CAMBRIDGE CITY COUNCIL

Craig A. Kelley
City Councillor

To: Donna Lopez, City Clerk

From: Craig A. Kelley, City Councillor

Date: June 21, 2018

Subject: Memorandum Submission

Please place the attached memorandum, "Cybersecurity: An Overview", on the City Council agenda as "Communications and reports from Other City Officials" for the June 25, 2018 meeting.

Thank you.

CAMBRIDGE CITY COUNCIL

Craig A. Kelley
City Councillor

MEMORANDUM

To: Cambridge City Council

From: Craig A. Kelley, City Councillor
Mark Gutierrez, Council Aide

Date: June 25, 2018

Subject: Cybersecurity: An Overview

---

1. Introduction

Cybersecurity is no longer just an IT problem. Common threats like data theft, extortion, and vandalism are increasing and diversifying through evolving hacking software that allows more sophisticated attacks including disruption of infrastructure, disinformation, market manipulation, and espionage.[1] The U.S. Department of Homeland Security recognizes "As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend."[2]

Cyberspace is the field of non-physical information storage and transmission, their networks, and the tangibles they rely on. Cybersecurity is the protections and overall security of cyberspace.[3] It's easy to think of cyberspace as strictly digital, considering the popularity of "the cloud," digital devices, and WiFi, but the digital world is astonishingly physical. Physical attributes include cables, data centers, and a half-million miles of transcontinental submarine fiber optics lining the ocean floor, reaching as deep as Mount Everest is high. These cables and centers are subject to cybersecurity risks, as displayed by espionage and wiretapping during the Cold War, and are not immune from these and other threats.

2. Cyberattacks: A Closer Look

Cambridge, MA

March 2018. Population: 110,000. The Cambridge Health Alliance announced that a data breach revealed the private information of 2,500 patients. The leaked data was acquired from billing records and landed in the hands of an unauthorized third party.[4]

Atlanta, GA

April 2018. Population: 472,000. The city battled a ransomware malware attack that severely affected multiple departments causing disruptions with the court system, prevented people from paying bills and submitting important requests, and forcing the police department to resort to pen and paper to file reports. The sophistication of this strain of malware, called SamSam, and the lack of preparedness from the city is what made this attack so successful.[5] Atlanta was held hostage for a ransom of $52,000, but has allegedly denied payment and has since spent $2.6M on recovery efforts.[6]

Sarasota, FL

February 2016. Population: 56,000. A city employee clicked on an email attachment, appearing to be a regular document, only to launch a ransomware attack encrypting 160,000 files. Attackers demanded $33M in bitcoin to restore the files. The IT department had to unplug the city's servers before beginning the recovery process.[7]

Cockrell Hill, TX

December 2016. Population: 4,000. A ransomware attack encrypted all of the digital files that the police department had. The city refused to pay the $4,000 ransom, so the attackers deleted all of the department's records, dating back to 2009.[7]

911 Call Centers

Attacks on 42 911 call centers have been reported in which hackers disabled computer and dispatch systems and immobilized phone lines with bogus calls, leading to service shutdowns and even a child's death.[8]

U.S. Power Grid & Energy Infrastructure

Russian hackers gained access to energy and critical infrastructure sectors including nuclear generators, power plants, water facilities, aviation, and manufacturing facilities. The DHS and FBI said the computer systems and internal networks of multiple companies across the U.S. were infiltrated. The Kremlin hacking campaign used old and unsophisticated hacking techniques, and once in the systems, installed programs to surveil and collect information.[9]

Significant Cyber Incidents

The Center for Strategic and International Studies documented all significant cyber incidents since 2006. A significant incident is considered "cyber-attacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars."[10] They've counted 324 incidents from 2006 through April 2018, with a majority of them happening in the last 4 years. Attacks include the hacking of several state voter registries, an Uber breach, and North Korea's testing of U.S. electric companies' defense systems.

The biggest data breaches (greater than 30,000 records) from 2004 through 2017 were compiled into an interactive visualization illustrating the radical increase in both sensitivity of data and number of breaches over time (Attachment A). Attacks and breaches occurred globally against law enforcement agencies, defense and military arms, transportation networks, banks, universities, hospitals, financial institutions, scores of private sector companies, and even the Massachusetts State government.[11]

Privacy Rights Clearinghouse reports more than 10.5B records have been breached globally since 2005.[12] The Identity Theft Resource Center and CyberScout report over 1B exposed records from more than 8,000 breaches in the U.S. alone (Figure 1).[13]

