PERSONA-BASED SECURITY

Dr. Deepak Subramanian

Security is sometimes a laggard in adopting bleeding-edge topics.

WHY ARE WE HERE?

Persona-based security is one of the bleeding-edge topics in today’s world that demands attention.

Should we embrase it or is it not up to task ?

Does it incite discussion and exploration ?

Lets discuss …

PART 1 - PERSONA – BASED SECURITY

BRILLIANT PEOPLE ARE IN ADS BUSINESS (APARENTLY) !!

"The best minds of my generation are thinking about how to make people click ads." - Jeff Hammerbacher

When you think of marketing and personas, what all can you think about

1. Learn about users to serve relevant ads
2. Send offers to the correct people
3. Create your ads in a manner that it reaches your target audience

PERSONAS ? ROLES ?

When you think of security and personas, what all can you think about

1. Profiling in physical security
2. Role-based access control ? (ok more on this later)
3. Adaptive learning for employees ?
4. Your ideas …

QUICK INTRO ..

- Persona is an evolving thing. It is not a to be considered as designed and stable.
- Based on the level of detail of the persona, more accuracy can be obtained but that also means lesser people fall into the category.
- It is important to do a sanity check from time to time.

SOME CHARACTERISTICS - PERSONA

A **Persona** is a detailed user model that represents archetypical users.

- In other words, a persona has the characteristics of a group of similar users. A persona is not necessarily a real person but a fictitious one modelled with a set of characteristics

A **Persona** may be defined by his or her goals.

- A hallmark work by Cooper first explained that Personas are used in goal-directed design [2]. Goals are different than the tasks in that a goal is an end condition while a task is an intermediate process that is necessary to accomplish goals.

A **Persona** is created by analyzing the real users' goals, behaviors and motivations.

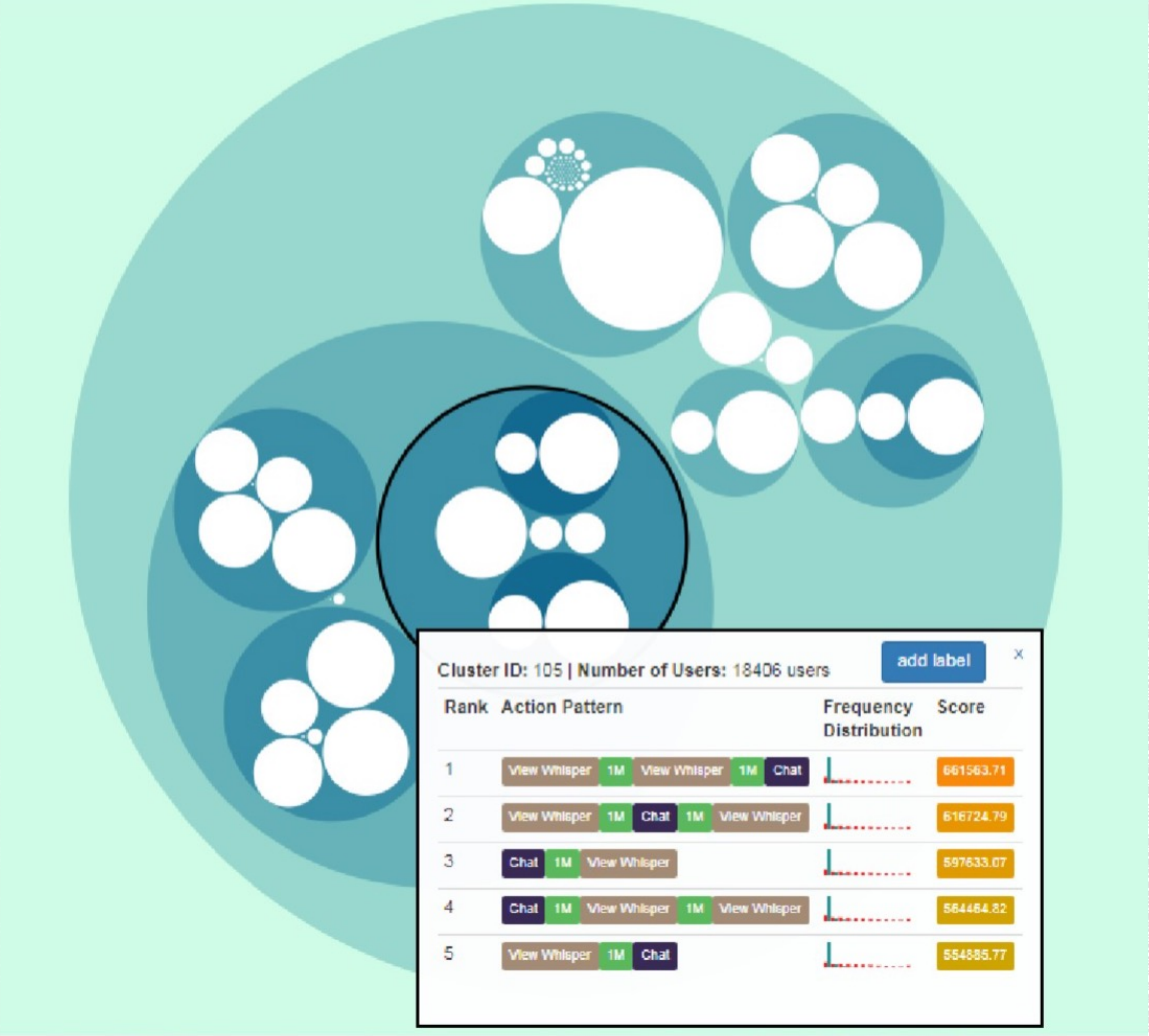
- We will look into the creation of personas soon.

TWO TYPES OF CREATING PERSONAS

Clustering

Restricted Foundation Personas

CLUSTERING



Cluster ID: 105 | Number of Users: 18406 users

Rank	Action Pattern	Frequency Distribution	Score
1	View Whisper 1M View Whisper 1M Chat		661563.71
2	View Whisper 1M Chat 1M View Whisper		616724.79
3	Chat 1M View Whisper		597633.07
4	Chat 1M View Whisper 1M View Whisper		564464.82
5	View Whisper 1M Chat		554885.77

- Can be Unsupervised
- Allows for indeterminate number of clusters

For large enough data – clusters are always going to be more practical and accurate.

Lets discuss the disadvantages ?

