

Bug Bounty Program (BBP)

Case study : Swiss Post

In the frame of the ETH course :
Psychological Aspects of Risk Management and Technology
Lecturer: Jan Schmutz
Semester: HS2020

Introduction



Anais Bouchat

Recently graduated from Life sciences at EPFL.

Since September 2020, is completing her Master in Health Sciences and Technology with a specialty in Neurosciences at ETHZ.



Andrea Betancourt

Independent consultant on sustainable and international development.

Pursuing MAS at the MTEC program whilst focusing on corporate sustainability.

Introduction



Giulia Beanato

Holds a PhD in Microelectronics from EPFL.
Working with ABB Switzerland as Senior Engineer, Software Architect. Pursuing MAS MTEC at ETHZ, currently in the second semester.



Serina Koshy

Working for Credit Suisse in the Swiss Universal Bank Area as Assistant Vice President as Access Manager and Product Owner.
Pursuing MAS at the MTEC program whilst focusing on management.

Agenda

- Introduction
- Digital transformation
- Corporate Culture
- Customer Perception
- Risk Analysis
- Conclusion

Methods



Interviews

6 employees from Swiss Post's security, IT and business development departments, as well as on public information of their BBP.



Survey

Public survey with 144 participants, across various age groups and focusing primarily on Swiss residents



Literature

Literature review across all sectors of industry especially customer service based



Programs

Review literature on other experiences on BBP implementation

Research Questions

How does BBP impact Digital Transformation?

What are the internal implications of BBP in corporate culture?

How can BBP be used to drive Digital Transformation?

What are the external implications of a BBP regarding customer perception and digital trust?

Bug Bounty at Swiss Post

White-hat Hackers: Ethical computer hacker / Computer security expert



VS.



Hire white-hat hackers to find bugs and vulnerabilities: for each reported critical vulnerability, the hacker receives a compensation



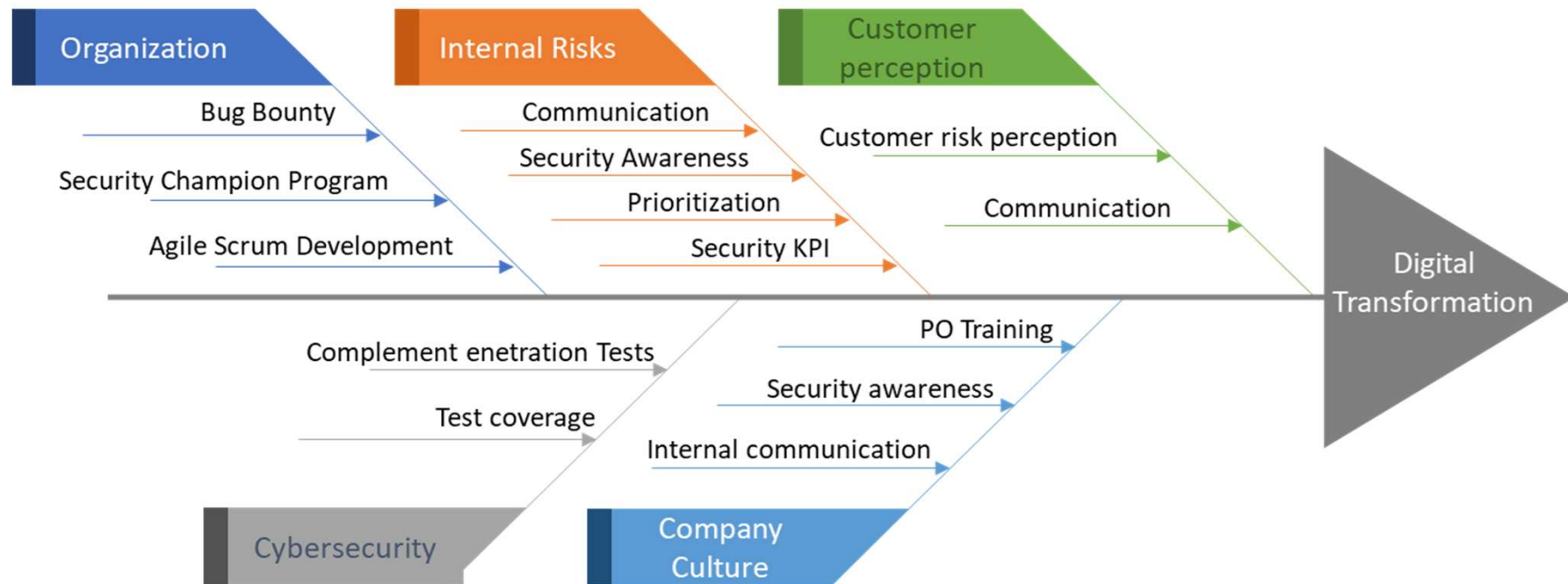
Collaborate with an external bug bounty platform

