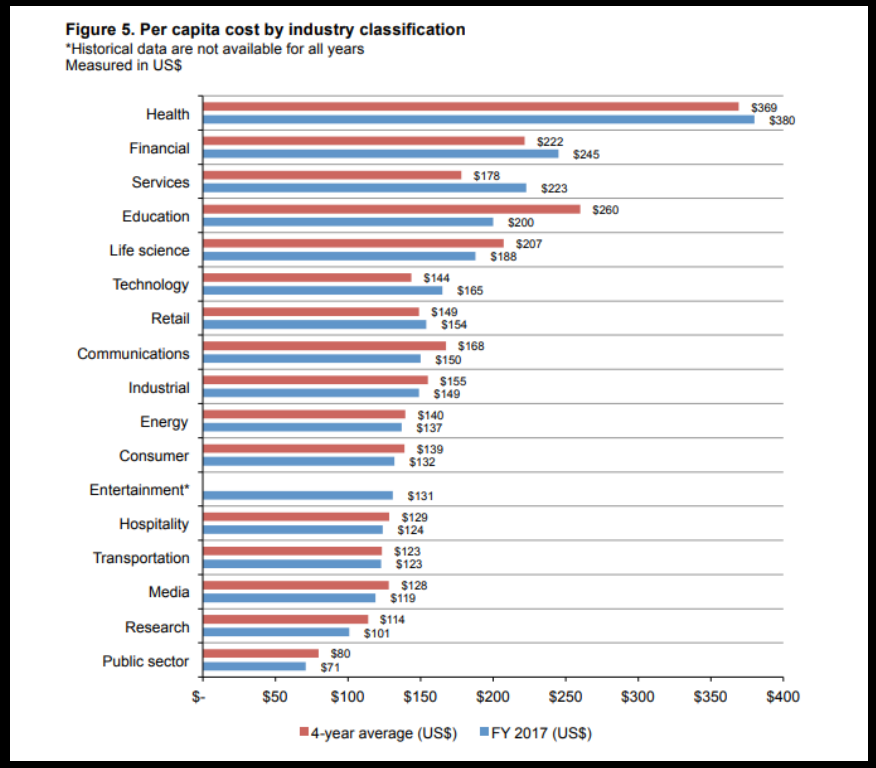
Cybersecurity – What is going on here…

CSUSM Cybersecurity Education Hub
Teresa Macklin
Fall 2019

Overview

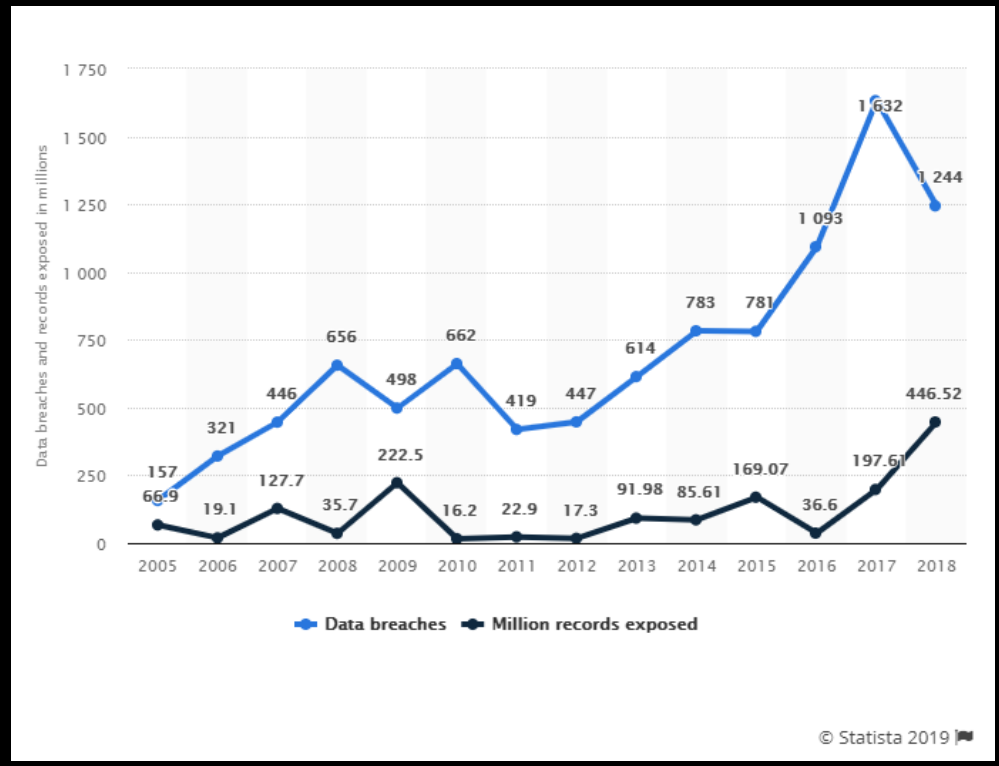
- Current Threats & Patterns
- Interesting/Historic Cybersecurity Events
- Cybersecurity Careers