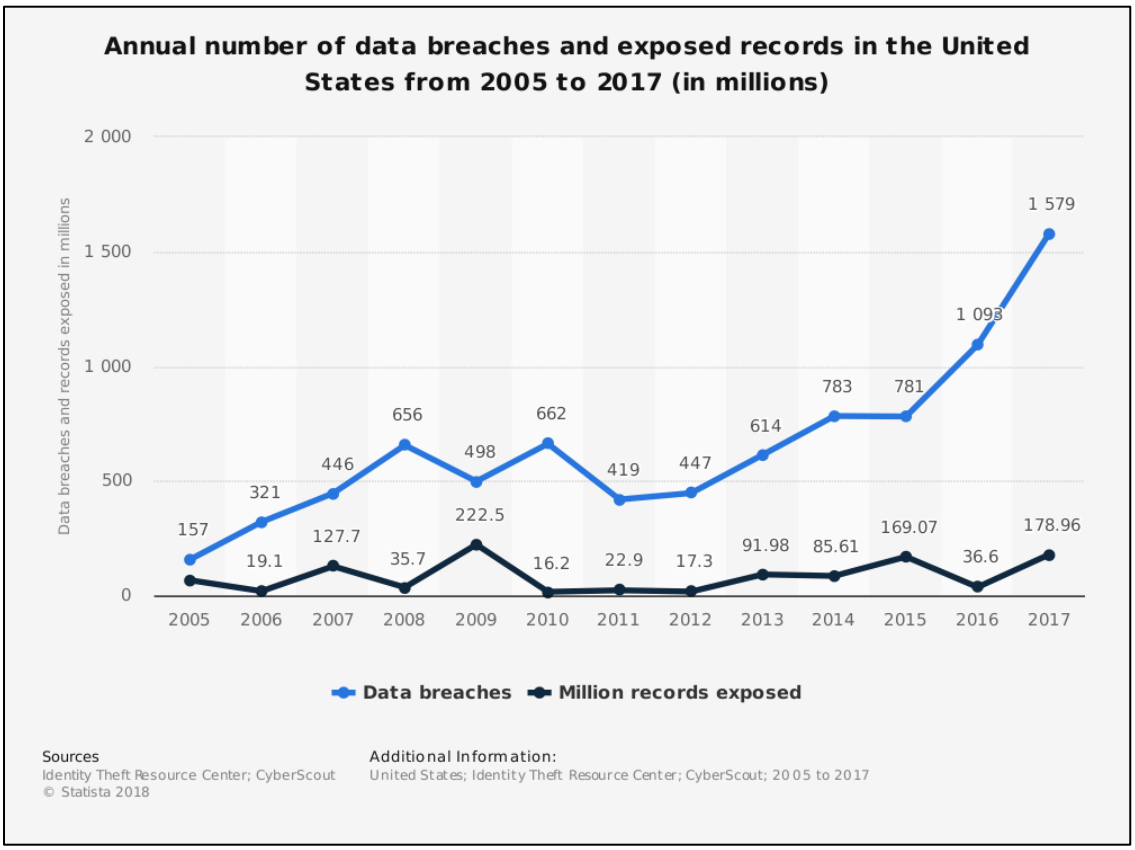


Figure 1

3. The Rapid Growth of Data and Cyber Threats

Global Data

In 2011, global data volume was just shy of 2 zettabytes (or 2 trillion gigabytes).[14] In 2016, that number reached 16ZB. The International Data Corporation (IDC) released a new report predicting that in 2025, the total volume will reach 163ZB to support critical infrastructure, medical devices, autonomous vehicles, smart devices, business and government operations, and artificial intelligence, to name a few.[15] That amount of data would fill 40 trillion DVDs, reaching to the moon and back 100 million times. Much of this data growth will be in the life-critical and enterprise sectors, and it's expected that the average "connected" person will interact with a connected device 4,800 times per day.[16] In 2021, 1 million minutes of video content will cross the network every second to support things like surveillance and consumer entertainment.[17]