Digital Transformation

Digital transformation research survey*:

16% perceived to have successfully improved performance in the long term.

7% short-term performance improvement, not sustained.



*Malladi, S. S. & Subramanian, H. C. (2018). Bug Bounty Programs for Cyber-Security: Practices, Issues and Recommendations. DOI 10.1109/MS.2018.2880508, IEEE Software

Cybersecurity

Digital Transformation

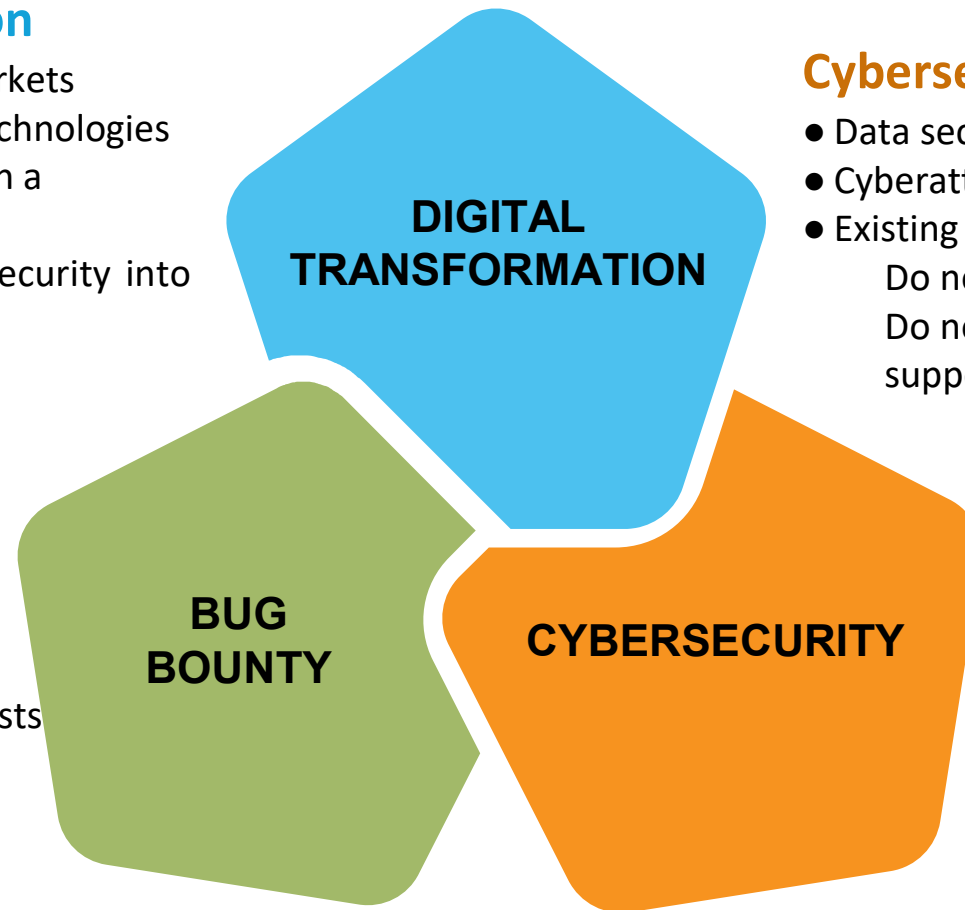
- Increasingly digitalized markets
- Exploit benefit of digital technologies
- Cyber security risks: trap in a “Digital Deadlock”
- Need to integrate cyber security into the business value chain

Cybersecurity

- Data security risks
- Cyberattacks
- Existing security models:
 - Do not keep up with the digital pace
 - Do not provide enough specialized support to developers

Bug Bounty

- Complement penetration tests and standard security tests
- Enable continuous security improvement
- Increase test coverage



