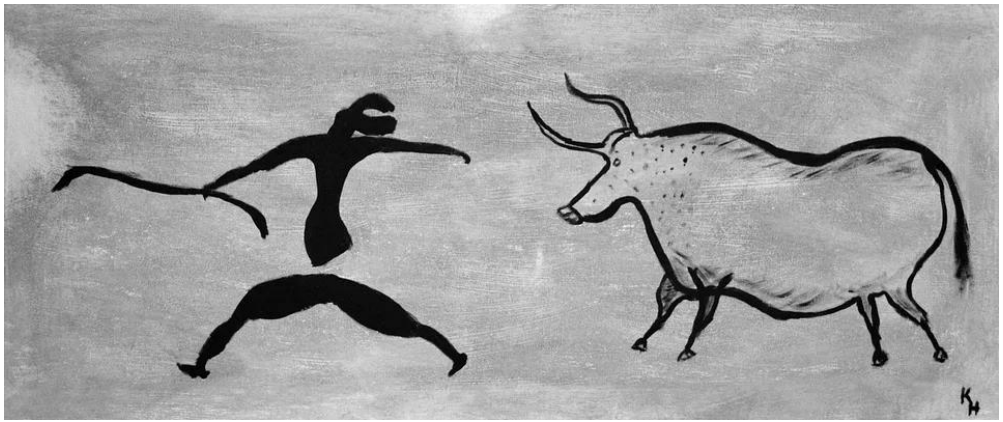
Data breach evolution - is society growing numb to data breaches?

