DESIGN – WEEK 2

Collecting data and abstracting the data.

CYBER ATTACK TRENDS

"Data Abstraction"

This week we collected the required data for the questions we formulated previous week. We also classified the data that we collected according to its data type and attributes.

- Show from which countries the most cyber attacks originate

Geography	2016 World rank	2016 Overall average	2015 World rank	2015 Overall average	Annual change
United States	1	24.0%	2	18.9%	5.1%
China	2	9.6%	1	23.7%	-14.1%
Brazil	3	5.8%	10	2.0%	3.8%
India	4	5.1%	3	3.4%	1.7%
Germany	5	3.4%	8	2.2%	1.1%
Russia	6	3.1%	11	1.9%	1.2%
United Kingdom	7	2.6%	7	2.3%	0.3%
France	8	2.4%	9	2.1%	0.3%
Japan	9	2.3%	12	1.6%	0.7%
Vietnam	10	2.2%	23	0.9%	1.3%

Figure 1 Mailicious Activity by source: Overall rankings, 2015-2016

- ~~Show which countries are targeted the most by cyberattacks~~
- Replaced by: Which sectors are the most targeted

	Incidents				Breaches			
	Total	Small	Large	Unk	Total	Small	Large	Unk
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51
Total	42,068	606	22,273	19,189	1,935	433	278	1,224

Figure 2 Number of Security Incidents by Victim Industry and organization size

- What are the goals/motivations of these attacks?