RESTRICTED FOUNDATION PERSONAS

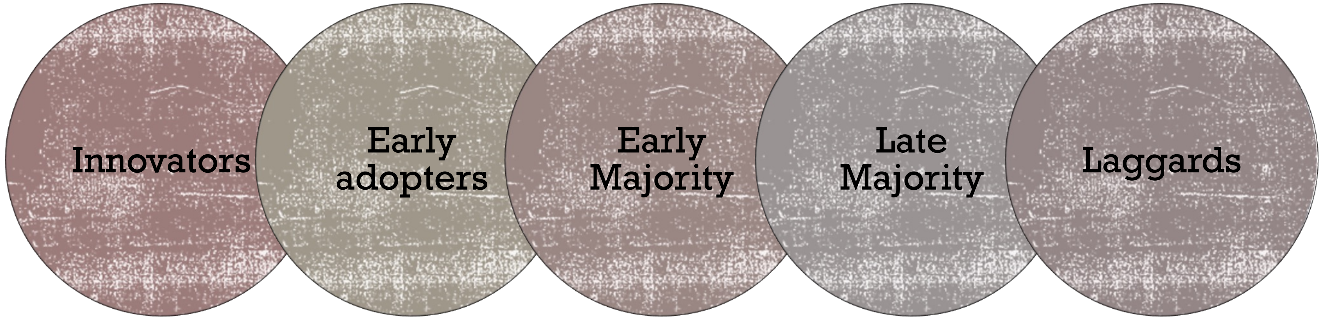
Target-Customer Characterizations

Goal-oriented design

TARGET-CUSTOMER CHARACTERISTICS

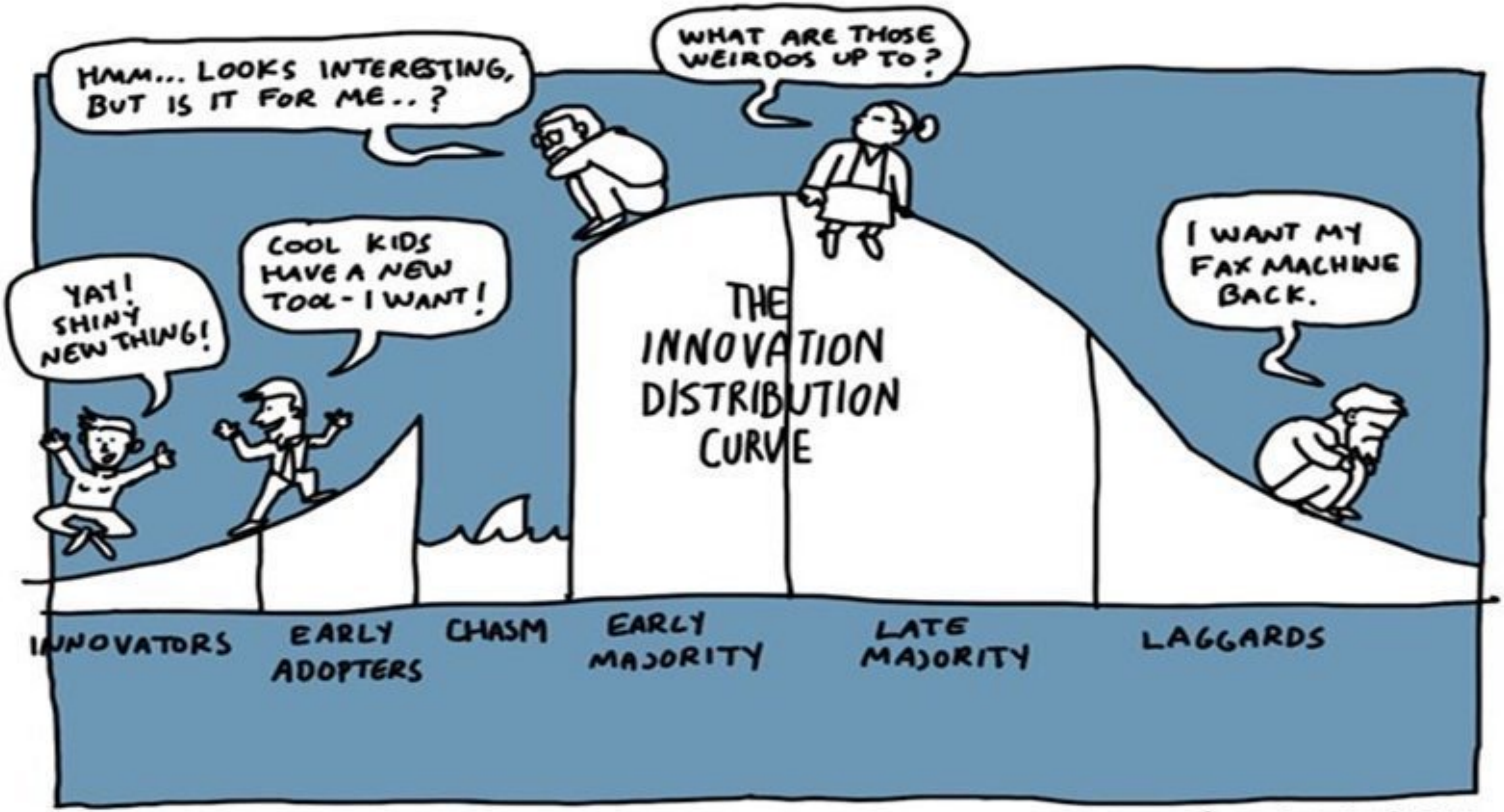
- Since personas were typically from a marketing, sales and advertising angle, it is important to look at the "Target-customer"
  - What kind of customer are they looking at ? [basic characteristics => broad categories]
  - What kind of broad categories are you looking to classify customers to ?
- Idea is to built "Foundational personas" based on the targer user/customer
- One of the most important works in this way of thinking is by G.A. Moore – "Crossing the chasm"
- Quite the model when we use "Role-based" controls in security

CROSSING THE CHASM



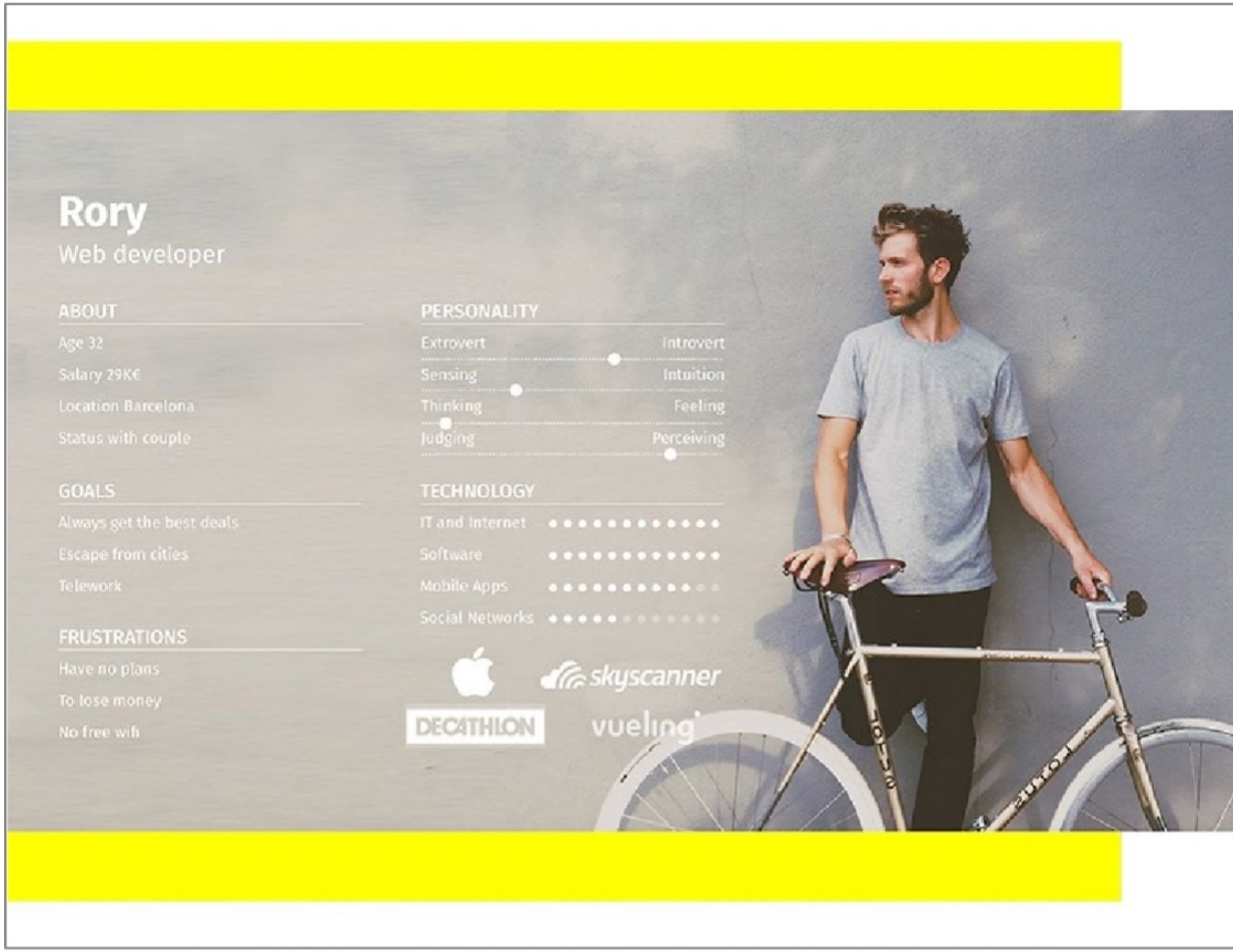
Hallmark work by G.A.Moore:

1/ The book actually talks about the chasm – how to move from early adopters to early majority
2/ But all categories are very important for marketers because it is how a ”technology adoption cycle” might happen.