Upward Trends



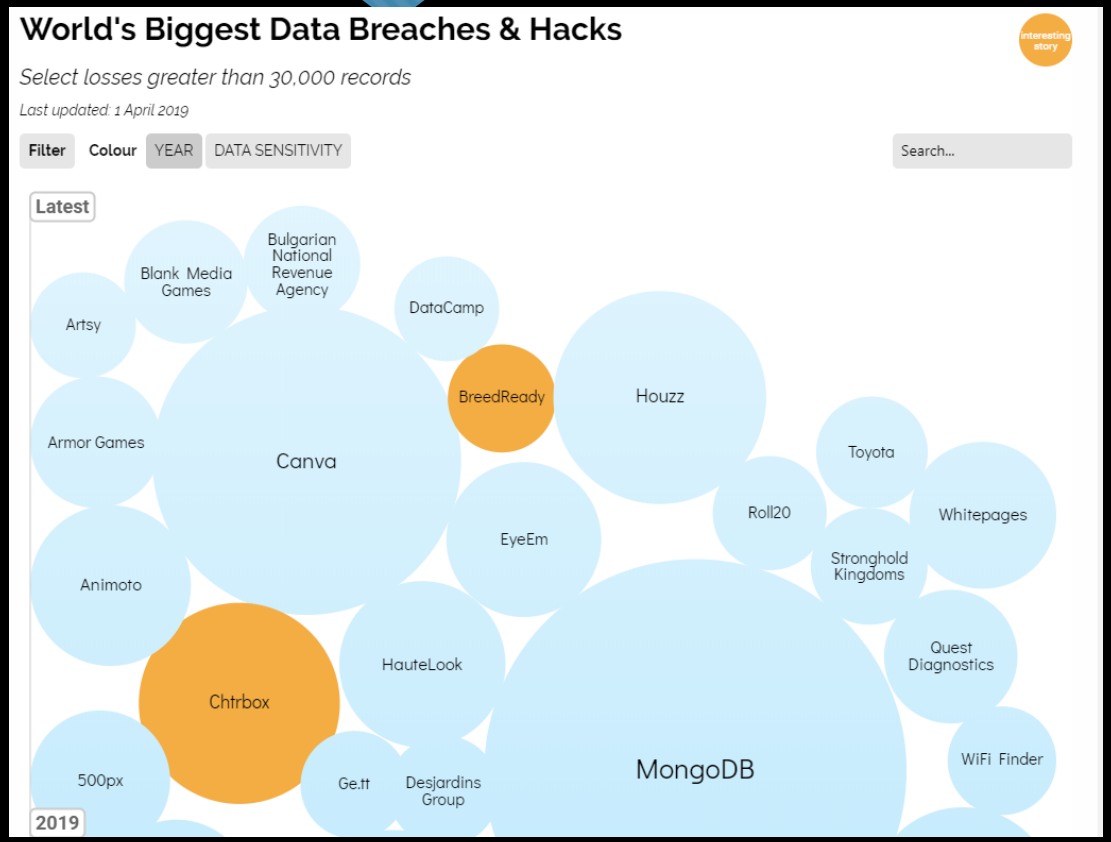
From the Ponemon Report 2017: https://www.ibm.com/security/infographics/data-breach/