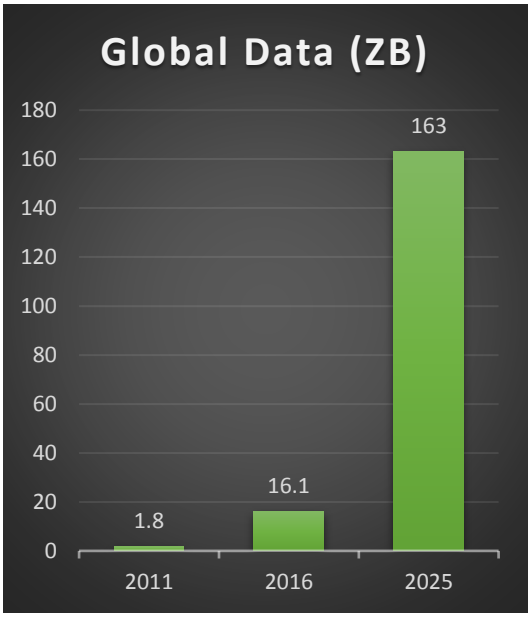


Figure 2: Global Data Growth

Cyber Threats and Vulnerabilities

Heimdal Securities identified and explained a complete list of all 52 types of cyberattacks, in 8 categories, carried out by 3 types of attackers. A spear phishing attack led to the hacking of the Democratic National Committee. Spyware can sit undetected on multiple computers and collect data to report back to the attackers, and ransomware can hijack computer networks and demand payment for the release of associated data.[18] Privileged Escalation Attacks get a 'beach head' into a system via a personal computer and all of these attacks beg the questions "What are you afraid of?" and "What is your threat model?"

Many of these attacks are highly calibrated and executed with military precision by talented individuals who know how to hide their identity and hit hard. Attackers look for soft targets and often governments offer a perfect target due to:[19]

- A lack of synchronization across critical systems and third parties.
- High quality and quantity of data.
- Difficulty in attracting high-demand cybersecurity professionals.
- Governments don't typically look at cyberspace as an enterprise-wide risk like the private sector does.
- Governments relegate the cybersecurity responsibility to under-funded and under-equipped IT departments and vendors.
- A cultural willingness not to ask, "Did this email really come from that person."

4. Resiliency & Proactive Measures

Three months before Atlanta was hit, the city failed a security compliance assessment[20] that could have prevented the attack and saved them millions of dollars. Security is a process, not a product[21] and with a sharp increase in use and dependency on technology in an ever-evolving digital world, being proactive is a prerequisite for resiliency. Cybersecurity is also a national security issue. FEMA aides in emergency and disaster situations and fire departments protect people and property from damage. Arguably, the Department of Homeland Security and state agencies should bear the responsibility of protecting cyberspace, in addition to municipal efforts.[22]

Bad cybersecurity itself is self-reinforcing as it is easy to think that since a cyberbreach has not occurred yet, the security is adequate. Given the crippling impact of cyberbreaches, it is hard to take this issue too seriously. Nonetheless, it is easy to get mired in jurisdictional issues as cyberevents can stretch across municipal, regional, state and international boundaries. Even something as seemingly mundane as participants interacting on Nextdoor.com, for example, is often done via out-of-state servers. The lack of clear jurisdiction can confuse responsibility(ies) for enforcement and reaction.

There is always a trade-off between user convenience and security and also between security and budgets. Additionally, user access can present challenges in that some users may have access to parts of a system or network for which they have responsibility, but no need for access, and this excess access increases the risk of a cyberbreach. While cyberbreaches such as defacing a website are reputational in nature and pose less operational danger to a government, any system that deals with sensitive personal data or finances requires absolute protection. This protection must extend to third-party vendors, to include how a government keeps its interactions with vendors such as credit card companies secure. Attention must also be paid to how shared portals with other organizations, such as the Cambridge Health Alliance or even the School Department, might increase vulnerabilities.

Some protective measures like site blocking can lead to operational challenges as city staff may need to research issues on sites that are "blocked." Municipal employees should have appropriate expectations of how secure their data and computer usage is. This should include when using the city's Wi-Fi on their phones, using apps and so forth. People should understand that anonymity, or the lack thereof, is a different issue from censorship.

Agencies in Action[7]

- Washington State offers free cybersecurity audits to over a dozen municipalities. Washington pays for the tests through a voter-approved initiative that allows the state auditor to appropriate millions of dollars for performance audits like cybersecurity.
- Michigan formed a squad of stand-by volunteers, the Michigan Cyber Civilian Corps (MiC3), to provide technical assistance if the state gets hit with a crippling cyberattack in any of its 1,300 local governments.

- Michigan also launched a pilot program with five local governments to test whether a chief information security officer (CISO) can operate as a shared service. The idea is to have a certified, trained, cyber-professional to assist local governments lacking the expertise that more resourceful agencies may have.
- Sugar Land, Texas has its first CISO to confront cybersecurity issues. He's a cybersecurity expert that serves as part of IT.