HMM... LOOKS INTERESTING, BUT IS IT FOR ME..?
WHAT ARE THOSE WEIRDOS UP TO?
COOL KIDS HAVE A NEW TOOL - I WANT!
YAY! SHINY NEW THING!
I WANT MY FAX MACHINE BACK.
THE INNOVATION DISTRIBUTION CURVE
INNOVATORS
EARLY ADOPTERS
CHASM
EARLY MAJORITY
LATE MAJORITY
LAGGARDS

BUSINESSILLUSTRATOR.COM

RESTRICTED FOUNDATION PERSONAS



Rory

Web developer

ABOUT

Age 32

Salary 29K€

Location Barcelona

Status with couple

GOALS

Always get the best deals

Escape from cities

Telework

FRUSTRATIONS

Have no plans

To lose money

No free wifi

PERSONALITY

Extrovert — Introvert

Sensing — Intuition

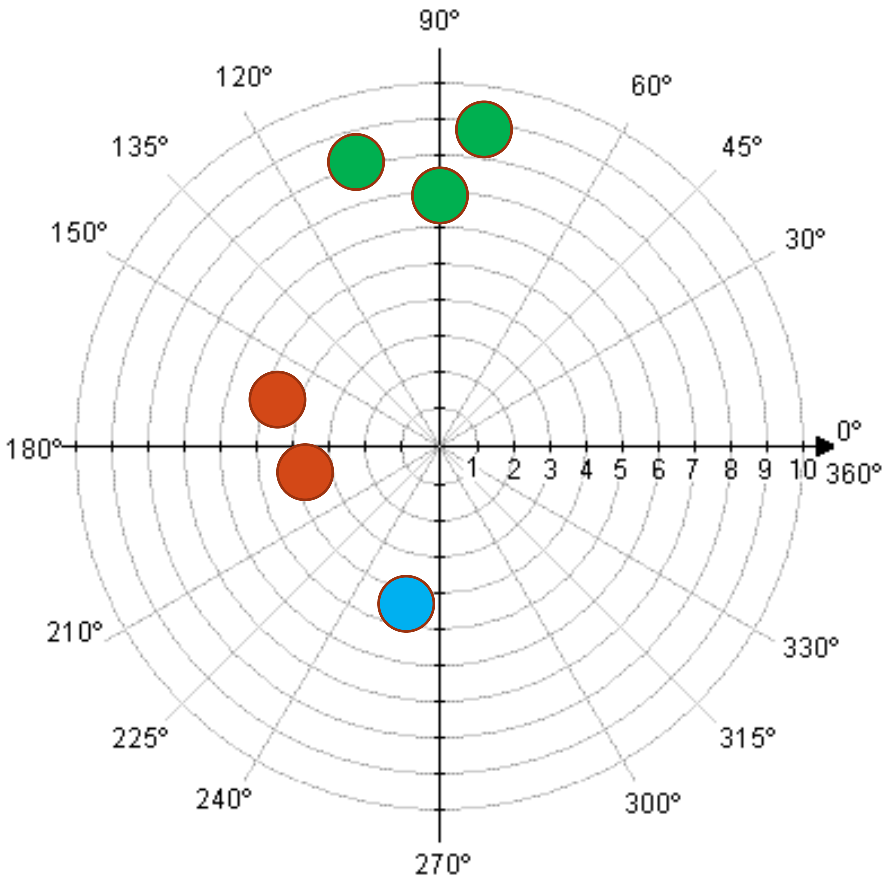
Thinking — Feeling

Judging — Perceiving

TECHNOLOGY

IT and Internet	●●●●●●●●●●●●
Software	●●●●●●●●●●●●
Mobile Apps	●●●●●●●●●●○○
Social Networks	●●●●●○○○○○○○

Figure 5: An example persona with personal goals (Ref. Persona examples [11])

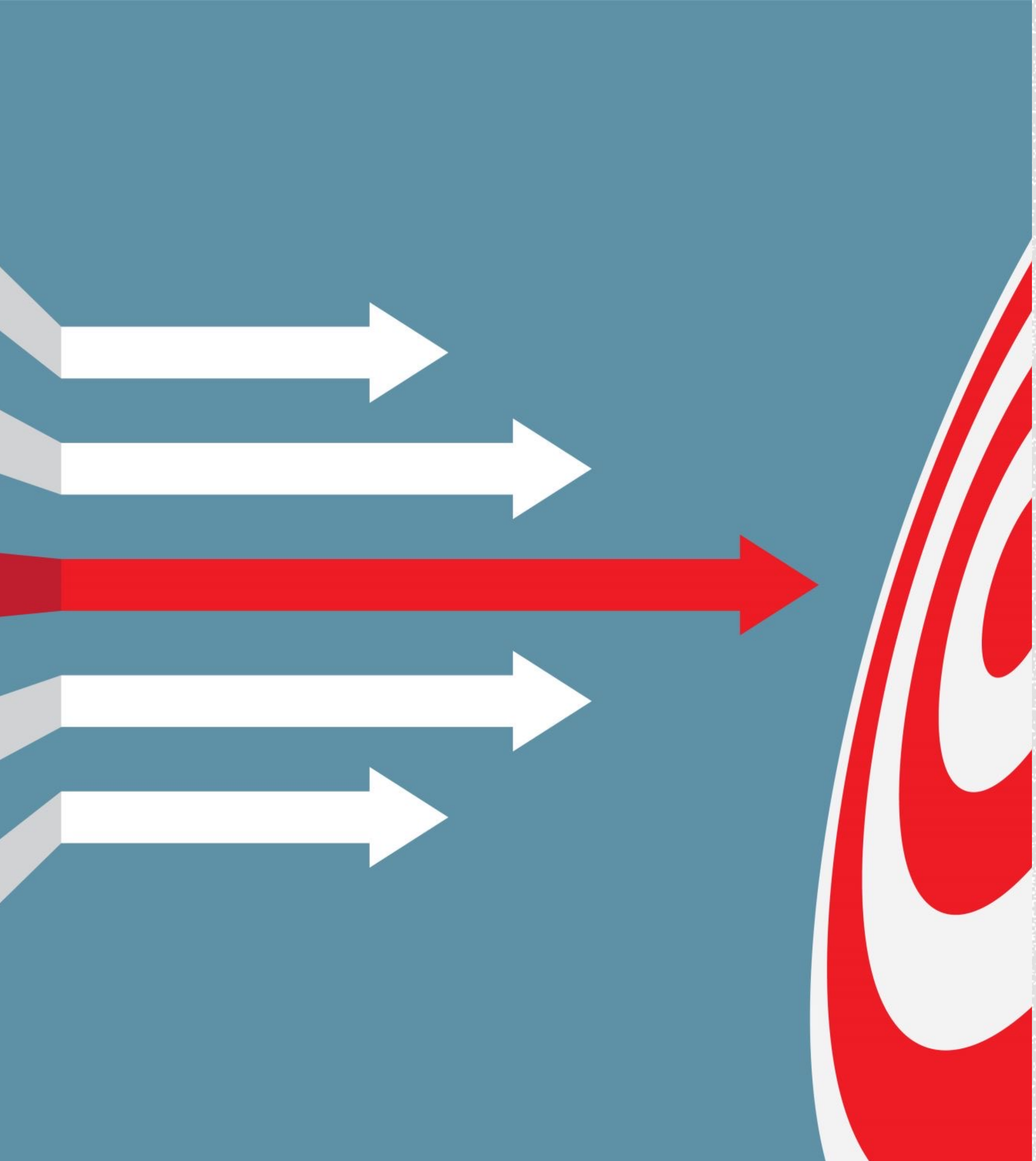


TARGET-USER CHARACTERISTICS

- Does not consider the end goal of the product much
  - More focused on orientation of the product to the user
- Very good at
  - Critical features of the target persona

