



DATA BREACHES * * * *

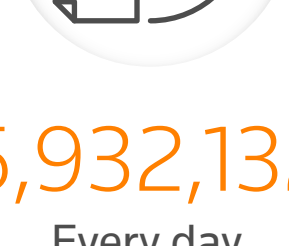
PROTECT YOUR PRIVACY: ENCRYPTION IS ESSENTIAL

14,717,618,286

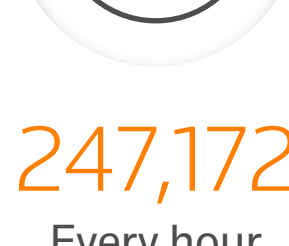
DATA RECORDS LOST OR STOLEN SINCE 2013

Only 4% of breaches were "secure breaches" where encryption was used and the stolen data was rendered useless.

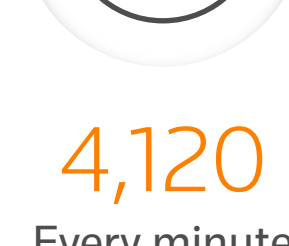
Data records lost or stolen at the following frequency:



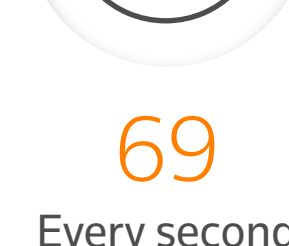
5,932,132
Every day



247,172
Every hour



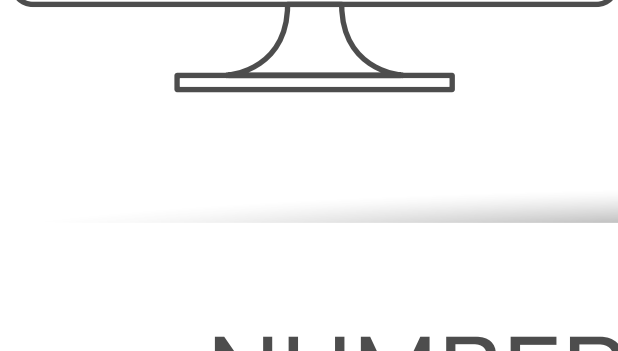
4,120
Every minute



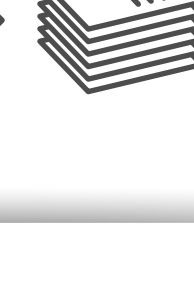
69
Every second

Learn the facts about data privacy and take precautions to ensure your organization isn't the next victim of a malicious attack.

TOP 3 BIGGEST DATA BREACHES OF 2018



1.1 Billion records affected



500 Million records affected



340 Million records affected

NUMBER OF BREACH INCIDENTS BY SOURCE

Although malicious breaches were most common, inadvertent breaches from human error and system glitches were still the root cause for nearly half of all data breaches.

