QONTO

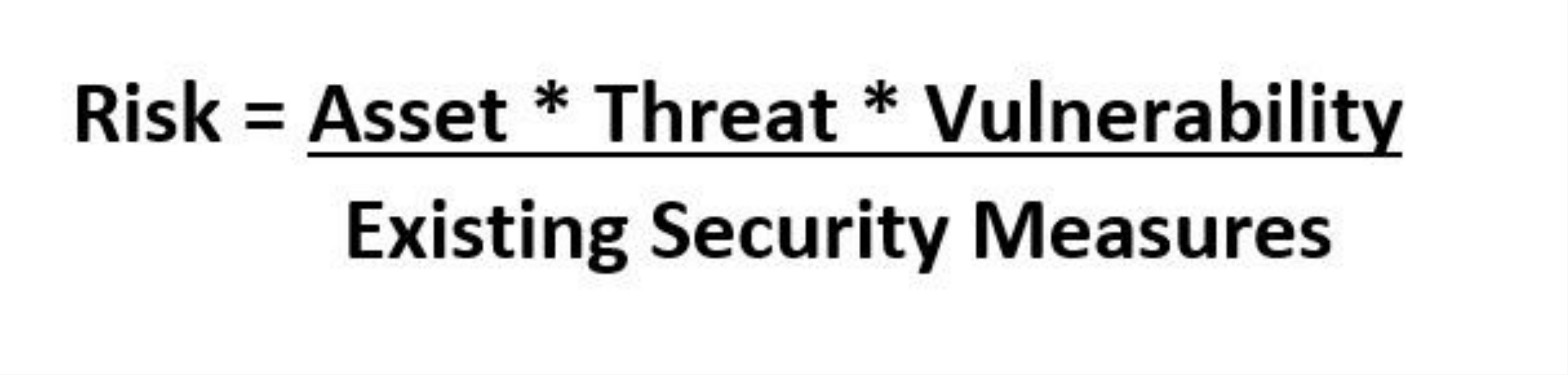
SUBMITTED BY:
Yogithasatyasai Pantham

(yogitha557@gmail.com)

PROFFESSOR:
Hadi EL-KHOURY

RISK

“Risk is constituted when ever a threat is able to access an asset by exploiting one or more vulnerabilities and by circumventing existing security measures.”



$$\text{Risk} = \frac{\text{Asset} * \text{Threat} * \text{Vulnerability}}{\text{Existing Security Measures}}$$

DESCRIPTION

- The Paris-based FinTech startup provides an online banking service that allows entrepreneurs, startups and SMEs to create an account in less than 5 minutes. With Qonto you can instantly receive an IBAN and get started to manage your company’s physical and digital business cards and perform your day to day operations. Founded in 2016, Qonto so far raised €11.6 million in funding from Alven Capital, well known business angels, as well as from Valar Ventures, the venture capital fund backed by Peter Thiel.
- The service will be expanded to Spain, Germany and Italy in 2019.

USER STORY:

qonto
Easy business banking

"For a freelancer, traditional banks are really archaic. With Qonto, I know exactly how much I pay for every service I need.“

-**Jean Charle Guichard**
Freelance videographer

"Manage my providers and teams expenses is now easy, fast and smart with Qonto! The cherry on top: the best customer service you can dream of!“

-**Olivier Ramel**
CE@Kymono

SUN OF ACTORS

DNS

USER

Credit Mutuel Arkea

AWS

FGDR

Lebara

Mobile Application

OBASHI

	A	B	C	D	E	F	G	FEDCBA
O	User	User	Lebara	Go Daddy.inc	AWS	▨	Qonto	
B	Client	Credit Mutual Arkea	ISP	Go Daddy	Amazon.inc	▨	Qonto.inc	
A	Qonto	▨	▨	DNS	●	▨	Qonto Server	
S	IOS	▨	▨	Windows 10	Windows 10	▨	Windows 10	
H	Iphone 8	▨	▨	H.P	DELL	▨	H.P	
I	4G/3G	4G/3G		Ethernet	Ethernet	▨	Ethernet	
G	FR	FR	FR	US	US	FR	FR	

HACKER STORIES:

#HS1:- As a hacker employed by terrorist, I want to get the details of top most business people, in order to hijack/attack/threaten the business people.

#HS2:- As a criminal hacker, I want to overwrite the transaction sent by the user online Qonto banking application with my own transaction, in order to get their money into my account.