GOAL ORIENTED DESIGN

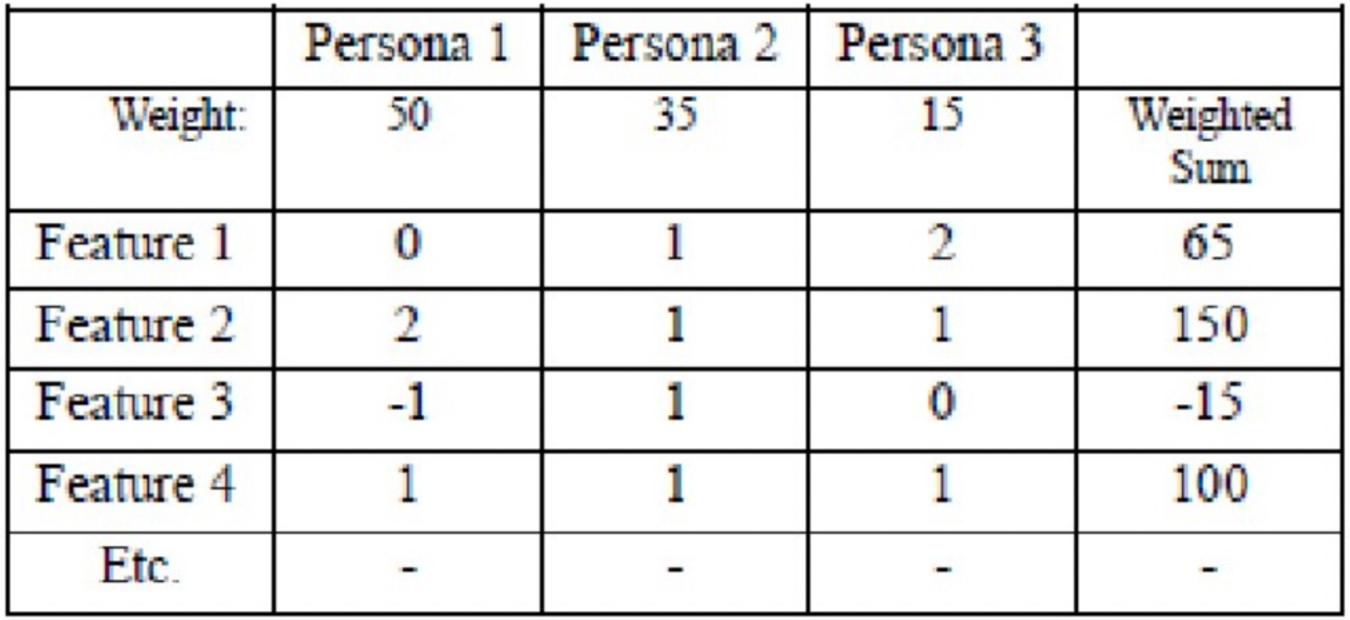
- Goal-oriented design is just as the name suggested – focused on goals
- One proponent of this class of model is by Alan Cooper in his book "The inmates are running the asylum"
- Another is from Pruitt and Grudin which is an improvement over cooper's work specifically for the IT context
  - Finding a representative user for each persona is key need
  - Very rigorous



GOALS [REF. BLOMKVIST]

Personal goals :	Simple and universal Eg. Not to make mistakes, get an adequate amount of work done
Corporate goals :	Organisational goals Eg. Increase market share Sell product A
Practical goals :	Practical goals bridge the gap between the objectives of the organization and the objectives of the individual.
False goals :	Not really a key goal of the peoject Eg. Use less memory

MICROSOFT PRUITT & GRUDIN



	Persona 1	Persona 2	Persona 3	
Weight:	50	35	15	Weighted Sum
Feature 1	0	1	2	65
Feature 2	2	1	1	150
Feature 3	-1	1	0	-15
Feature 4	1	1	1	100
Etc.	-	-	-	-

Figure 6: Weighted persona matrix (Ref. Pruitt and Grudin [3])

EXAMPLE OF GROCERY SHOPS

Amazon – Image processing

My Super Market – Colruyt – bar codes

The small shop near my house – price labels

Characteristics	**Moore model**	**Cooper model**	**Pruitt-Grudin Model**
Creation	Arbitrary/ Expert Consortium	Focus Group and surveys	Focus Group with expert consortium inputs
Foundation Personas	Yes – Less Detailed	Yes - Detailed	Yes - Detailed
Sanity Check	No	Yes	Yes
Target challenges	Yes – Strong mapping	Yes – weak mapping	Yes – weak mapping
Goals-based	No	Yes	Yes
Needs-based	Yes	No	Yes
Feedback	No (*) – Basic update mechanism	Yes – new goals	Yes – new goals
Known applications	Mainly in marketing	Mainly in design	IT applications
Year of conception	1991	1998	2003
Reference	Crossing the Chasm	The inmates are running the asylum	ACM Research Paper (Affiliated to Microsoft Research)

PROS	CONS
Target users'/customers' requirements are well considered	Corporate requirements are secondary to users'
Extensive understanding of users' characteristics provides reliable metrics for customizing the product to the users' needs	Time and effort in understanding users' evolving characteristics is non-trivial
Can be used to formalize a lot of existing arbitrary mechanisms in the organization	Persona is a complex model involving many possible variations. Such complexities require careful creation and constant maintenance
Has wide-ranging applications in different parts of the organization eg. Security, Human Resources	Requires co-ordination between different groups since maintaining personas is non-trivial

“The level of detail of the personas at creation, the sanity check mechanism to check the correctness and accuracy of the personas, the feedback from the personas as the context evolves, and finally the mapping to the targets’ characterizations/goals based on the model are all important issues when using personas.”

PART 2 – THREAT MODEL

SOME FUNDAMENTALS

- Access control fundamentals
- Threat modeling fundamentals
  - Threat Actors
  - Threat Vectors
  - Risk

