SCRAMFS
ENCRYPTED FILE SYSTEM

Worldwide Data Breach Dossier

A selection of this decade's data breaches, lessons learnt and opportunities for improvement.

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Document v1.02 22nd Feb 2018

This is a worldwide epidemic

Who is affected?

- Two-thirds of Americans (198m)
  - Names, dates of birth, home addresses, phone numbers, and voter registration

- Half of Filipinos (55m)
  - Names, physical address, place of birth, height, weight, gender, marital status and parents' names, email addresses, passport numbers & expiry dates, fingerprint records (15.8m),

- Half of South Africans (30m)
  - Names, full identity numbers, income, gender, employment history, phone numbers, home addresses

- Reflects a sorry state of I.T. security. As an industry, we have failed to adequately secure people's data.

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Trying to understand the problem

Common data breaches grouped by category

Cloud leaking: exposing data by mistake

"Leaving the front door open"

Republican National Committee voter data (198m voters) from S3 bucket

Australian Broadcasting Corporation (1800 database backups, TV programs) from S3 bucket

Chicago voter data (1.8m voters) from backup files in S3 bucket

Accenture (137+GB of data, database dumps, 40,000 plaintext passwords) from S3 bucket

Australian Red Cross Blood Bank leak (550,000 donors) from database backup on web server

South African citizen data leak (55m citizens) from database backup on public web server

Verizon customer data (14m customers) from compressed text files in S3 bucket

Stewart Airport, NY, leak (emails, government files, password list) from backups exposed to Internet

Hacking: exploiting technical vulnerabilities

"Breaking down the front door"

Philippines data breach (55m voters) incl. fingerprint data. (Unknown hack)

iCloud hacking / celebrity photos (brute force password guessing)

TalkTalk customer data (SQL injection)

Gartner: 80% to 95% of cloud security failures to 2020 will be the customer's fault, not the cloud provider's.

IBM: From 2013-2017, 9 billion records were breached, but only 4% of them were encrypted.

References: https://twitter.com/nmacdona/status/668853313690030080 | https://www.gartner.com/newsroom/id/3143718 | http://ibmsystemsmag.com/mainframe/trends/security/enterprise-encryption/

Physical theft or loss

Lloyd's Bank – missing storage device

Zurich Insurance Plc – lost tape backup

Nationwide Building Society – stolen laptop

London Heathrow Airport – lost USB key

Malware

Forever 21 (POS malware)

Eddie Bauer (POS malware)

Exfiltration: insider job

Panama papers

Paradise papers

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Lessons learnt

- Leaks are often caused by poor data handling procedures by both the organisation collecting the data, and by 3rd party contractors.
- Everyone is affected, no-one is immune:
  - **Corporates / large business** (Accenture, TalkTalk, Verizon),
  - **Banks** (Lloyds),
  - **SMEs** (Forever 21, Panama & paradise papers),
  - **Non-profits** (Red Cross Blood Bank),
  - **Political parties** (RNC),
  - **Governments** (South Africa, Philippines)
  - **Individuals** (celebrities)

Lessons learnt

- Encryption was not used to secure data in the previous examples, but if properly implemented, could have prevented most breaches:

Cloud leaks	Breach entirely preventable with client-side encryption.
Hacking	For cloud credential compromise, breach entirely preventable with client-side encryption. More active hacking attacks can be slowed down when encryption is combined with pseudonymisation and intelligent cryptographic key controls.
Physical theft	Breach entirely preventable with client-side encryption.
Malware	When securely integrated, client-side encryption will prevent most malware from stealing data.
Exfiltration	More difficult to prevent, but when integrated into a Data Loss Prevention system, client-side encryption can help limit the breach or trigger alerts.

- By using client-side encryption, there is substantial room to improve the security of data.

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Lessons learnt

- Systems need to be engineered for security by design & default.
  - I.T. administrators should integrate encryption into data handling processes for automatic security.
    - All secondary copies of data (backups, archives, migrations, transfers) should be encrypted.
    - Client-side encryption should be used for cloud data and local (on-premise) data.
  - Software developers should integrate encryption into systems where possible.
    - Sensitive information (e.g. biometrics, health, financial) should be encrypted and stored in encrypted storage, separate to the main database.
    - Pseudonymisation should be used to link the main database with encrypted storage.

Recent Data Breaches

from around the world...

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD

Republican National Committee

USA – June 2017

Leaked GOP Data On 198 Million Americans Wasn't Even Protected By A Password

It's been revealed that a conservative analytics company left a massive amount of information on American voters exposed and it could've been downloaded by anyone who stumbled across it.

Human error. Data leaked from CSV files in a misconfigured S3 bucket.