24% Human Error



Costing \$133* per stolen record

25% System Glitch



Costing \$132* per stolen record

51% Malicious or criminal attack



Costing \$166* per stolen record

*Cost to repair breach and recover lost data

Over 90% of known malware infiltrates systems via email



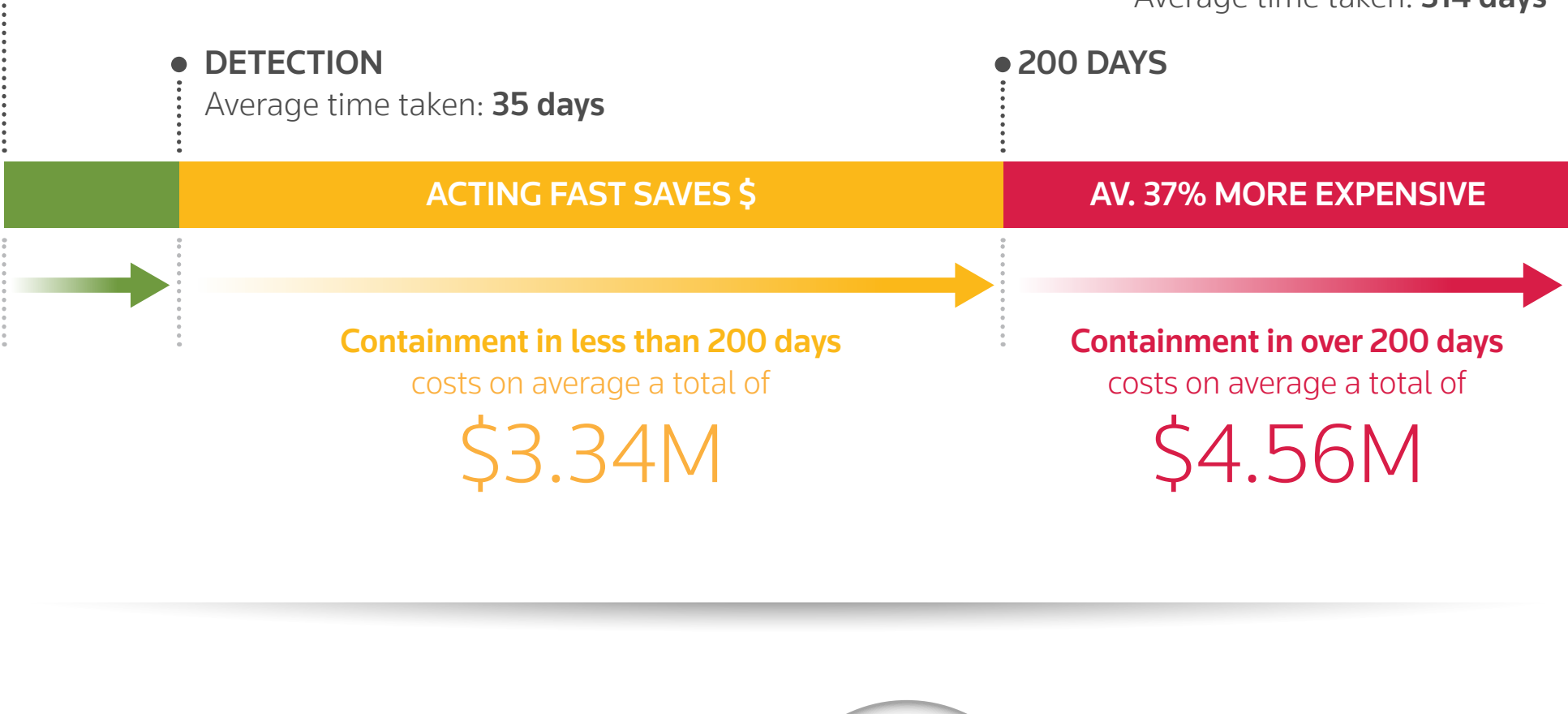
File types:

45% Office Doc

26% Windows App

22% Other

TIMELINE OF A DATA BREACH



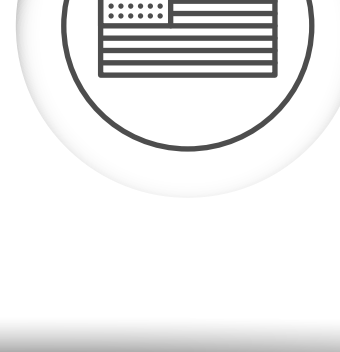
AVERAGE TOTAL COST OF DATA BREACH:

\$3.92M
\$150 per record lost



Most costly industry: **Healthcare**

\$6.45M

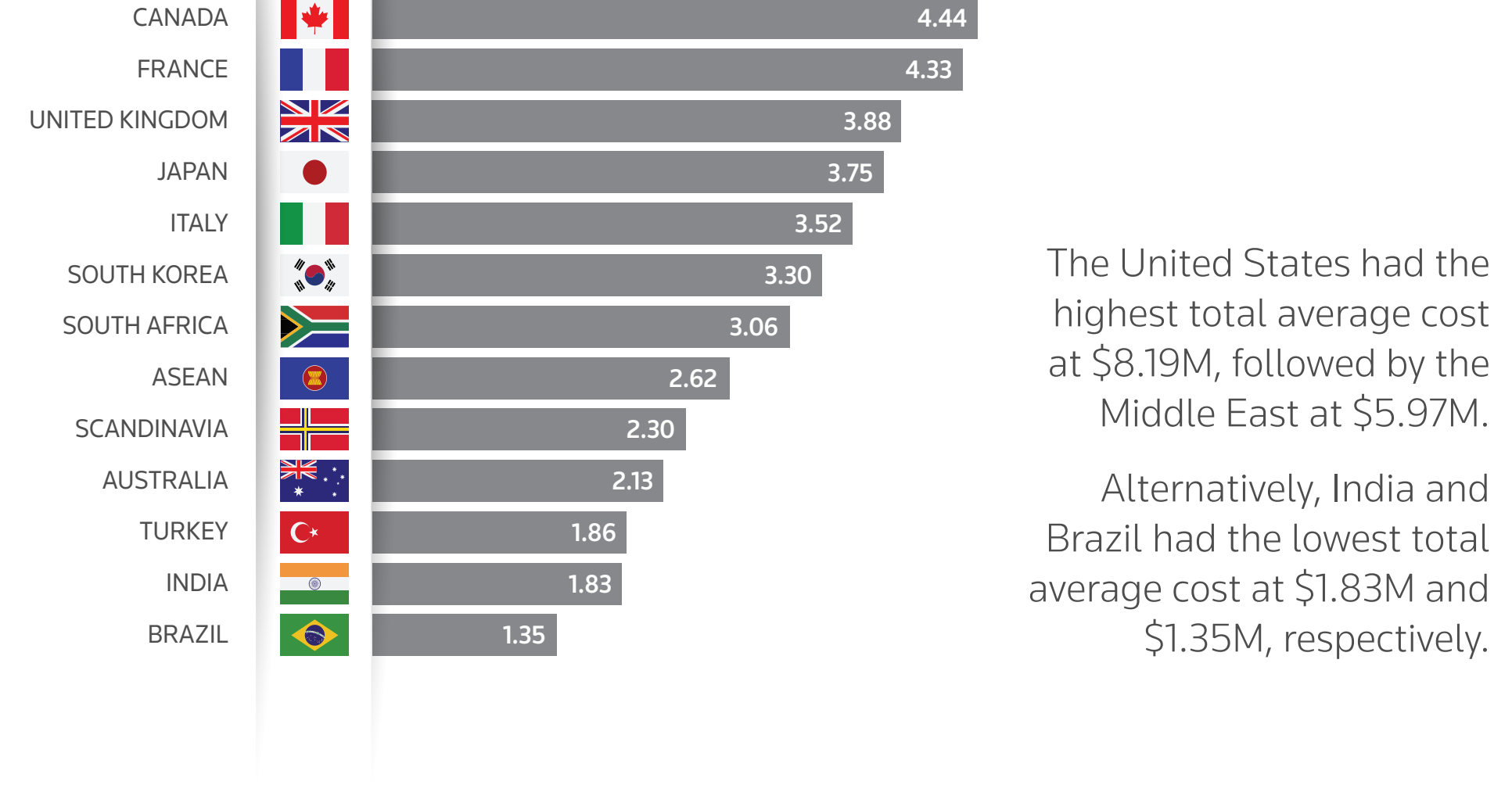


Most expensive country: **The United States**

\$8.19M

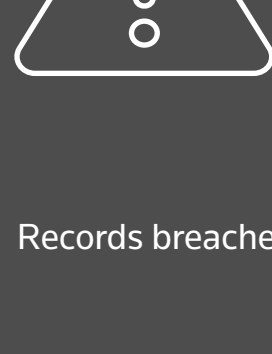
THE AVERAGE TOTAL COST OF A DATA BREACH

by country or region in 2018 (measured in US\$ millions)



COST OF A MEGA BREACH

A mega breach is more than 1 million records lost or stolen.



GDPR

GENERAL DATA PROTECTION REGULATION

Out of the 23 million small businesses in Europe required to comply with the General Data Protection Regulation (GDPR) implemented in 2018, around **half of them are failing GDPR compliance on two crucial requirements.**

The GDPR requires businesses to:

1. Describe data processing activities in clear, plain language to data subjects

2. Identify a lawful basis for using someone's data



Among the 30%...