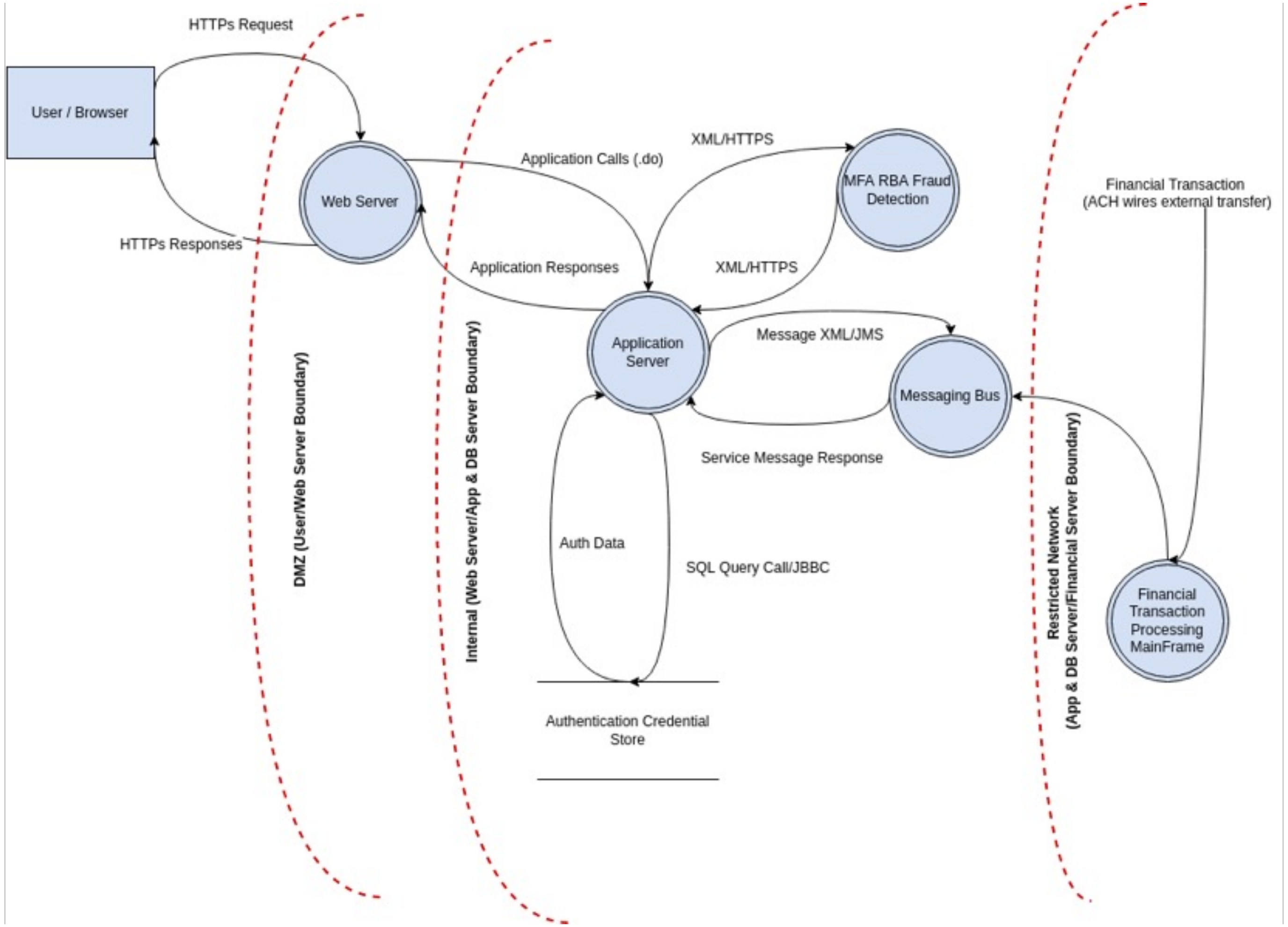
ROLE-BASED ACCESS CONTROL

Role based access control is a classical example of trivial foundational personas

WHAT IS THREAT MODELING

- This is not a pure threat modeling course so I will be brief .. ☺
- Theat models provied a clear and concise area of the threats the principal faces and the likelihood of it.

A SIMPLE THREAT MODEL (DFD)


HTTPs Request
User / Browser
Web Server
HTTPs Responses
Application Calls (.do)
XML/HTTPS
MFA RBA Fraud Detection
Financial Transaction (ACH wires external transfer)
Application Responses
XML/HTTPS
Application Server
Message XML/JMS
Messaging Bus
Service Message Response
DMZ (User/Web Server Boundary)
Internal (Web Server/App & DB Server Boundary)
Auth Data
SQL Query Call/JBBC
Restricted Network (App & DB Server/Financial Server Boundary)
Financial Transaction Processing MainFrame
Authentication Credential Store

A USER STORIES DRIVEN APPROACH ?

- Stage 0: Basic threat models – Role based implications but not more like STRIDE
- Stage 1: Roles based attack trees
- Stage 2: User stories = tied to a threat model => Moore model
- Stage 3: Abuser stories = completes the threat model => Goal oriented design

Data Flow Diagrams – DFDs can be detailed/low in detail as you make them. So they do not feature as a category here. However they are very relevant.

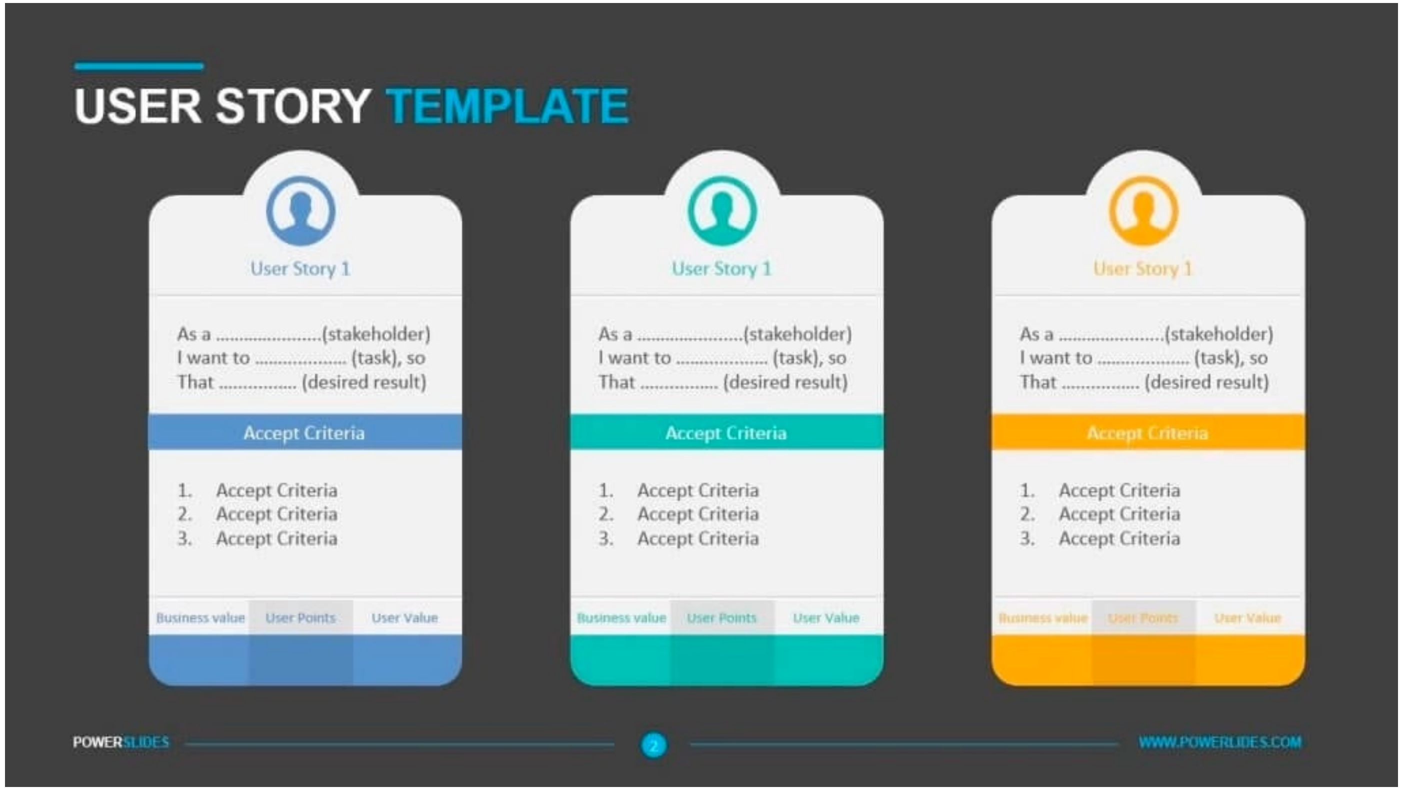
EXAMPLE OF GROCERY SHOPS

Amazon – Image processing

My Super Market – Colruyt – bar codes

The small shop near my house – price labels

RESTRICTED FOUNDATION PERSONAS



USER STORY TEMPLATE

User Story 1

As a ....(stakeholder)
I want to .... (task), so
That .... (desired result)