Recommendations

- Cambridge's IT Strategic Plan is 5 years out of date and does not address cybersecurity. A review and update of this policy to reflect current technology trends, city business needs, and proactive cybersecurity measures is essential.[21]
- Identify if the City has an information security policy and a disaster recovery/business continuity plan. If the City does not have them, they should be created and implemented, if the City does have them, they should be reviewed for currency and a process should be developed to ensure they are continuously updated.[21] As with a hurricane or other, more familiar type of disaster, we need to have a relevant recovery plan prior to the event.
- Conduct an assessment, penetration test, audit, or other review to lower the City's risk profile, to include equipment, testing and training. Identify the crucial security vulnerabilities and low-hanging fruit.[22] This will not be cheap.
    - What must happen now?
    - What can wait?
    - What are long-term plans for upgrades, hiring, etc?
    - Are access levels appropriately curtailed?
- Develop a disaster recovery plan in case computers or communication systems become unusable.[22]
- Consider obtaining cyber breach insurance to defray the cost of any potential cyber disaster.[22]
- Research state resources and other municipalities with similar goals and determine if joint training, purchasing or other efforts could help with cybersecurity.
- Research non-governmental resources such as the Kennedy School's Defending Digital Democracy Project, offering a playbook for cybersecurity.[21]
- Consider splitting cybersecurity responsibilities from general IT responsibilities. There are no City positions with cybersecurity in their title, which does not mean cybersecurity is being ignored, but is competing with other important responsibilities.[21]
- Clarify and make public CPD's cybercrime unit's responsibilities and capabilities.
- Create a Chief Cybersecurity Officer position or clearly identify a current position with that responsibility for the City as a whole and within relevant departments.[22]
- Review training—specialized training for those in the IT/cybersecurity fields, and general training for staff.[22] Some training is already done but given the risk that users pose to the systems they use, a review and probable expansion of cybersecurity training for all

involved. People need to understand that cybersecurity is *their* problem too.

- Consider having the 2020 fiscal year budget specifically identify cybersecurity resources.[21]

References

[1] https://www.forbes.com/sites/edelmantechnology/2017/10/11/cyber-security-is-a-business-risk-not-just-an-it-problem/#53763acf7832
[2] https://www.dhs.gov/cybersecurity-overview
[3] https://blogs.cisco.com/security/cyberspace-what-is-it
[4] https://www.bostonglobe.com/metro/2018/03/30/cambridge-health-alliance-says-some-its-patients-data-was-compromised/7skcaSVG9GbYaFNSTpWLtN/story.html
[5] https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/
[6] https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/
[7] http://www.govtech.com/security/GT-OctoberNovember-2017-Small-Towns-Confront-Big-Cyber-Risks.html
[8] https://www.nbcnews.com/news/us-news/hackers-have-taken-down-dozens-911-centers-why-it-so-n862206
[9] https://www.vox.com/world/2018/3/28/17170612/russia-hacking-us-power-grid-nuclear-plants
[10] https://csis-prod.s3.amazonaws.com/s3fs-public/180425_Significant_Cyber_Events_List.pdf?pqetcWcwV7mvAo33_lAZFlQVQz7.E0qh
[11] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
[12] https://www.privacyrights.org/data-breaches
[13] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
[14] https://www.zdnet.com/article/data-volume-to-hit-1-8zb-in-2011/
[15] https://www.seagate.com/our-story/data-age-2025/
[16] https://www.seagate.com/files/www-content/our-story/trends/files/data-age-2025-infographic-2017.pdf
[17] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html#_Toc484556829
[18] https://heimdalsecurity.com/blog/cyber-attack/
[19] https://www.forbes.com/sites/dantedisparte/2018/04/02/cities-held-for-ransom-lessons-from-atlantas-cyber-extortion/#385685725996
[20] https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/
[21] Tannenbaum, Saul. 2018/06/08. Cybersecurity meeting.
[22] Berman, Seth. 2018/06/08. Cybersecurity meeting.