60% created new policies

15% had extra staff training or communications

11% changed firewall or system configurations

6% created new contingency plans*

*Remaining 8% - Other

27% of businesses had cyber security policies in place

2018



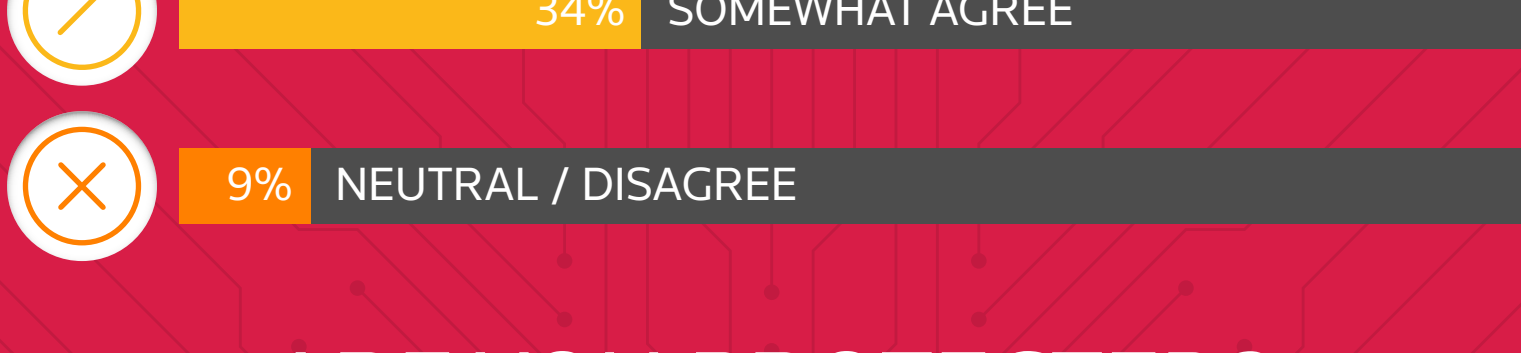
2019

Only 33% of businesses have cyber security policies in place

HOW COMPLIANT ARE YOU?

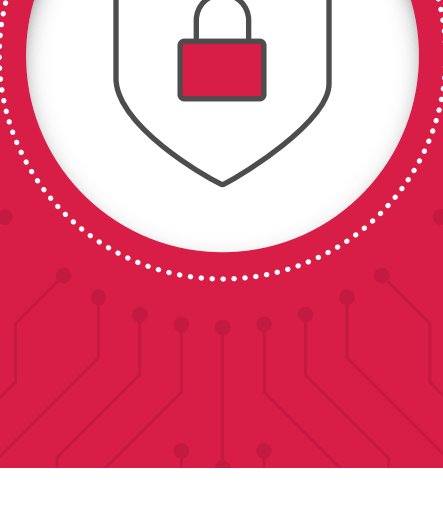
716 small European businesses were asked:

"Does your organization describe its data processing activities in clear, plain language to data subjects?"



ARE YOU PROTECTED?

22% of businesses surveyed said they **do not use technical measures to protect personal data**



Of those who said they did use technical measures, **encryption was the measure mentioned most often**



TOP TIPS

Here are some ways you and your company can strengthen your data privacy:



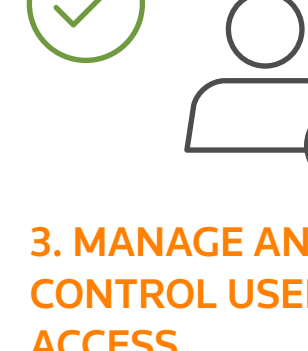
1. ENCRYPT YOUR SENSITIVE DATA

Locate your sensitive data and encrypt it. Whether your data resides on-premises, in virtual environments, the cloud or is in motion, encryption will render it useless to attackers.



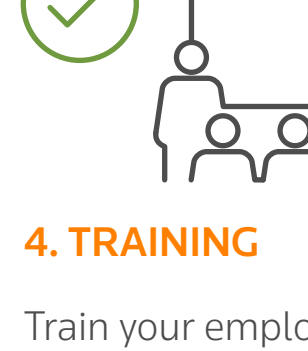
2. SECURE AND OWN YOUR ENCRYPTION KEYS

Store encryption keys securely and separately from encrypted data. By centrally managing the key lifecycle, you ensure you maintain ownership and control of your data at all times.



3. CONTROL AND MANAGE USER ACCESS

Manage and control access to your corporate resources and apps by verifying a user's identity, assessing and applying the right access policy, and enforcing the appropriate access controls using single sign on.



4. TRAINING

Train your employees and management to ensure they are knowledgeable of various laws and regulations. **Thomson Reuters Compliance Learning courses provide interactive online training to ensure your company stays compliant.**

Build your culture of compliance With Thomson Reuters Compliance learning

Learn more

SOURCES
 1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf
 2. https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#2-marriott-starwood-hotels-500-million-20
 3. https://databreachcalculator.myibm.com/
 4. https://gdpr.eu/2019-small-business-survey/
 5. https://www.ibm.com/downloads/cas/ZBZLYKX
 6. https://securethebreach.com/