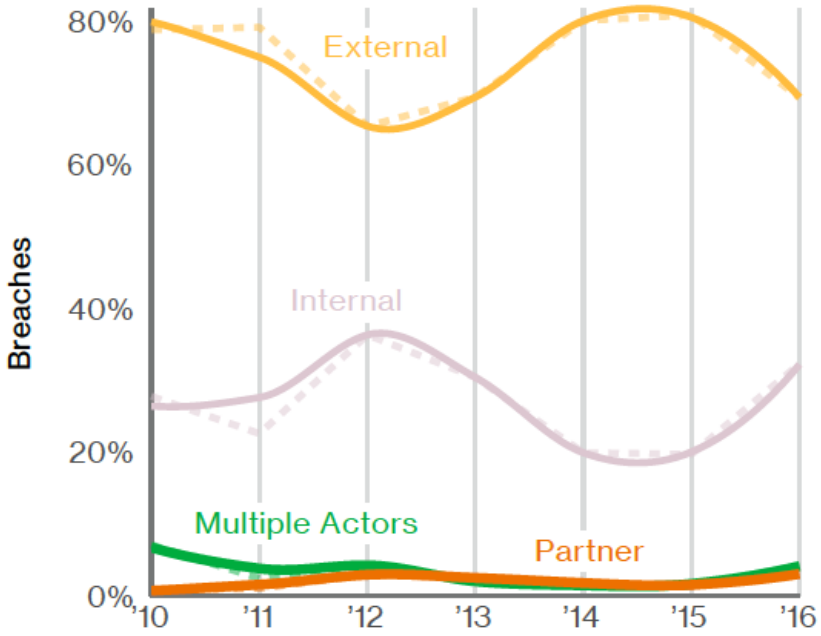

Figure 3 Threat actor categories over time

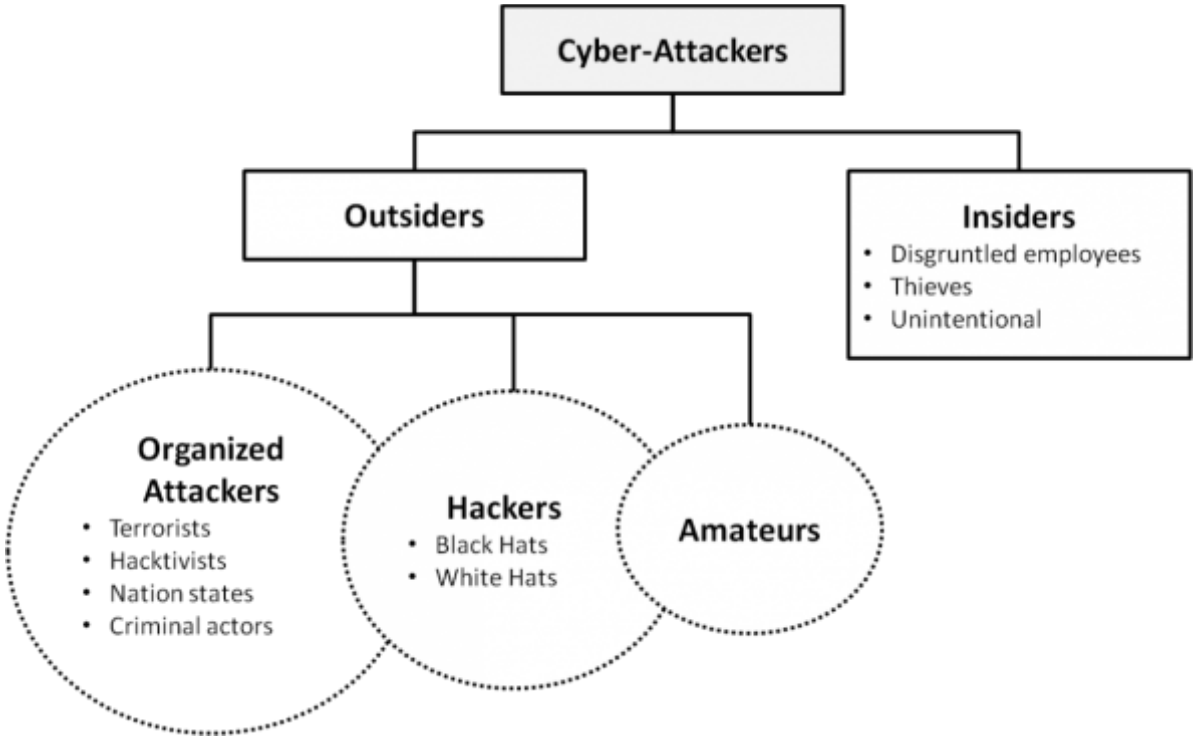

Figure 4 Types of Cyber Attackers

Tabel 1 **Dreigingsmatrix**

Bron van dreiging	Doelwitten: Overheden	Private organisaties	Burgers
Beroepscriminelen	Verstoring ICT Manipulatie van informatie Diefstal en publicatie of verkoop van informatie Overname ICT	Verstoring ICT Manipulatie van informatie Diefstal en publicatie of verkoop van informatie Overname ICT	Verstoring ICT Manipulatie van informatie ↓ Diefstal en publicatie of verkoop van informatie Overname ICT
Staten	Digitale spionage Offensieve cybercapaciteiten Diefstal en publicatie van informatie	Digitale spionage Offensieve cybercapaciteiten Diefstal en publicatie van informatie	Digitale spionage
Terroristen	Verstoring/overname van ICT	Verstoring/overname van ICT	
Cybervandalen en scriptkiddies	Diefstal informatie Verstoring ICT	Diefstal informatie Verstoring ICT	Diefstal en publicatie van informatie
Hacktivisten	Diefstal en publicatie verkregen informatie Defacement ↑ Verstoring ICT Overname ICT	Diefstal en publicatie verkregen informatie Defacement ↑ Verstoring ICT Overname ICT	Overname ICT ↑
Interne actoren	Diefstal en publicatie of verkoop verkregen informatie Verstoring ICT	Diefstal en publicatie of verkoop verkregen informatie Verstoring ICT	
Private organisaties		Diefstal informatie (bedrijfsspionage)	Commercieel ge-/misbruik of 'doorverkopen' gegevens
Geen actor	Uitval ICT	Uitval ICT	Uitval ICT

Figure 5 Dreigingsmatrix

Outsiders

- Organized attackers:
  - Geopolitieke (of interne) machtspositie verbeteren (statelijke actoren)
  - Maatschappelijke verandering veroorzaken, bevolking erniste vrees aanjagen of politieke besluitvorming beinvloeden (terroristen)
  - Ideologische motieven (hacktivisten)
  - Geldelijk gewin (Beroepscriminelen)
- Hackers:
  - Baldadigheid, hacken omdat het kan, geldelijk gewin (Black hats)
  - Aantonen van kwetsbaarheden en helpen verbeteren (White hats)
- Amateurs

Insiders

- Ontevreden werknemers: reputatieschade veroorzaken aan het bedrijf
- Dieven: lekken van bedrijfsgeheimen, eventueel voor geldelijk gewin
- Onopzettelijk: nalatigheid

- Specify which methods are used the most in these attacks (For example, data breaches, malware, ransomware)

Figure 6 Industry comparison (left: all security incidents, right: breaches only)

- What kind of impact do these attacks have and what is the social importance of these attacks?
    - 30 substations were switched off, and about 230 thousand people were left without electricity for a period from 1 to 6 hours. (Ukraine, 2015)
    - Mogelijk nog iets noemen over Nederlandse waterinfrastructuur (SCADA)
    - https://nos.nl/artikel/2155789-verkiezingsuitslag-makkelijk-te-hacken.html

DATA CLASSFICATION

Figure 1

Data set Type: Table

Data Types:

- Items: countries
- Attributes: ranks & percentages

Data set availability: static

Attribute Types: categorical/ordered (Quantitative)

Figure 2

Data set Type: Table

Data Types:

- Items: sector
- Attributes: Incidents and breaches

Data set availability: static

Attribute Types: categorical

Figure 3

Data set Type: Field

Data Types: grid, positions, attributes

Data set availability: static

Attribute Types: ordered: quantitative

Figure 4

Data set Type: Tree

Figure 5

Data set Type: Table

Data Types:

- Items: actors
- Attributes: targets

Data set availability: static

Attribute Types: categorical

Figure 6

Data set Type: Table

Data Types:

- Items: attack type
- Attributes: sector, color

Data set availability: static

Attribute Types: categorical, ordered: quantitative