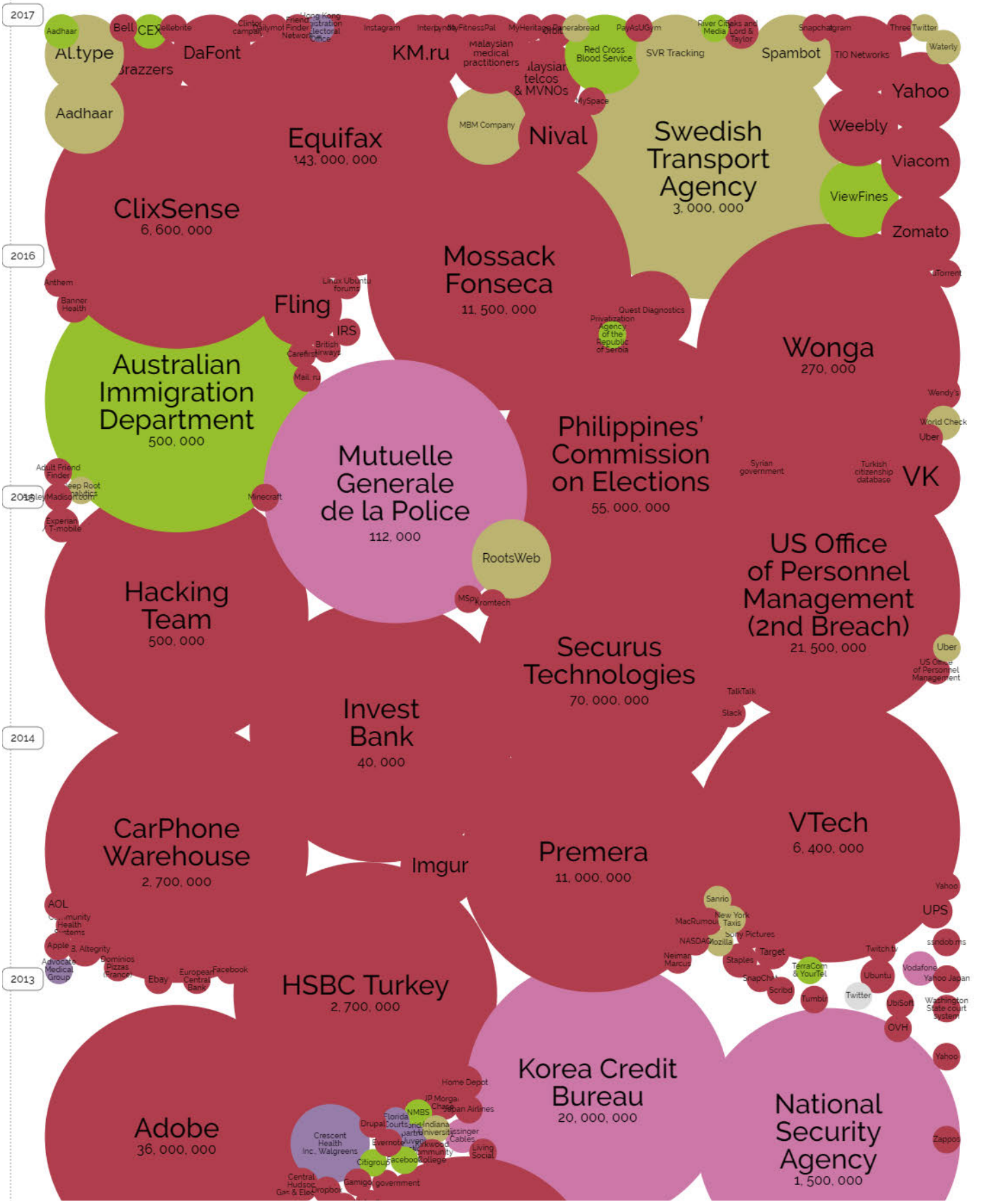
Figure 1- https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
Figure 2- Gutierrez, Mark. 2018/06/14.