Swiss Post Organization

Agile Scrum Development

- Key enabler to guarantee a fast response.
- Product Owner (PO) must be aware of the importance of the security aspect in order to prioritize them against customer features and time to market

AGILE SCRUM

Security Champions

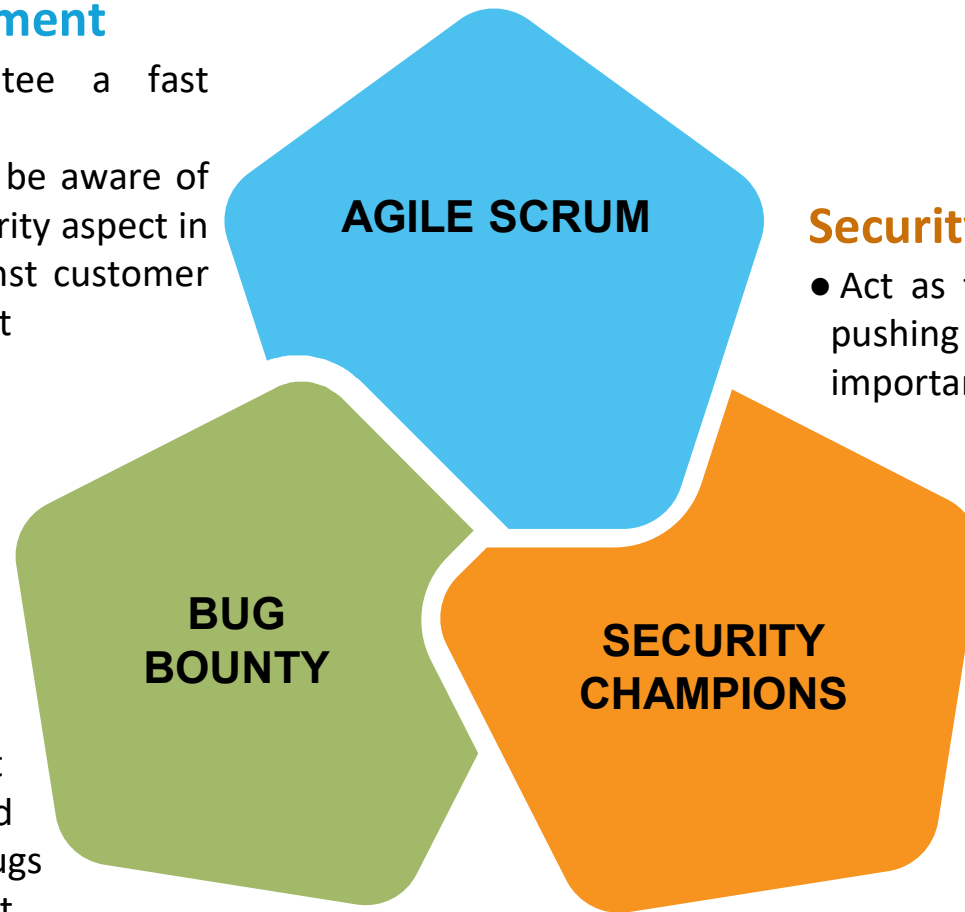
- Act as the security stakeholder pushing the right level of importance