- America's largest breach (to date)
- 198 Million American voters affected
- 1.1 TB of information
- Names, dates of birth, home addresses, phone numbers, and voter registration details leaked
- Data leaked by data analytics firm, Deep Root Analytics, a 3rd party data analytics firm.

Source: https://www.forbes.com/sites/leemathews/2017/06/19/gop-firm-leaked-info-200-million-americans/

Australian Broadcasting Corporation

Australia – November 2017

ABC Commercial data leak, including database backups, found by Ukrainian firm

PM By Tom Joyner

Updated 17 Nov 2017, 4:29pm

A Ukrainian cybersecurity firm has discovered an unsecured cache of ABC Commercial files, which it says includes two years of database backups, email addresses and hashed passwords.

The files were found by cybersecurity firm Kromtech on an incorrectly configured internet service.

The company initially attempted to alert the ABC of the data breach on Wednesday.

Kromtech head of communications Bob Diachenko said the firm found the publicly accessible data by

PHOTO: The data was stored in a widely-used online repository service run by internet giant Amazon, called Amazon S3. (ABC News)

Human error. Misconfigured Amazon S3 bucket.

- 1800 daily database backups
- Names, emails and hashed passwords of ABC employees.
- Customer names, commercial correspondence, internal system credentials, network diagrams

Source: http://www.abc.net.au/news/2017-11-17/abc-data-leaked-online-discovered-by-ukrainian-firm/9159022

Chicago Voter Data

USA · IL – August 2017

1.8 million Chicago voter records exposed online

Selena Larson

A voting machine company exposed 1.8 million Chicago voter records after misconfiguring a security setting on the server that stored them.

Election Systems & Software (ES&S), the Nebraska-based voting software and election management company, confirmed the leak on Thursday.

In a blog post, the company said the voter data leak contained names, addresses, birthdates, partial social security numbers and some driver's license and state ID numbers stored in backup files on a server. Authorities alerted ES&S to the leak on Aug. 12, and the data was secured.

Human error. Misconfigured Amazon S3 bucket.

- 1.8 million Chicago voters affected
- Names, addresses, birth dates, partial SSNs, driver's license, state ID numbers, stored in backup files
- Caused by 3rd party contractor, a voting software and election management company from Nebraska

Source: http://money.cnn.com/2017/08/17/technology/business/chicago-voter-records-exposed-upguard/index.html

Accenture

Global – September 2017

Accenture left a huge trove of highly sensitive data on exposed servers

The four exposed servers had no password, but contained the "keys to the kingdom."

By Zack Whittaker for Zero Day | October 10, 2017 -- 13:00 GMT (00:00 AEDT) |

Topic: Security

Human error. Four misconfigured Amazon S3 buckets.

- Highly sensitive and commercial data about Accenture Cloud Platform, its workings and clients.
- Accenture internal access keys and credentials, master encryption key in Amazon's Key Management Service. Credentials for Accenture Google & Azure accounts, Zenoss logs.
- Credentials of Accenture clients, 40,000 plaintext passwords.

Source: http://money.cnn.com/2017/08/17/technology/business/chicago-voter-records-exposed-upguard/index.html

Australian Red Cross Blood Bank

Australia - October 2016

Red Cross Blood Service admits to personal data breach affecting half a million donors

Updated 28 Oct 2016, 5:41pm

The personal data of 550,000 blood donors that includes information about "at-risk sexual behaviour" has been leaked from the Red Cross Blood Service in what has been described as Australia's largest security breach.

The organisation said it was told on Wednesday that a file containing donor information was placed on an "insecure computer environment" and "accessed by an unauthorised person".

The file contained the information of blood donors from between 2010 and 2016.

PHOTO: The file contained the information of blood donors from between 2010 and 2016. (ABC Adelaide: Brett Williamson)

Human error. Data leaked from database backup put on public web server.

- Australia's largest breach (to date)
- 550,000 blood donors affected
- Names, addresses, date of birth, gender and details of "at risk sexual behaviour" leaked
- Database backup accidentally posted to publicly facing website by 3rd party contractor. File was not encrypted.

Source: http://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036

South African Citizen Data Leak

South Africa - October 2017

Millions caught in South Africa's 'worst data breach'

By Pumza Fihlani
BBC News, Johannesburg

20 October 2017 Share

Data leaked from database backup put on public web server.

- South Africa's largest breach (to date), over 30 million affected.
- Names, full identity numbers, income, gender, employment history, phone numbers, home addresses leaked.
- 27GB database backup file posted to publicly facing website by a real estate company. File was not encrypted.

Source: http://www.bbc.com/news/world-africa-41696703

Verizon Customer Data

USA - October 2017

Millions of Verizon customer records exposed in security lapse

Customer records for at least 14 million subscribers, including phone numbers and account PINs, were exposed.