Accept Criteria

1. Accept Criteria
2. Accept Criteria
3. Accept Criteria

Business value | User Points | User Value

User Story 1

As a ....(stakeholder)
I want to .... (task), so
That .... (desired result)

Accept Criteria

1. Accept Criteria
2. Accept Criteria
3. Accept Criteria

Business value | User Points | User Value

User Story 1

As a ....(stakeholder)
I want to .... (task), so
That .... (desired result)

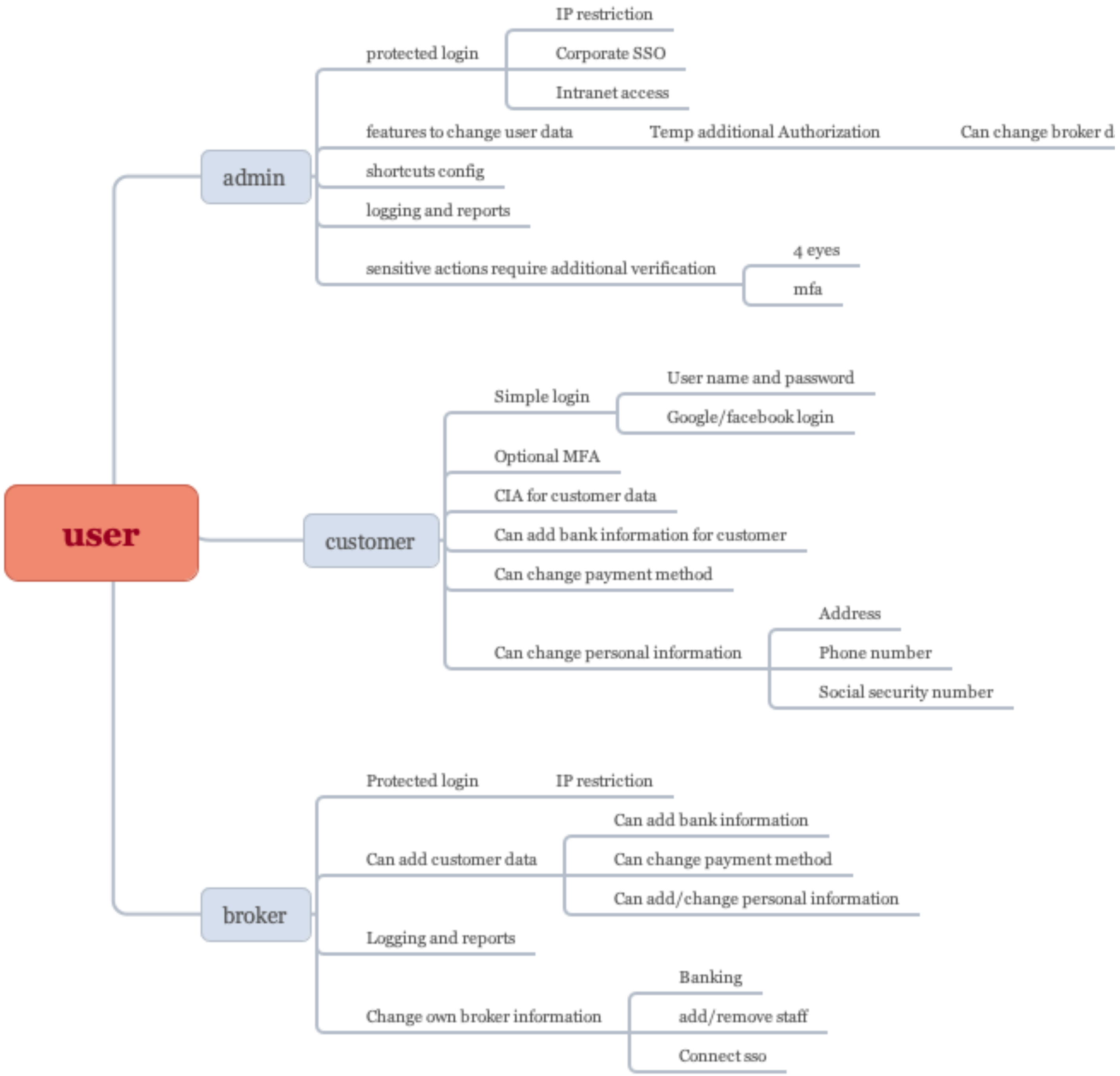
Accept Criteria

1. Accept Criteria
2. Accept Criteria
3. Accept Criteria

Business value | User Points | User Value

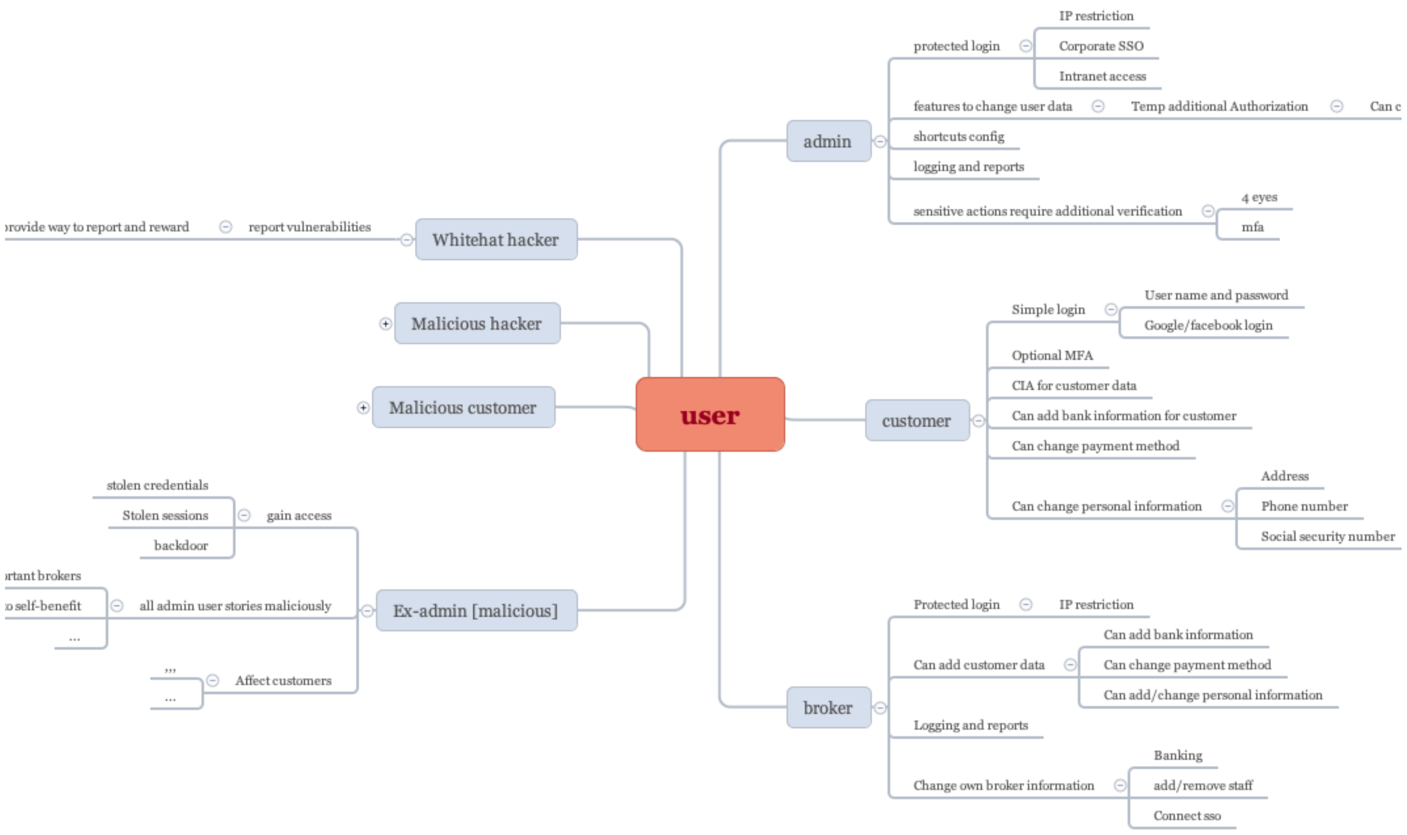
POWERSLIDES 2 WWW.POWERLIDES.COM

USER TREE



- user
  - admin
    - protected login
      - IP restriction
      - Corporate SSO
      - Intranet access
    - features to change user data
      - Temp additional Authorization
        - Can change broker d
    - shortcuts config
    - logging and reports
    - sensitive actions require additional verification
      - 4 eyes
      - mfa
  - customer
    - Simple login
      - User name and password
      - Google/facebook login
    - Optional MFA
    - CIA for customer data
    - Can add bank information for customer
    - Can change payment method
    - Can change personal information
      - Address
      - Phone number
      - Social security number
  - broker
    - Protected login
      - IP restriction
    - Can add customer data
      - Can add bank information
      - Can change payment method
      - Can add/change personal information
    - Logging and reports
    - Change own broker information
      - Banking
      - add/remove staff
      - Connect sso

ABUSERS + USERS

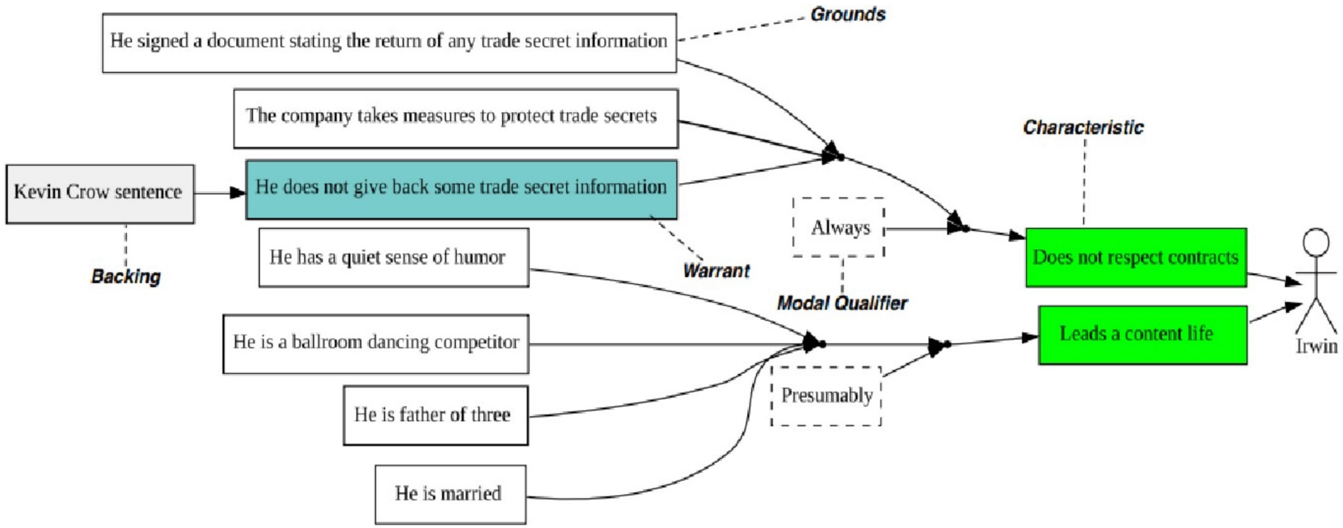


- user
  - admin
    - protected login
      - IP restriction
      - Corporate SSO
      - Intranet access
    - features to change user data
      - Temp additional Authorization
        - Can c
    - shortcuts config
    - logging and reports
    - sensitive actions require additional verification
      - 4 eyes
      - mfa
  - customer
    - Simple login
      - User name and password