Aldermore

28 April 2020

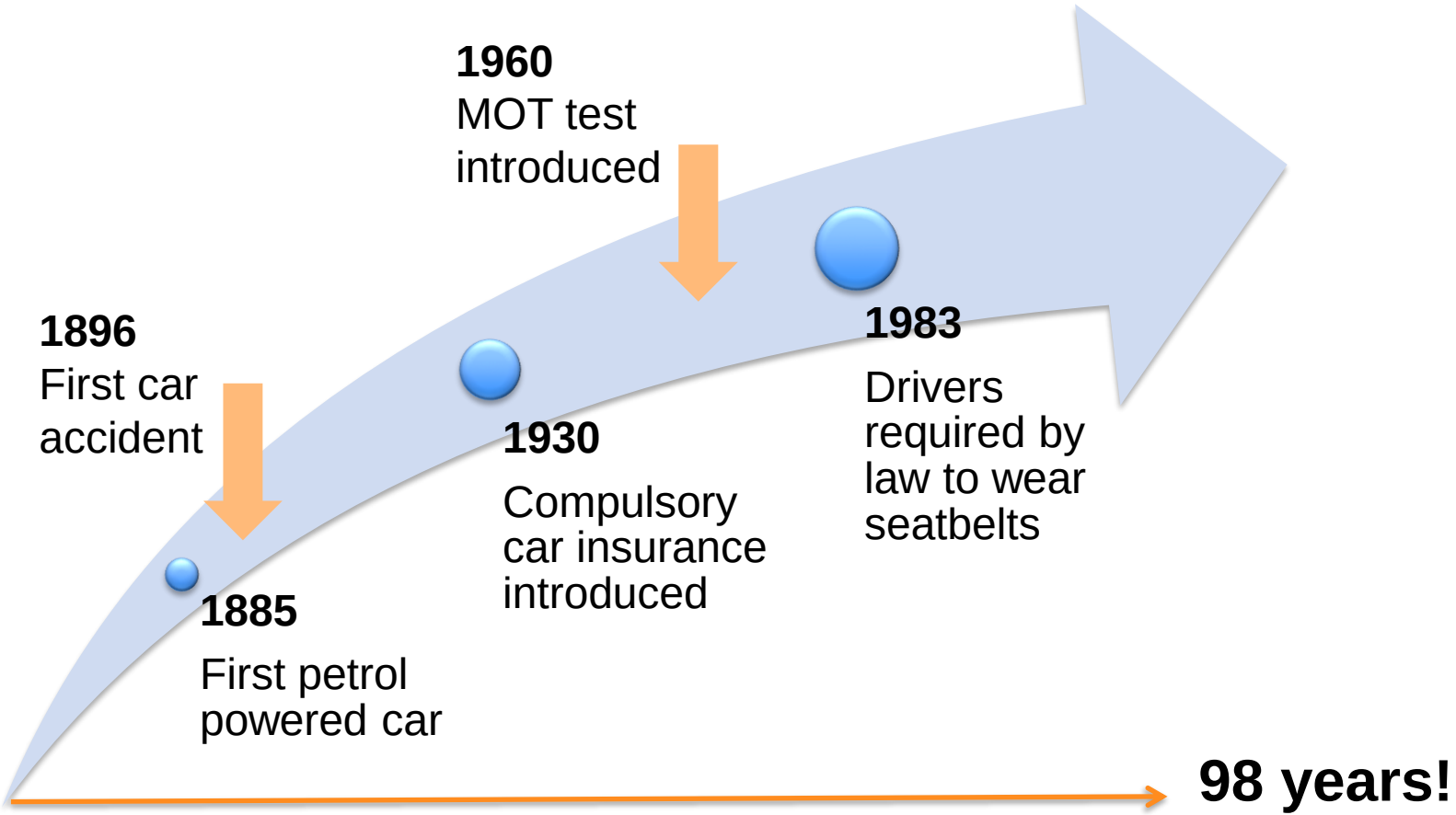
The first (data) breach

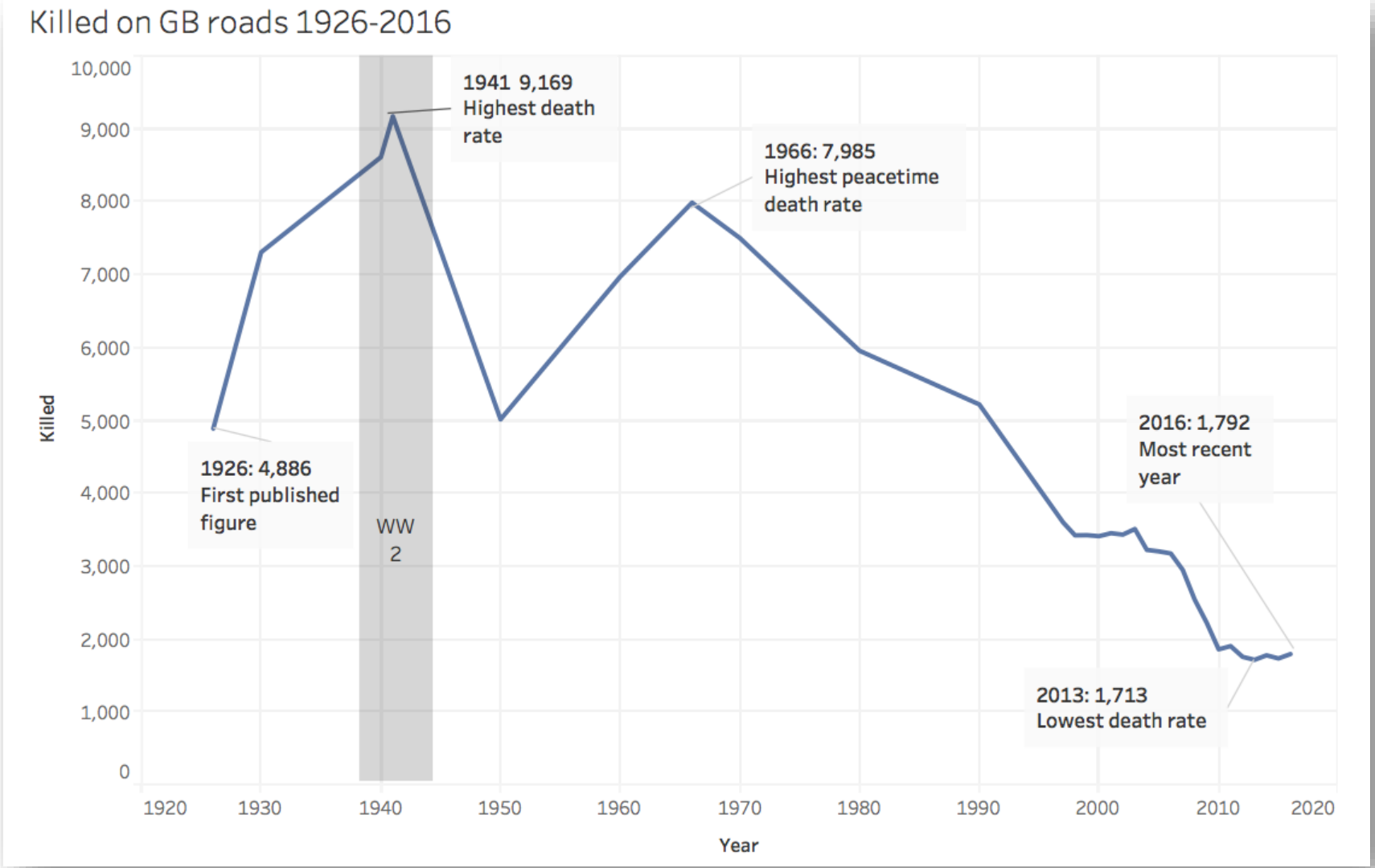
“One early landmark incident occurred in 1984, when the credit reporting agency TRW Information Systems (now Experian) realized that one of its database files had been breached. **The trove was protected by a numeric passcode that someone lifted from an administrative note at a Sears store and posted on an “electronic bulletin board”**—a sort of rudimentary Google Doc that people could access and alter using their landline phone connection. From there, anyone who knew how to view the bulletin board could have used the password to access the data stored in the TRW file: **personal data and credit histories of 90 million Americans**. The password was exposed for a month. At the time, TRW said that it changed the database password as soon as it found out about the situation.”