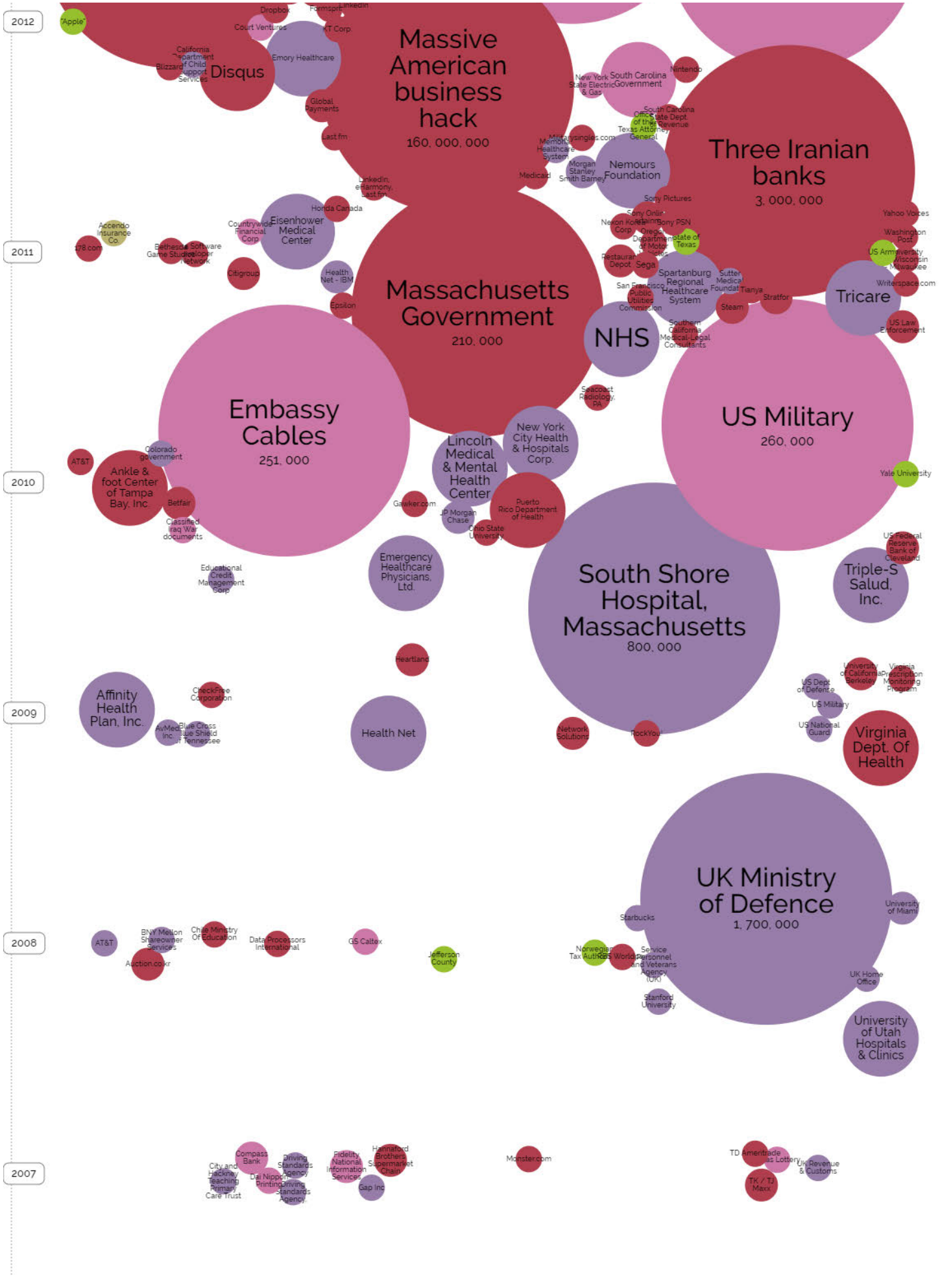
World's Biggest Data Breaches

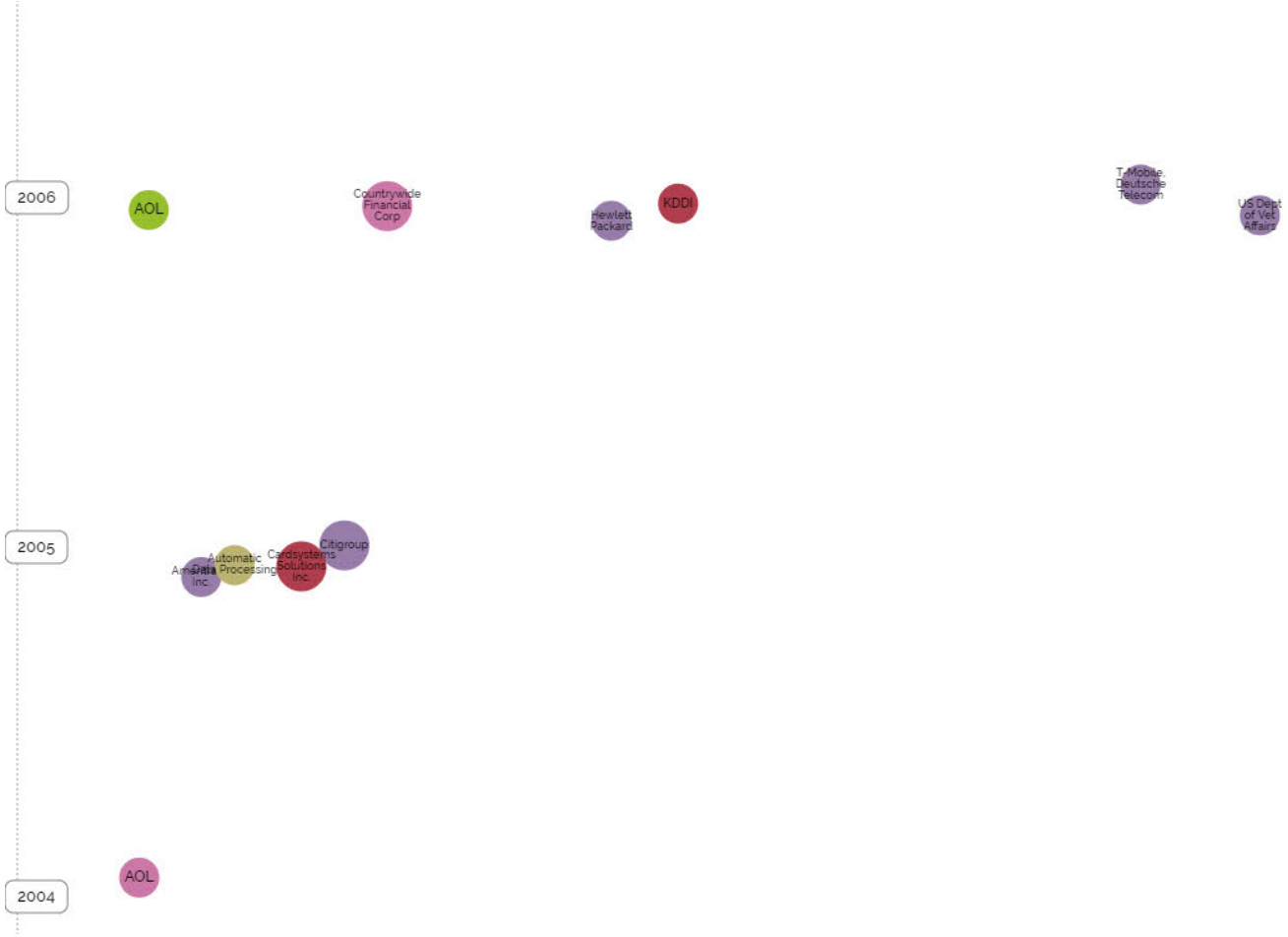
Selected losses greater than 30,000 records