      - Google/facebook login
    - Optional MFA
    - CIA for customer data
    - Can add bank information for customer
    - Can change payment method
    - Can change personal information
      - Address
      - Phone number
      - Social security number
  - broker
    - Protected login
      - IP restriction
    - Can add customer data
      - Can add bank information
      - Can change payment method
      - Can add/change personal information
    - Logging and reports
    - Change own broker information
      - Banking
      - add/remove staff
      - Connect sso
  - Whitehat hacker
    - report vulnerabilities
      - rovide way to report and reward
  - Malicious hacker
  - Malicious customer
  - Ex-admin [malicious]
    - gain access
      - stolen credentials
      - Stolen sessions
      - backdoor
    - all admin user stories maliciously
      - rtant brokers
      - o self-benefit
      - ...
    - Affect customers
      - ,,,
      - ...

ATTACKER PROFILES – THREAT QUANTIFICATION

- Collecting persona details can reveal more information about potential threat actors
- If an actor behavior is well-established, it can form a basis for other actors that fit the same persona
- Always note that these could be false positives since creating personas comes with its own risks

ATTACKER PROFILES – THREAT QUANTIFICATION


Grounds
He signed a document stating the return of any trade secret information
The company takes measures to protect trade secrets
Characteristic
Kevin Crow sentence
He does not give back some trade secret information
Always
Backing
He has a quiet sense of humor
Warrant
Does not respect contracts
Modal Qualifier
He is a ballroom dancing competitor
Leads a content life
Irwin
Presumably
He is father of three
He is married

ORGANIZATIONAL THREAT MODEL

- Do you think your organization has a persona
- How would you look at your organizational persona ?
- Do different parts of the organization have different personas ?

Conservative

Innovative

Paranoid

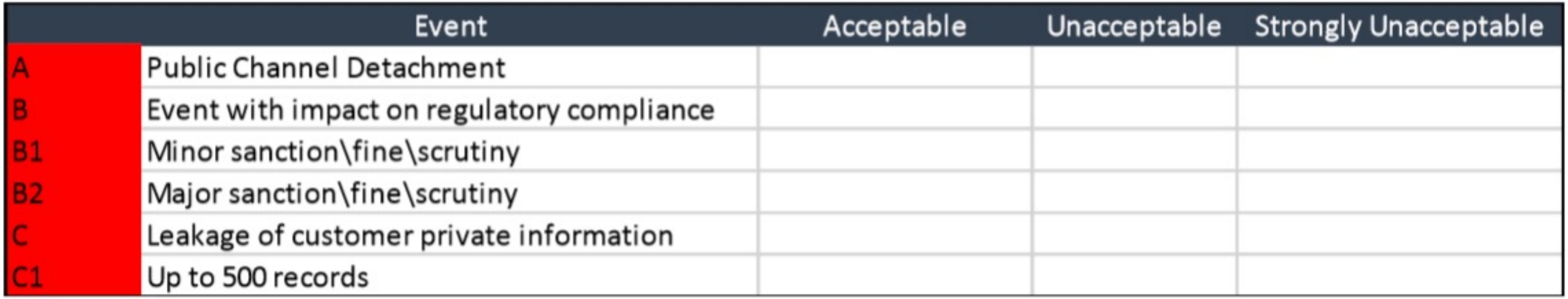
Profit centric

Purpose driven

ORGANIZATIONAL THREAT MODEL - WEIGHTED !