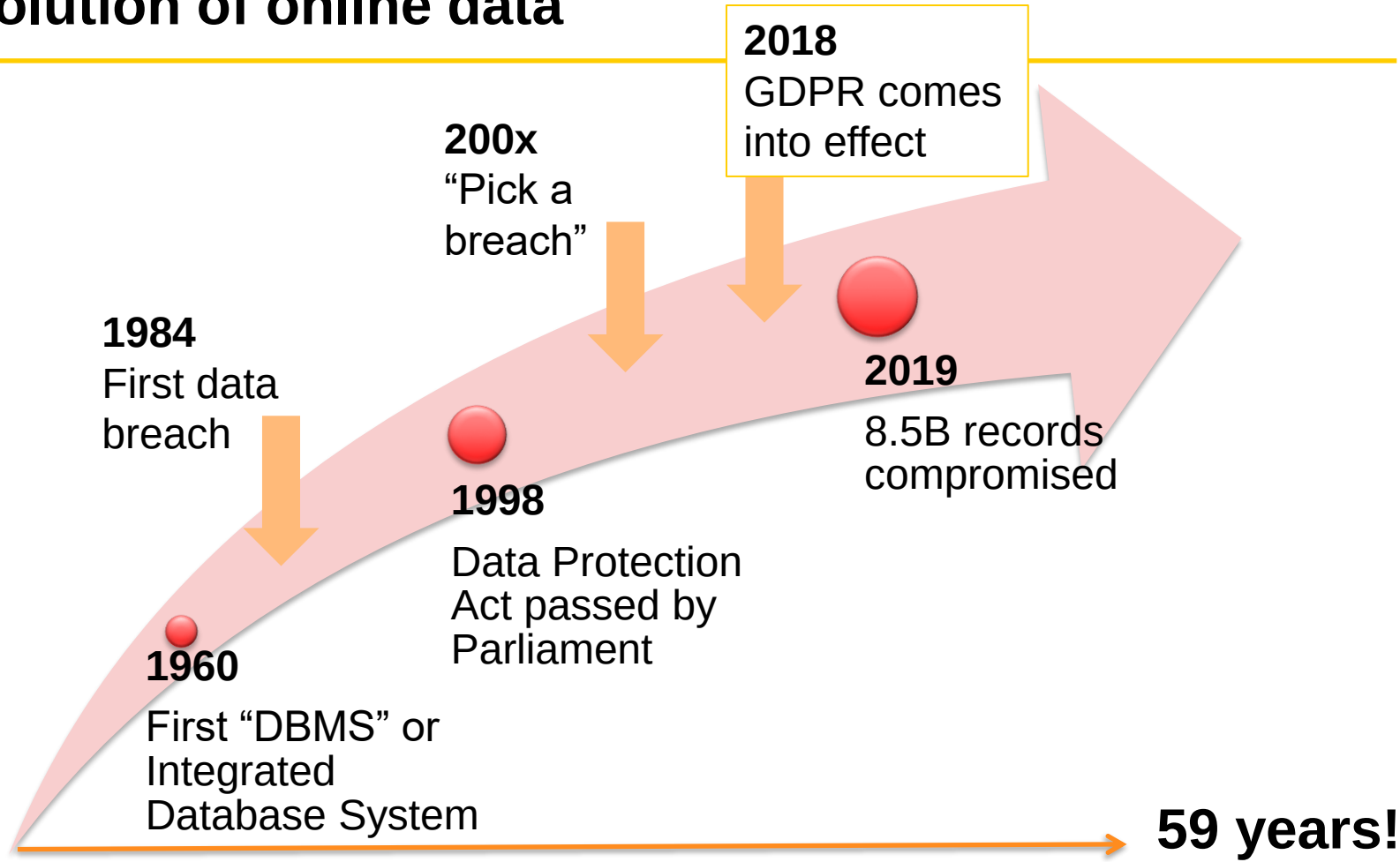
https://www.wired.com/story/wired-guide-to-data-breaches/

