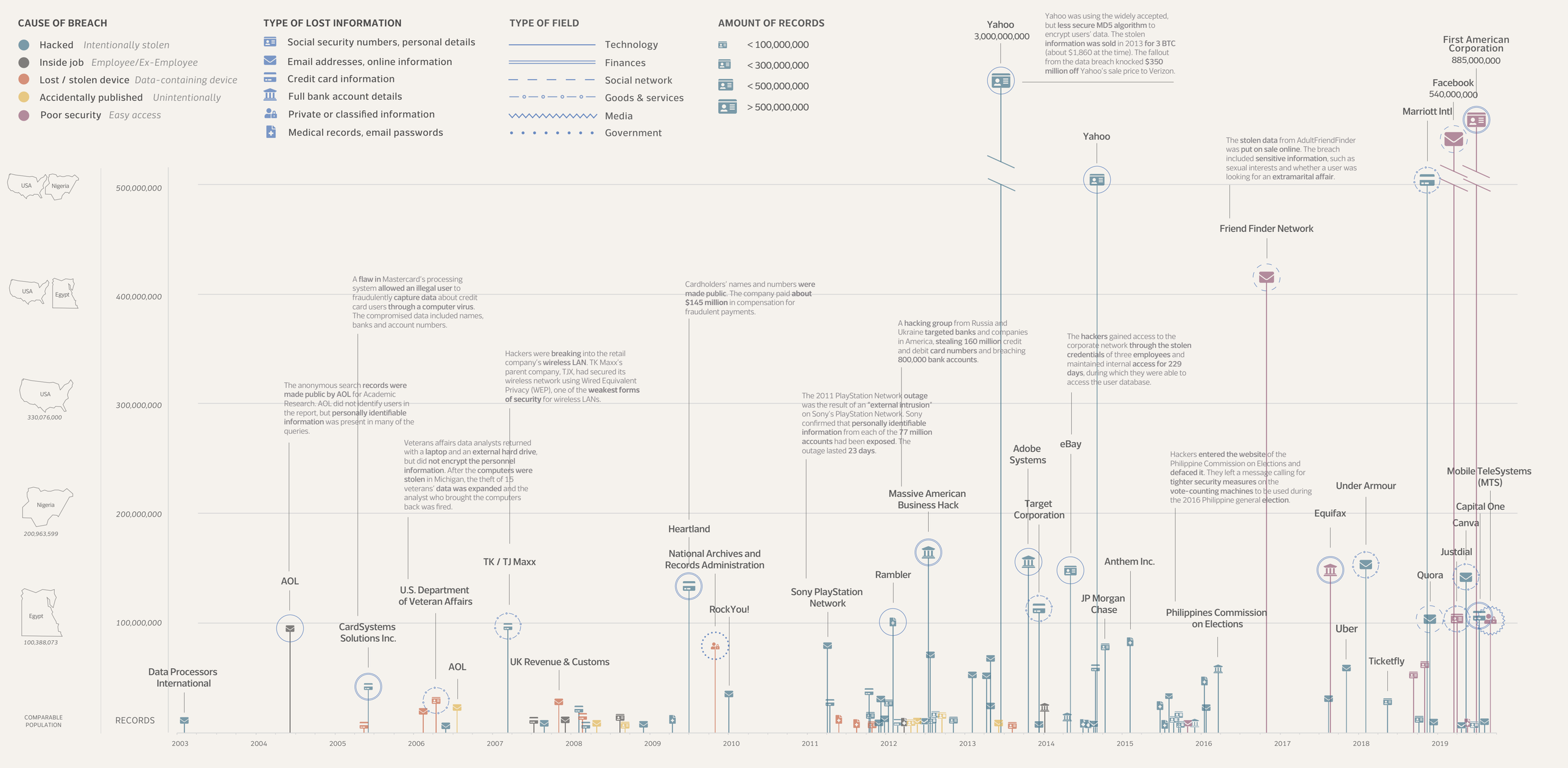
CAUSE OF BREACH
Hacked Intentionally stolen
Inside job Employee/Ex-Employee
Lost / stolen device Data-containing device
Accidentally published Unintentionally
Poor security Easy access
TYPE OF LOST INFORMATION
Social security numbers, personal details
Email addresses, online information
Credit card information
Full bank account details
Private or classified information
Medical records, email passwords
TYPE OF FIELD
Technology
Finances
Social network
Goods & services
Media
Government
AMOUNT OF RECORDS
< 100,000,000
< 300,000,000
< 500,000,000
> 500,000,000
USA
Nigeria
USA
Egypt
USA
330,076,000
Nigeria
200,963,599
Egypt
100,388,073
COMPARABLE POPULATION
500,000,000
400,000,000
300,000,000
200,000,000
100,000,000
RECORDS
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
Yahoo
3,000,000,000
Yahoo was using the widely accepted, but less secure MD5 algorithm to encrypt users' data. The stolen information was sold in 2013 for 3 BTC (about $1,860 at the time). The fallout from the data breach knocked $350 million off Yahoo's sale price to Verizon.
Yahoo
First American Corporation
885,000,000
Facebook
540,000,000
Marriott Intl
The stolen data from AdultFriendFinder was put on sale online. The breach included sensitive information, such as sexual interests and whether a user was looking for an extramarital affair.
Friend Finder Network
A flaw in Mastercard's processing system allowed an illegal user to fraudulently capture data about credit card users through a computer virus. The compromised data included names, banks and account numbers.
Cardholders' names and numbers were made public. The company paid about $145 million in compensation for fraudulent payments.
A hacking group from Russia and Ukraine targeted banks and companies in America, stealing 160 million credit and debit card numbers and breaching 800,000 bank accounts.
The hackers gained access to the corporate network through the stolen credentials of three employees and maintained internal access for 229 days, during which they were able to access the user database.
The anonymous search records were made public by AOL for Academic Research. AOL did not identify users in the report, but personally identifiable information was present in many of the queries.
Hackers were breaking into the retail company's wireless LAN. TK Maxx's parent company, TJX, had secured its wireless network using Wired Equivalent Privacy (WEP), one of the weakest forms of security for wireless LANs.
Veterans affairs data analysts returned with a laptop and an external hard drive, but did not encrypt the personnel information. After the computers were stolen in Michigan, the theft of 15 veterans' data was expanded and the analyst who brought the computers back was fired.
The 2011 PlayStation Network outage was the result of an "external intrusion" on Sony's PlayStation Network. Sony confirmed that personally identifiable information from each of the 77 million accounts had been exposed. The outage lasted 23 days.
Hackers entered the website of the Philippine Commission on Elections and defaced it. They left a message calling for tighter security measures on the vote-counting machines to be used during the 2016 Philippine general election.
Data Processors International
AOL
CardSystems Solutions Inc.
U.S. Department of Veteran Affairs
AOL
TK / TJ Maxx
UK Revenue & Customs
Heartland
National Archives and Records Administration
RockYou!
Sony PlayStation Network
Rambler
Massive American Business Hack
Adobe Systems
Target Corporation
eBay
Anthem Inc.
JP Morgan Chase
Philippines Commission on Elections
Equifax
Under Armour
Uber
Ticketfly
Quora
Justdial
Canva
Capital One
Mobile TeleSystems (MTS)