#HS3:- As an Smart person (to start a new company), I want to hack the database and process , in order to copy idea and also to destroy it.

#HS4:- As a Cozy bear team(hired by Russian govt.), I want to hack the details and financial plans of all users, in order to give it to the Russian govt.

#HS5:- As a security agent of Boursorama banque, I want to create a bug in mob app of Qonto, in order to corrupt all the accounts.

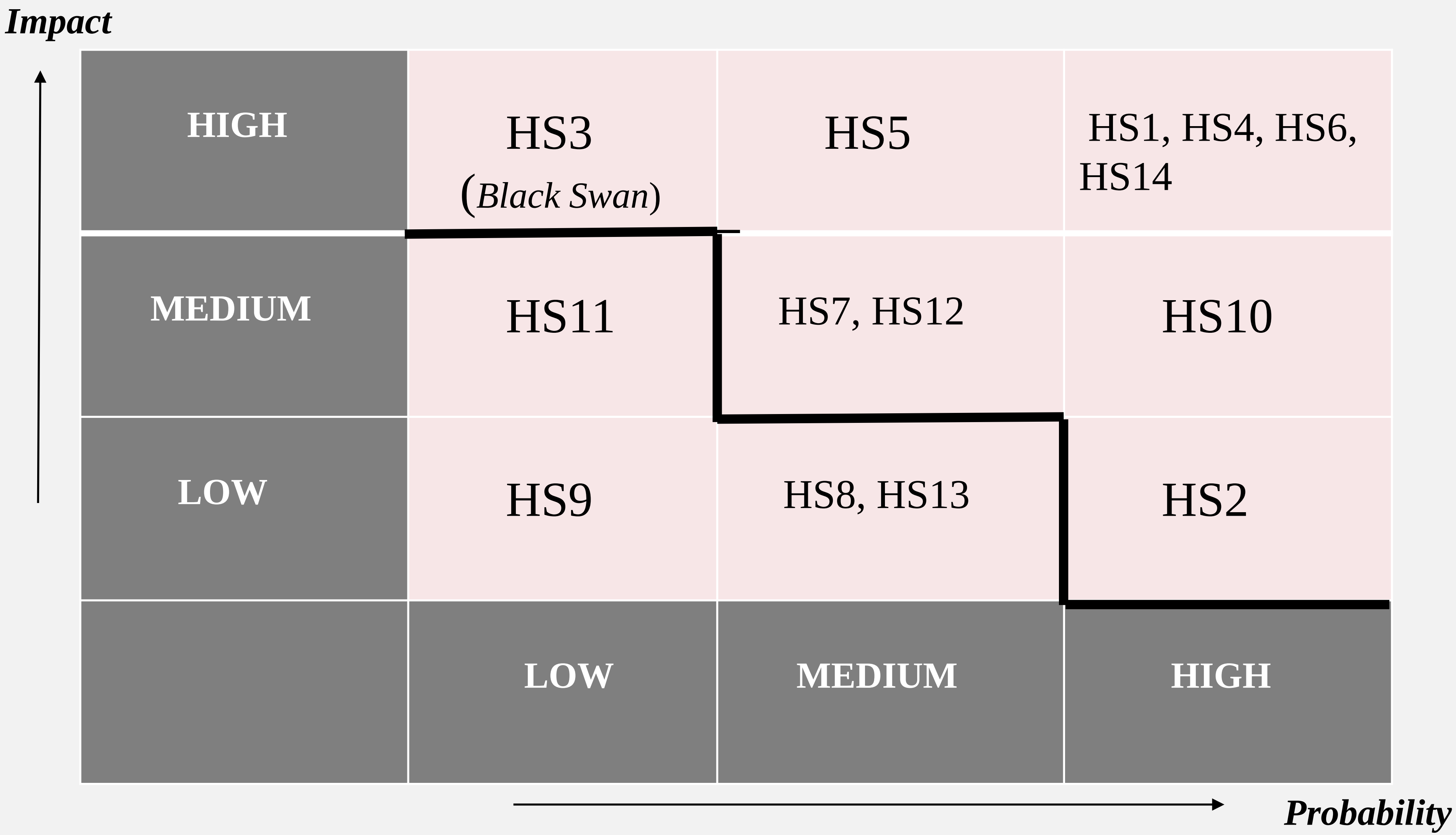
#HS6:- As a member of Dark Hydrus, I want to target educational Institutions, in order to deduct complete amount from them and get the French educational system down.