Annual number of data breaches and exposed records in US, 2008 – 2018



https://www.statista.com

What does it look like?



- Growth in number of data breaches
- Affects all sectors
  - Individuals – identity theft, payment card fraud
  - Companies – intellectual property loss, damage to operations
  - Healthcare – ransomware, loss of privacy
  - Cyberwar …
  - Election interference …

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

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

Threats Differ by Industry Sector

Chart from Verizon Data Breach Investigation Report - these annual reports can be found online – visit https://enterprise.verizon.com/resources/reports/dbir

Why, Oh Why?

- Identity theft
- It is worth money!
- Fraud (healthcare, online transactions, payment card)
- Use of your computer resources
- Intellectual property theft
- Corporate espionage
- State espionage

Hacker service	Price
Social Security number (sold as part of 'Fullz' dossier)	$30
Date of birth	$11
Health insurance credentials	$20
Visa or MasterCard credentials	$4
American Express credentials	$7
Discover credit credentials	$8
Credit card with magnetic stripe or chip data	$12
Bank account number (balance of $70,000 to $150,000)	$300 or less
Full identity 'Kitz'	$1,200 to $1,300

Famous Cybersecurity Event: Stuxnet

- Stuxnet – First (probably first) use of "malware" to target the physical world
- Discovered Summer 2010
- Beginning of "cyber warfare" (except psyops but that is another lecture!)
- Used to alter the speed of centrifuges in a single nuclear processing facility in Iran
- Sabotaged facilities experienced reduced output of enriched uranium

Famous Cybersecurity Event: 2016 Election

- Use of social media for psychological operations against United States
- Purpose was "sow discord" among votors
- Russia developed "troll farms" (known as Internet Research Agency)
- Targeted democrats – phishing against Clinton campaign manager
- With compromised computes – extracted campaign documents and published them
  - Purpose was to exacerbate "Hillary vs Bernie" conflict among Democratic and Independents
- Target state election agencies – extracted voter registration
- Used data to target voters

Famous Cybersecurity Event: Marai Botnet

- Internet of Things (IoT) – devices, devices everywhere
- Devices hard to secure
- Vulnerable IOT devices compromised by simple default password method
- Fall 2016 - used to create botnet/denial-of-service attack against internet infrastructure

Famous Cybersec Event: Target

- Target – giant retail store chain
- HVAC company equipment is on Target's network
- 2013 - HVAC engineer gets "spearphished" and his credentials are stolen
- With stolen credentials, hackers get access to Target systems
- Hackers plant malware on cash register systems
- Steal payment card info
- Cards then used to make purchases and/or card info sold on black market

Jobs in Cybersecurity

- Broad range of careers
- Skills sets vary – organizational to technical
- Range from Audit & Compliance to Risk Analyst to Penetration Tester to Incident Responder to Chief Information Security Officer
- Cyberseek website has lots of data about careers and education

Jobs

- Security Analyst - https://www.cybersecurityeducation.org/careers/how-to-become-a-security-specialist/
- Security Software Developer
- Security Consultant
- Information Security Officer - https://www.cybersecurityeducation.org/careers/how-to-become-a-security-specialist/
- Penetration Tester - https://www.cybersecurityeducation.org/careers/penetration-tester/
- Incident Responder
- Information Security Auditor - https://www.cybersecurityeducation.org/careers/security-auditor/