(updated 8th May 2018)

YEAR | *BUBBLE COLOUR* YEAR | METHOD OF LEAK | *BUBBLE SIZE* NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER




2012
2011
2010
2009
2008
2007
"Apple"
Dropbox
Foxmsprs
LinkedIn
Court Ventures
KT Corp.
Disqus
Emory Healthcare
Massive American business hack
160, 000, 000
Global Payments
Last.fm
LinkedIn, eHarmony, Last.fm
Honda Canada
Eisenhower Medical Center
Countrywide Financial Corp
Accendo Insurance Co.
178.com
Bethesda Game Studios
Software Modder Network
Citigroup
Health Net - IBM
Epsilon
Massachusetts Government
210, 000
Embassy Cables
251, 000
AT&T
Colorado government
Ankle & foot Center of Tampa Bay, Inc.
Betfair
Classified Iraq War documents
Educational Credit Management Corp
Emergency Healthcare Physicians, Ltd.
Gawker.com
JP Morgan Chase
Ohio State University
Puerto Rico Department of Health
Lincoln Medical & Mental Health Center
New York City Health & Hospitals Corp.
Heartland
Affinity Health Plan, Inc.
CheckFree Corporation
AvMed Inc.
Blue Cross Blue Shield of Tennessee
Health Net
Network Solutions
RockYou
South Shore Hospital, Massachusetts
800, 000
NHS
Seacoast Radiology, PA
Three Iranian banks
3, 000, 000
New York State Electric & Gas
South Carolina Government
Nintendo
South Carolina Office of State Dept. Revenue
Office of the Texas Attorney General
Memorial Healthcare System
Medicaid
Morgan Stanley Smith Barney
Nemours Foundation
Sony Pictures
Sony Online Entertainment
Nexon Korea Corp
Sony PSN
Oregon Department of Motor Vehicles
State of Texas
Restaurant Depot
Sega
Spartanburg Regional Healthcare System
Sutter Medical Foundation
Tianya
San Francisco Public Utilities Commission
Steam
Stratfor
Southern California Medical-Legal Consultants
US Military
260, 000
Yale University
Tricare
Yahoo Voices
Washington Post
US Army
University of Wisconsin Milwaukee
Writerspace.com
US Law Enforcement
US Federal Reserve Bank of Cleveland
Triple-S Salud, Inc.
University of California Berkeley
Virginia Prescription Monitoring Program
US Dept of Defense
US Military
US National Guard
Virginia Dept. Of Health
UK Ministry of Defence
1, 700, 000
Starbucks
University of Miami
Norwegian Tax Authority
Service Personnel and Veterans Agency (UK)
UK Home Office
Stanford University
University of Utah Hospitals & Clinics
AT&T
BNY Mellon Shareowner Services
Auction.co.kr
Chile Ministry Of Education
Data Processors International
GS Caltex
Jefferson County
Compass Bank
City and Hackney Teaching Primary Care Trust
Dai Nippon Printing
Driving Standards Agency
Driving Standards Agency
Fidelity National Information Services
Hannaford Brothers Supermarket Chain
Gap Inc
Monster.com
TD Ameritrade
as Lottery
UK Revenue & Customs
TK / TJ Maxx