SECURITY CHAMPIONS

BUG BOUNTY

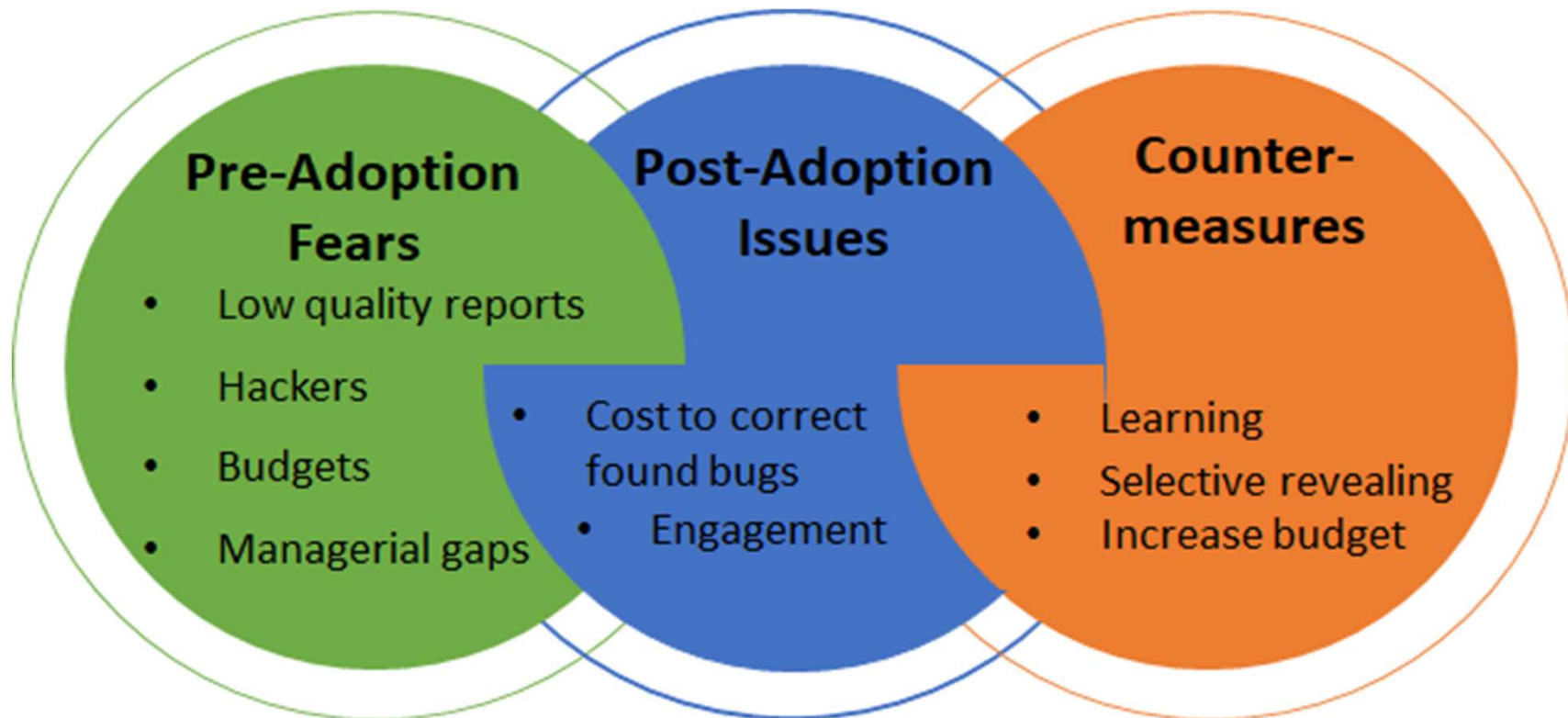
Bug Bounty

- White-hat hackers find and report the bugs to Swiss Post
- An expert evaluates them and forwards the highly critical bugs to the concerned department



Corporate Culture

Past Findings



Source: Al-Banna, M. & Benatallah, B. & Schlagwein, D. & Barukh, M. C. & Bertino, E. (2018). Friendly Hackers to the Rescue: How Organizations Perceive Crowdsourced Vulnerability Discovery in Twenty-Second Pacific Asia Conference on Information Systems, Japan

Corporate Culture

Starting with BBP at Swiss Post

Security Officers highly enthusiastic, trusting and open to the program

Swiss Post open to sharing information with white hackers from the get-go

Some differing perspectives among departments after first Bug Bounty

Corporate Culture

Lessons Learned

Beneficial to rely on third party platforms to work with white hackers

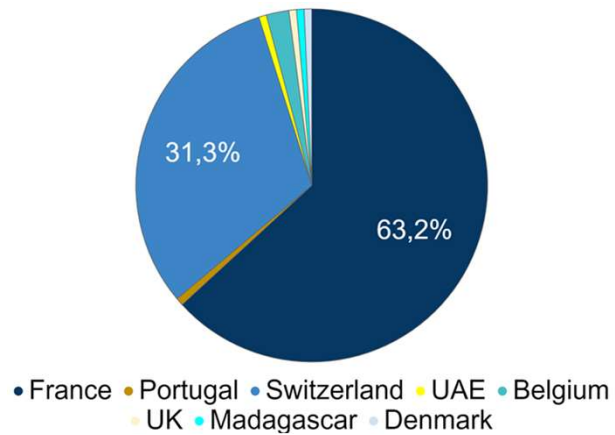
Reports were of good quality, which has helped Swiss Post learn further