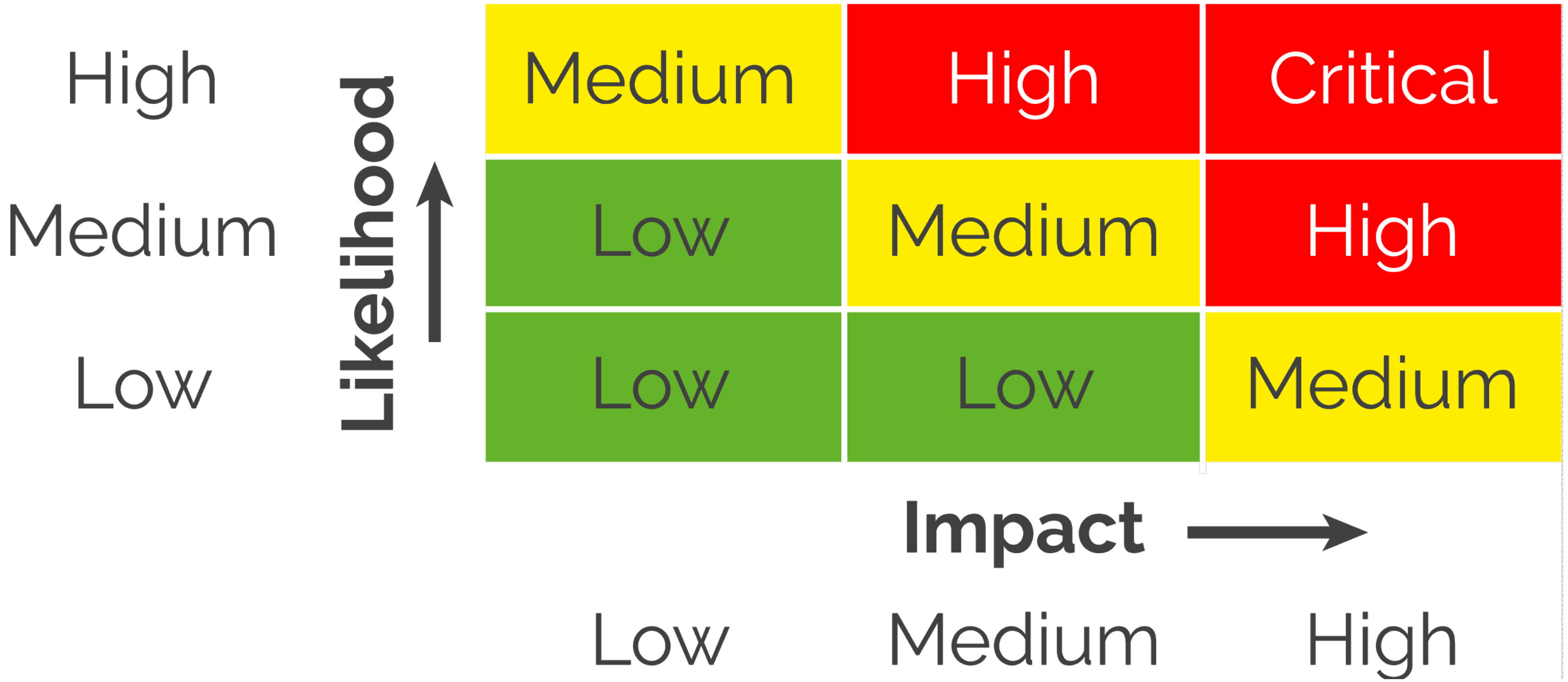
	First and fast	Paranoid	Innovate
Time to Market	5	1	5
Risk Avoidance	2	5	2
Pioneer	4	1	5
Service Level	2	3	3
Regulation	1	4	2
Customer trust loyalty	2	2	3

CYBER RISK DEF TABLE



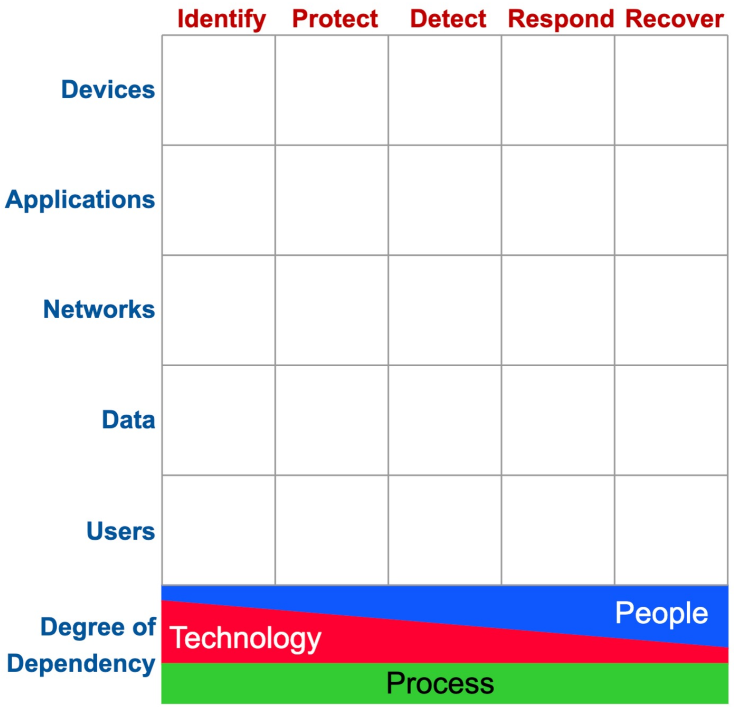
	Event	Acceptable	Unacceptable	Strongly Unacceptable
A	Public Channel Detachment			
B	Event with impact on regulatory compliance			
B1	Minor sanction\fine\scrutiny			
B2	Major sanction\fine\scrutiny			
C	Leakage of customer private information			
C1	Up to 500 records			

CYBER RISK MATRIX

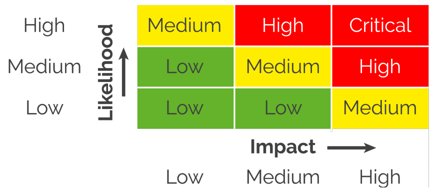


Likelihood ↑	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium
	Impact →		

CYBER RISK MATRIX



	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					



	Low	Medium	High
High	Medium	High	Critical
Medium	Low	Medium	High
Low	Low	Low	Medium

Likelihood
Impact

AN EXAMPLE

- There is an S3 bucket
- Application A is internet exposed. Application is innovation based – kanban application board. Developed by the R&D team in collaboration with a university.
- Application B is internal – doing some analysis. Very intense Waterfall model development. There is source code reviews, 4 eyes etc. Developed by a very experienced developer team with dedicated security engineers, analysts.
- Both have similar tools in place – a dependency check, a SAST tool…
- But ofcourse the applications are not of the same level of trustworthiness.
- When application A accesses application B, we start persona accesses. Application A has a persona that is not in line with Application B which means they need to be re-aligned.

EXERCISE 2 – 20 MINS

- Your company is a major software provider
  - You have many departments – ones that deal with banking industry for example have very strict requirements
  - You also have an active research department who want to be "researchers"
  - How do you take these into account to do an organizational threat model?

RESOURCES

- Threat modeling resources
  - Tools = OWASP Threat Dragon, MSFT Threat modeler, any software regardless
  - OWASP threat modeling channel on slack
    - https://github.com/owasp/www-project-threat-model
    - https://owasp.slack.com/messages/C1CS3C6AF
  - At least use free diagramming tools

  - Self-promotion: An open publication by me - https://www.linkedin.com/pulse/user-friendly-security-persona-based-deepak-subramanian/

Hands-on Threat modelling workshop

QUESTIONS ?

SUBUDEEPAK@OUTLOOK.COM