The evolution of the automobile

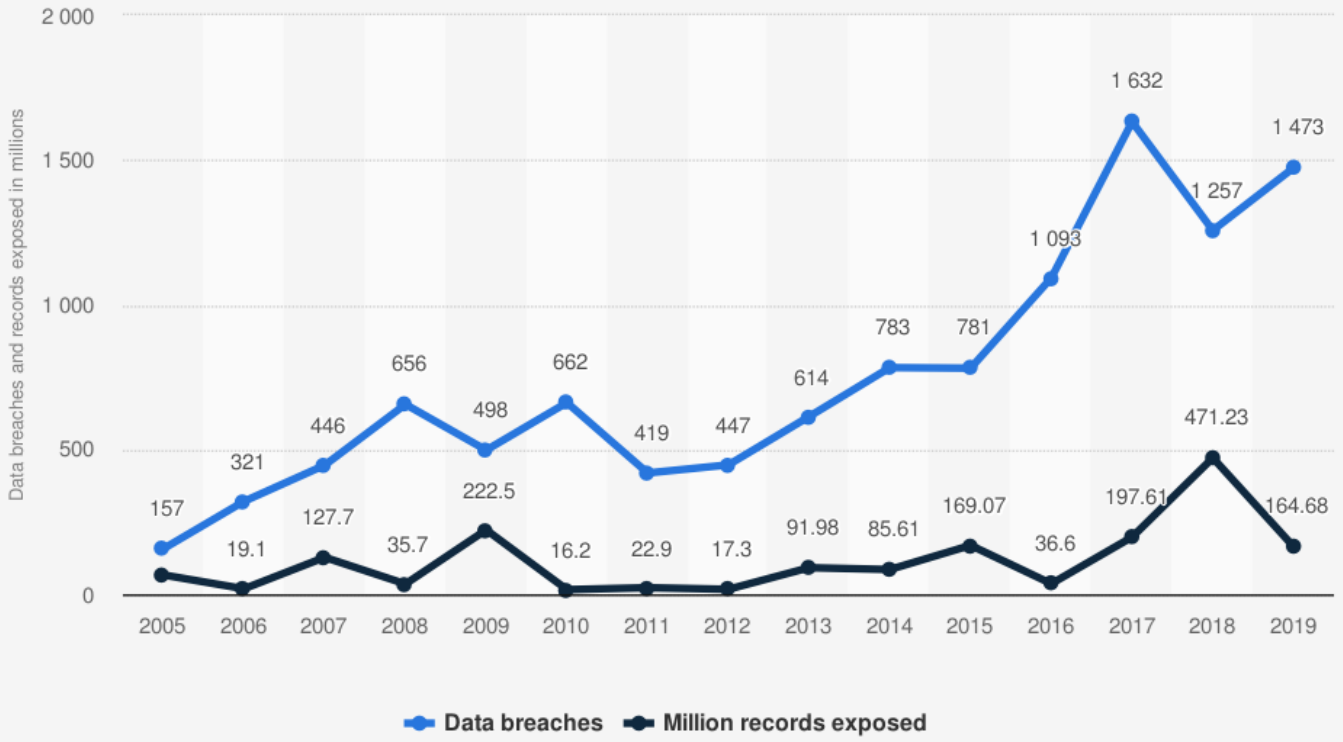



Killed on GB roads 1926-2016
10,000
9,000
8,000
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
Killed
1941 9,169
Highest death rate
1966: 7,985
Highest peacetime death rate
2016: 1,792
Most recent year
1926: 4,886
First published figure
WW 2
2013: 1,713
Lowest death rate
1920
1930
1940
1950
1960
1970
1980
1990
2000
2010
2020
Year

The evolution of online data



Annual number of data breaches and exposed records in the United States from 2005 to 2019 (in millions)



Source
Identity Theft Resource Center

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2019; sensitive records exposed; excluding non-sensitive records

Oh God, not the CLOUD!

Cyber threat: 8.5 bn records compromised in 2019, says IBM

More than 8.5 billion breached records were reported in 2019 with seven billion of them, or over 85 per cent, being due to misconfigured cloud servers and other improperly configured systems, according to a new report from IBM Security.

IANS | February 13, 2020, 08:17 IST

Data breaches are Life

EDITORS' PICK | 5,923 views | Feb 26, 2020, 12:19pm EST

Clearview AI, The Company Whose Database Has Amassed 3 Billion Photos, Hacked

Kate O'Flaherty Senior Contributor ⓘ

Cybersecurity

I'm a cybersecurity journalist.

"Unfortunately, data breaches are part of life in the 21st century,"

		How Many People Affected	Disclosed
1	Aadhaar Breach	1,000,000,000	January 2018
2	Starwood-Marriot Breach	500,000,000	September 2018
3	Exactis Breach	340,000,000	June 2018
4	Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5	Quora Breach	100,000,000	December 2018
6	MyHeritage Breach	92,000,000	June 2018
7	Facebook Breach	87,000,000	September 2018
8	Elasticsearch Breach	82,000,000	November 2018
9	Newegg Breach	50,000,000	September 2018
10	Panera Breach	37,000,000	April 2018

The ICO and fines

ICO fined Cathay Pacific £500,000 for security failures (the maximum it could fine under the old DPA 1998 regime)

The ICO found Cathay Pacific's systems were entered via a server connected to the internet and malware was installed to harvest data.

A catalogue of errors were found during the ICO's investigation including:

- back-up files that were not password protected
- unpatched internet-facing servers
- use of operating systems that were no longer supported by the developer
- inadequate anti-virus protection

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/international-airline-fined-500-000-for-failing-to-secure-its-customers-personal-data/

How are companies still getting breached?