#HS7:- As a psychic hacker, I will stop the notifications to all the users, in order to put them in a tensed situation.

HACKER STORIES:

#HS8:- As a crazy hacker, I want to hack the details of a user, in order to loot the complete amount and blackmail him.
#HS9:- As a employee of a CGI, I want to grab the details of my CEO and company, in order to become rich.
#HS10:- As a angry risk manger of Qonto, I want to erase all the passwords and solve it back, in order to get promotion.
#HS11:- As a bored manager of Qonto, I want to change all the admin details, in order to stop the transactions.
#HS12:- As a ex-employee of Qonto, I want to deduct some amount from all the users every month, in order to reduce the volume of the customers.
#HS13:- As a hacker(hired by gf/bf of Renault's CEO), I want to hack the username and password, in order to transfer some money to my account.
#HS14:- As a member of sea-lotus, I want to create a technological bomb, in order to blast the Qonto and the investors will be in loss.

RISK ANALYSIS:



Impact

HIGH	HS3 (*Black Swan*)	HS5	HS1, HS4, HS6, HS14
MEDIUM	HS11	HS7, HS12	HS10
LOW	HS9	HS8, HS13	HS2
	LOW	**MEDIUM**	**HIGH**

Probability

RISK MITIGATION FOR HACKER STORIES:

HS1: As a hacker employed by terrorist, I want to get the details of top most business people, in order to hijack/attack/threaten the business people.

ANSSI SECURITY MEASURES:

RULE-8: Identify each individual accessing the system by name and distinguish the user/administrator roles.

RULE-12: Change the default authentication settings on devices and services.

RULE-32: Secure the network connection of devices used in**.**

HS2: As a criminal hacker, I want to overwrite the transaction sent by the user online Qonto banking application with my own transaction, in order to get their money into my account.

ANSSI SECURITY MEASURES:

RULE-14: Implement a minimum level of security across the whole IT stock.

RULE-16: Use a centralised management tool to standardise security policies.

RISK MITIGATION FOR HACKER STORIES:

HS4: As a Cozy bear team(hired by Russian govt.), I want to hack the details and financial plans of all users, in order to give it to the Russian govt.

ANSSI SECURITY MEASURES:

RULE-25: Secure the dedicated network interconnections with partners.
RULE-1: Train the operational teams in information system security.
RULE-2: Raise users' awareness about basic information security.
RULE-6: Organise the procedures relating to users joining, departing and changing positions.
RULE-8: Identify each individual accessing the system by name and distinguish the

HS5: As a security agent of Boursorama banque, I want to create a bug in mob app of Qonto, in order to corrupt all the accounts.

ANSSI SECURITY MEASURES:

RULE-17: Activate and configure the firewall on workstations
RULE-36: Activate and configure the most important component logs.
RULE-37: Define and apply a backup policy for critical components.

RISK MITIGATION FOR HACKER STORIES:

HS7: As a psychic hacker, I will stop the notifications to all the users, in order to put them in a tensed situation.

ANSSI SECURITY MEASURES:

RULE-24: Protect your professional email.

RULE-36: Define and apply a backup policy for critical components

HS10: As a angry risk manger of Qonto, I want to erase all the passwords and solve it back, in order to get promotion.

ANSSI SECURITY MEASURES:

RULE-1: Train the operational teams in information system security.

RULE-2: Raise users' awareness about basic information security.

RULE-6: Organise the procedures relating to users joining, departing and changing positions.

RULE-8: Identify each individual accessing the system by name and distinguish the user/administrator roles.

MAPPING THE MITIGATION:

RISK MITIGATION

Impact

HIGH **v**	HS3 ← (*Black Swan*)	HS5 ←	HS1, HS4, HS6, HS14
MEDIUM	HS11 ←	HS7, HS12 ←	HS10
LOW	HS9	HS8, HS13 ←	HS2
	LOW	**MEDIUM**	**HIGH**

Probability

REFERENCES:

1. https://qonto.eu/en
2. https://attack.mitre.org/groups/
3. https://www.arkea.com/banque/assurance/credit/mutuel/c_13273/fr/page-d-accueil
4. https://www.ssi.gouv.fr/guide/40-essential-measures-for-a-healthy-network/

By: Yogitha

D. Yogitha