By Zack Whittaker for Zero Day | July 12, 2017 -- 13:00 GMT (23:00 AEST) | Topic: Security

An Israeli technology company has exposed millions of Verizon customer records, ZDNet has learned.

As many as 14 million records of subscribers who called the phone giant's customer services in the past six months were found on an unprotected Amazon S3 storage server controlled by an employee of Nice Systems, a Ra'anana, Israel-based company.

Data leaked from text files in misconfigured Amazon S3 bucket.

- 14 million Verizon customers affected. Data in log files from 6 months of customer service calls.
- Customer names, home address, email addresses, cell numbers and account PINs, account balance and customer frustration score leaked.
- Data leaked by 3rd party contractor based in Israel, paid to analyze customer service interactions.

Source: http://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/

Stewart International Airport

USA · NY – February 2017

Security lapse exposed New York airport's critical servers for a year

Exclusive: The files included gigabytes of emails, sensitive government files, and a password list, which researchers say could give hackers "full access" to the airport's systems.

By Zack Whittaker for Zero Day | February 24, 2017 -- 13:00 GMT (00:00 AEDT) |

Topic: Security

Human error. Misconfigured NAS device.

- Backup drive images of servers sent to on-site NAS device.
- NAS device was configured to act as cloud storage, open to the world.
- 760GB of data leaked, including TSA letters of investigation, employee SSNs, network passwords, and 107GB of emails.
- Encryption was not used.

Source: http://www.zdnet.com/article/unsecured-servers-at-new-york-airport-left-exposed-for-a-year/

Philippines Voter Data

The Philippines – March 2016

When a nation is hacked: Understanding the ginormous Philippines data breach

14 APRIL 2016

Remember when OPM got breached last year? There was a lot of excitement in various parts of the world (namely the US) because here we had a government department (Office of Personnel Management), *and they'd just lost 21.5 million records!* These records included such sensitive data as names, dates of birth and addresses and by any reasonable measure, it was serious – that's almost 7% of the country's population!

Hacking attack.

- The Philippine's largest breach (to date)
- 55 Million Filippino voters affected
- 76GB of compressed data, including a MySQL database backup
- Email addresses, passport numbers & expiry dates, fingerprint records, physical address, place of birth, height, weight, gender, marital status and parents' names
- How data was obtained is unclear

Source: https://www.troyhunt.com/when-nation-is-hacked-understanding/

iCloud leaks
USA – August 2014

iCloud leaks of celebrity photos

From Wikipedia, the free encyclopedia

On August 31, 2014, a collection of almost 500 private pictures of various celebrities, mostly women, and with many containing nudity, were posted on the imageboard 4chan, and later disseminated by other users on websites and social networks such as Imgur and Reddit. The images were initially believed to have been obtained via a breach of Apple's cloud services suite iCloud,[1][2][3] but it later turned out that the hackers could have taken advantage of a security issue in the iCloud API which allowed them to make unlimited attempts at guessing victims' passwords.[4][5] However access was later revealed to have been gained via targeted phishing attacks.[6][7]

Hacking attack.

- A vulnerability in the iCloud API, allowing unlimited brute-force attempts at guessing passwords without lockout.
- Concurrently, targeted attacks on victims via phishing methods allowed hackers to break into iCloud accounts and access data
- Photos were download from iCloud accounts and shared publicly.

Source: https://en.wikipedia.org/wiki/ICloud_leaks_of_celebrity_photos

TalkTalk data breach

UK – October 2015

News › Business › Business News

TalkTalk given record fine over data breach that led to data theft of nearly 157,000 customers

The personal data of 156,959 customers including names, addresses, dates of birth, phone numbers were stolen

Zlata Rodionova | Wednesday 5 October 2016 13:00 BST | 3 comments

42 shares

Like Click to follow The Independent Online

Hacking attack.

- A SQL injection vulnerability .
- 157,000 customers affected
- Names, addresses, phone numbers, bank account details, birth dates leaked
- Company publicly admitted encryption was not used to secure private data.
- £400,000 fine issued by the UK ICO

Source: http://www.independent.co.uk/news/business/news/talktalk-fine-data-breach-theft-customers-information-stolen-record-penalty-a7346316.html

SCRAMFS
ENCRYPTED FILE SYSTEM

Fight the data breach epidemic through world-class encryption.

Easy to implement: simple interfaces for system administrators, software developers, and general users.

Versatile: protects a wide range of data, both on premise and in the cloud, via client-side encryption

Trustworthy: designed & peer-reviewed by leading cryptographers from around the world; designed for long-term security

SCRAM SOFTWARE
SECURING YOUR DATA IN THE CLOUD