- Database backups not encrypted
- Internet facing server accessible due to a known and publicised vulnerability
- Administrator console publicly accessible from the internet
- Unsupported operating system
- Inadequate or complete lack of server hardening
- Network users permitted to authenticate past the VPN without multi factor authentication
- Inadequate anti-virus system
- Inadequate patch management
- Lack of forensic capability
- Inappropriate account privileges
- Inadequate penetration testing
- Retention period were too long
- Ineffective management of proactive security measures

https://ico.org.uk/media/action-weve-taken/mpns/2617314/cathay-pacific-mpn-20200210.pdf?_sm_nck=1

They knowingly left security tools/controls broken for over a year.

They left plaintext credentials in text files.

The list goes on. They didn't have to "do the basics". If they only did a small PORTION of the basics effectively, they could have prevented or stopped the breach.

Show this thread

Equifax Process and Control Failures

No asset inventory (CSC01
No software inventory (CSC02)
No file integrity monitoring
No network segmentation
Broken SSL Visibility Appliance
Broken SSLV failed open
SSLV lacked certs for key systems
SAST failed to find Struts (user error)
No anomaly detection on web servers
Custom snort rule didn't work
Custom snort rule wasn't tested.
Network scanner didn't find Struts
Failed to detect webshells
Failed to detect interactive activity
File with cleartext creds accessible

16. Additional database access
17. DB queries were not restricted
18. No DB anomaly monitoring
19. No field-level encryption in DBs
20. No data exfiltration detection
21. DAST scanning failed to detect vulns
22. Ineffective IR plan/procedures
23. No owners assigned to apps or DBs
24. Comms issues due to corp structure
25. Lack of accountability in processes
26. Patching process lacked follow up
27. Old audit findings were not addressed
28. Insecure NFS configs
29. Logs retained for less than 30 days

How (not) to clean up after a data breach

“Equifax mishandled its public disclosure and response in the aftermath:

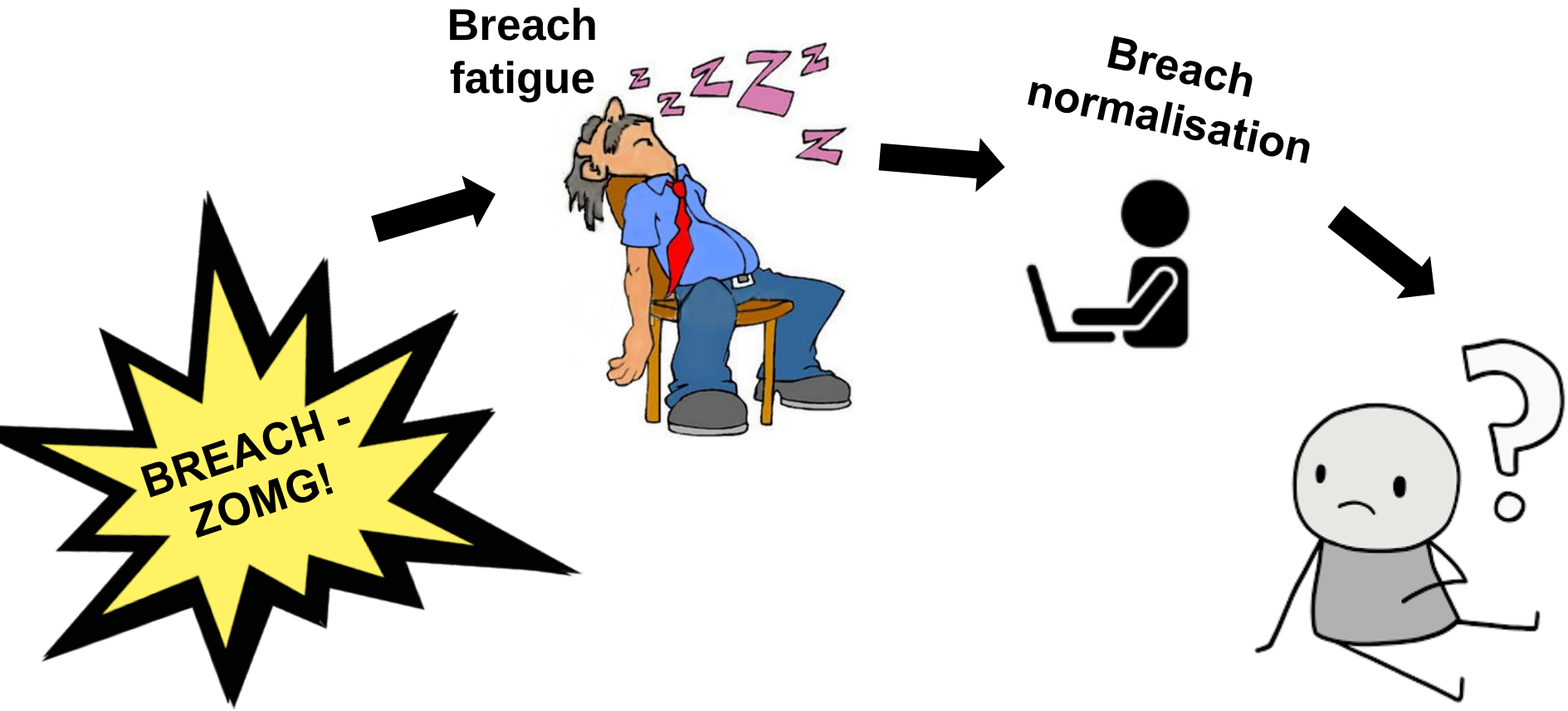
- The site the company set up for victims was itself vulnerable to attack, and it asked for the last six digits of people's Social Security numbers to check if their data had been impacted by the breach.