Communication needs to be clear and constant, including on compensations

Customer Perception

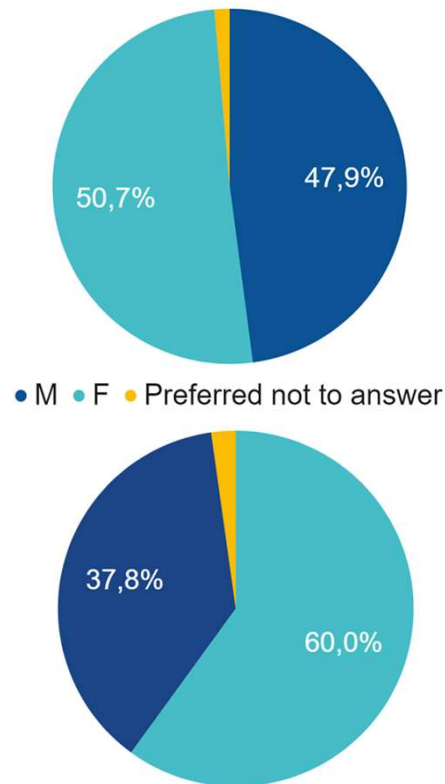
Survey Participants (144)

Residence country repartition



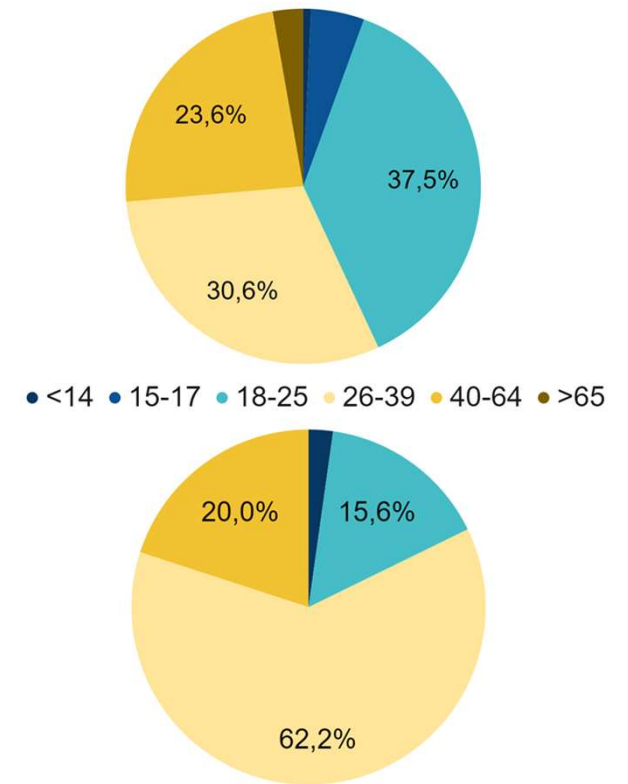
Gender distribution

(Top : total; Bottom: Switzerland)



Age distribution

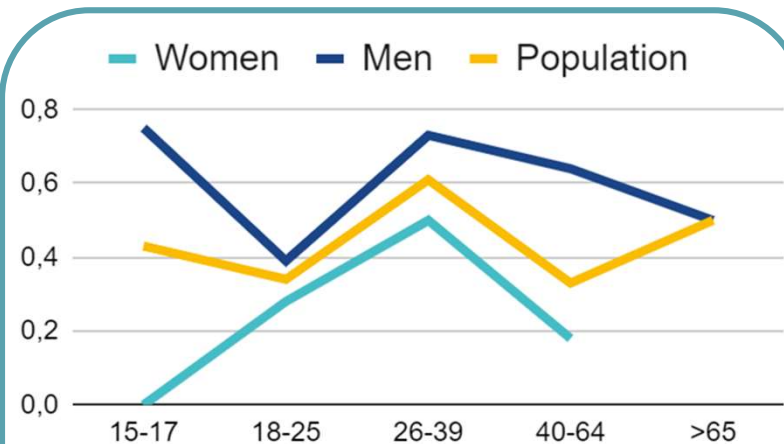
(Top : total; Bottom: Switzerland)