ORDER X-AXIS BY ALPHABETICAL DATA SENSITIVITY

SEND FEEDBACK

SEE THE DATA

Version 1.095 // design & concept: David McCandless
code: Tom Evans,
Powered by VIZSweet

informationisbeautiful.net

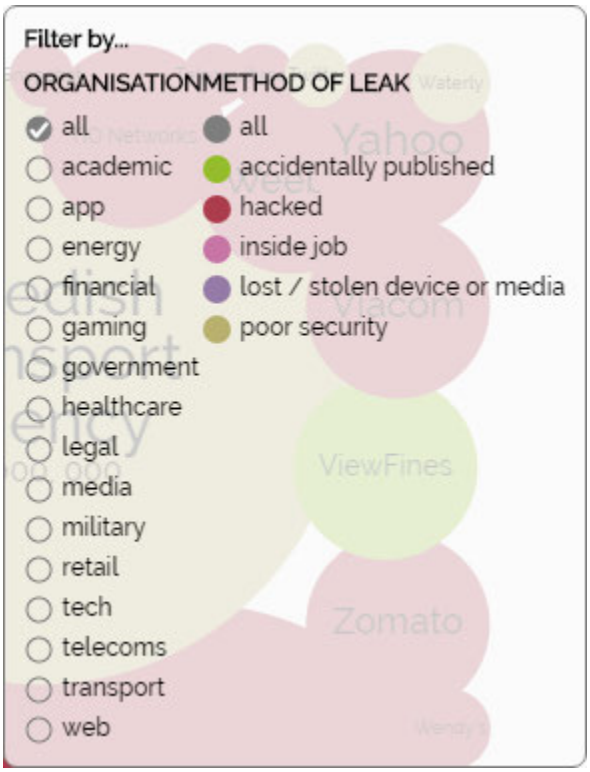
VIZsweet

Source: DataBreaches.net, IdTheftCentre, press reports
Research: Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson

Live link: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Bubbles are clickable to learn more information and read originating articles and reports.

Bubbles sized by Data Sensitivity
Bubbles colored by Method of Leak:



Olympic hackers may be attacking chemical warfare prevention labs

engadget **Jon Fingas**
Engadget June 19, 2018

The team behind the 2018 Winter Olympics hack is still active, according to

The team behind the 2018 Winter Olympics hack is still active, according to security researchers -- in fact, it's switching to more serious targets. Kaspersky has discovered that the group, nicknamed Olympic Destroyer, has been launching email phishing attacks against biochemical warfare prevention labs in Europe and Ukraine as well as financial organizations in Russia. The methodology is extremely familiar, including the same rogue macros embedded in decoy documents as well as extensive efforts to avoid typical detection methods.

While Kaspersky didn't directly point fingers, it brought up a number of clues suggesting that Russia was responsible. Most of the lab targets were people associated with an upcoming biochemical threat conference run by Spiez Laboratory, which just happened to be involved in the investigation of the nerve agent poisoning of former Russian double agent Sergei Skripal and his daughter Yulia. Also, Kaspersky noted that the custom images and messages in the documents were in "perfect" Russian, and

one of them specifically references the Skripal attack (conveniently, a piece where scientists couldn't definitively came from Russia).

So why target Russian financial outfits, then? Kaspersky acknowledged that there could be multiple parties involved (say, profit-oriented crooks in addition to state-sponsored attackers). However, it's generally accepted that Russia tried to frame North Korea for the Olympic hack. It's entirely possible that the Russian targets amounted to a false flag meant to cast doubt on the true origins of the attack. The focus on labs and the Skripal connection may have been meant to rattle the West for daring to attribute assassination attempts to Russia.

It may be difficult to completely prevent campaigns like this when political tensions are so high. Kaspersky believes the labs can curb this in the future, however, such as tightening their overall security and running impromptu security audits. It's also a reminder to be cautious -- a seemingly innocuous attachment can have dire consequences.

Securelist

- This article originally appeared on Engadget.