- Equifax also made the breach-response page a stand-alone site, rather than part of its main corporate domain—a decision that invited imposter sites and aggressive phishing attempts.

- The official Equifax Twitter account even mistakenly tweeted the same phishing link four times. **Four.”**

https://www.wired.com/story/wired-guide-to-data-breaches/

The “New Golden Age” of Computing?



What’s next?

- Demands for more transparency and faster response on security and data privacy concerns
- More regulation for corporations as pressure mounts from end users
- More fines due to GDPR-related findings and reports
- Requirements for “online users” – starting with school-age children

Any questions?

@BeckyPinkard

Aldermore

Read this stat earlier this week: "Data breaches exposed 4.1 billion records in the first half of 2019." varonis.com/blog/cybersecu...

That got me thinking about world population online vs number of credentials breached - what's the breach % total? #EnquiringMinds #Breaches #Passwords

https://twitter.com/BeckyPinkard/status/1208074725714546688?s=20

Enter some furious googling:

"What's the total number of online users 2019?"
"What is the average number of online accounts per user 2019?"

Wait a minute.....

"AVG NUMBER OF PASSWORDS PER USER 2019??"

This got tricky as info was not as current, but a 2018 McAfee report stated "Consumers who responded to the survey have an average of 23 online accounts that require a password, but on avg only use 13 unique passwords for those accounts"

You can see where I'm going with this....

4.39B online users x 23 accounts = 100.97B accounts
4.1B records / 100.97B accounts = 4% of all accounts breached

UNTIL YOU ACCOUNT FOR PASSWORD RE-USE

#ItGetsWorse #ShockHorror #ThatsALotOfAccounts

Accounting for a password re-use component, you decrease the overall number of possible credential pairs:

4.39B online users x 13 avg number of passwords = 57.07B unique passwords

4.1B records / 57.07B unique passwords = 7% of all passwords breached!

#FightMe #MyMathSkillsSuck

To conclude - none of this is scientific (or probably even correct), but it was a fun exercise and despite the huge numbers, hey hopefully there are still roughly 93% of all passwords that haven't been breached (yet)! #Winning

Happy Christmas security peeps!!!

Some links

https://selfkey.org/data-breaches-in-2019/

https://krebsonsecurity.com/category/data-breaches/

https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#6a037729bd54

https://www.lifelock.com/learn-data-breaches-history-of-data-breaches.html

https://privacyrights.org/data-breaches

https://www.wired.com/story/wired-guide-to-data-breaches/

https://blog.avast.com/data-breach-survival-guide