Customer Perception

Awareness: Gender and Age Biases

- 43.8% of the participants (55.6% in Switzerland)
- Men > Women (H: Society constructs)
- 26-39 y.o. more informed (H: BBP novelty)
- Age bias also in BBP acceptance in programmers



**Awareness of the existence of
BBP for different age subgroups**

Customer Perception

Security judgement of BBP

General Trustworthiness:

- + : 78.3 %
- ~ : 20.3 %
- - : 1.4 %

Response of Swiss Post employees:

- Risk already present
- No access to private data
- Hackers are traceable
- Use of artificial data for platforms containing sensitive data

Data privacy:

- Fear for 45.8% of the participants (CH: 35.6%)
- Risk of illegal use of customer data
- Risk of unintentional leak of data

The paradox of the efficient BBP:

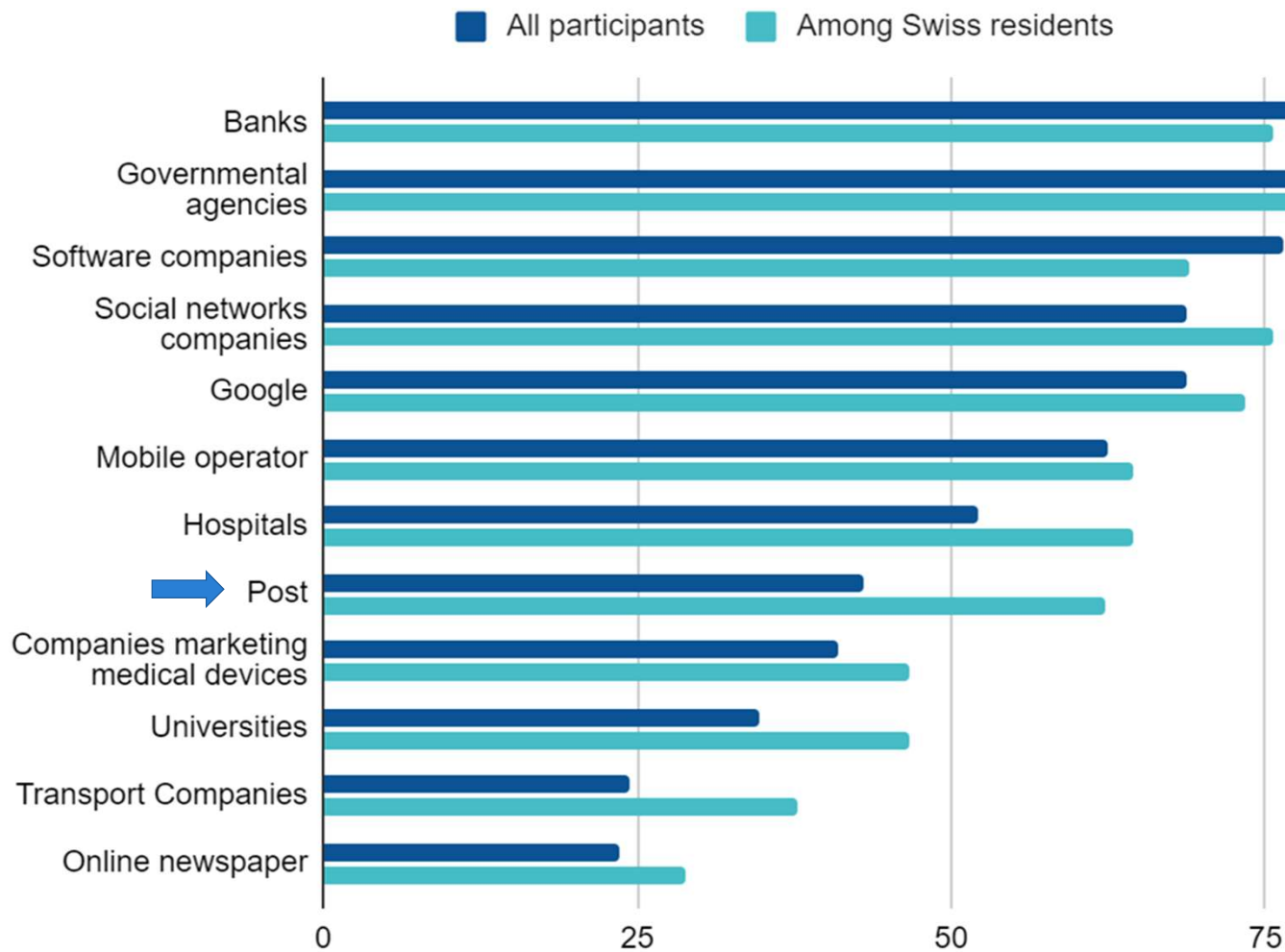
- Trust level decreases if BBP led to solving of many bugs



Informing
customers is key !

Customer Perception


Companies expected to participate in BBP



Swiss residents expect companies to take part in BBP 1.16 times more than the rest of the participants

Risk Analysis

STRENGTHS

- 1.Support from CISO
 - 2.Commitment and support from the Security Team
 - 3.Developers okay to learning from hackers
 - 4.Outsourcing to 3rd party platform
 - 5.Visibility from the BBP community
- 

Risk Analysis

RISKS

1. Fail to integrate to restructure BBP
2. Limited/Loss of top management commitment with performance indicators
3. Negative customer perception
4. Inadequate cyber-security to enable digital transformation

Risk Analysis



GAPS

1. Internal communication
2. Business Performance indicators
3. Compensation to internal staff to process BBP

Risk Analysis

RECOMMENDATIONS

- 1.Improve Internal communication
- 2.Provide more accessible and simple information for general public
- 3.Define business KPIs to access BBP performances

Conclusion

BBP needed to support cybersecurity and to enable digital transformation

Company culture needs to adapt to embrace the new challenges

Educate the public to refine their perception of the risks resulting from BBP

BUG BOUNTY AND ITS IMPACT ON SECURITY CULTURE

Background

Bug bounty programs (BBP):

Programs in which companies hire **legal hackers** to find bugs and vulnerabilities in their system. For each **reported vulnerability**, the hacker receives a **compensation**, and the company can solve the problem before it becomes the target of a cyberattack.

Bug bounty programs at Swiss Post ?

- Started at the end of 2019
- “Based” on an agile company structure and **Scrum development**
- Hackers community from “YesWeHack” **platform**
- For almost all their activities
- Still preceded by “classic” penetration Test
- No access to additional materials than the public ones

Research questions

- How does a BBP impact **digital transformation** ?
- How can BBP be used to drive **digital transformation** ?
- What are the internal implication of a BBP on the **corporate culture** ?
- What are the external implications of a BBP regarding **customer perception** and digital trust?

Methods

- **Semi-structured interviews** with 6 employees from Post’s security, IT and business development departments, as well as on **public information** of their Bug Bounty Program.
- **Public survey** (144 participants)
- **Most recent literature review on BBPs**
- Review similar programs in other companies

- Giulia Beanato
- Serina Koshy
- Andrea Betancourt
- Anaïs Bouchat

Digital Transformation

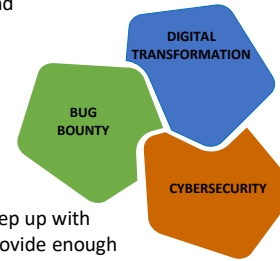
Swiss Post BBP

- Aids in **securing digital trust**
- Transformation tool to **help drive digital transformation**

- DIGITAL TRANSFORMATION**
- Increasingly digitalized market
 - Exploit the benefits of **digital technologies**
 - “Digital deadlock”
 - Need the **integration of cyber-security** into business value chain

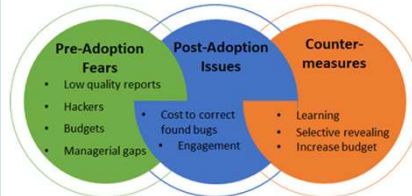
- BUG BOUNTY**
- **Complement** penetration and standard **security tests**
 - Enable **continuous security** improvement
 - Increases test coverage

- CYBERSECURITY**
- **Data security risks**
 - **Cyberattacks**
 - Existing models: i) do not keep up with the digital pace, ii) do not provide enough specialized support to developers



Corporate culture

Findings in other companies:



Post has overcome certain pre-adoption fears such as learning from **high quality reports**; relying on **third party support** to trust process and selected ‘hackers’; limiting scope and targeting different types/levels of ‘hackers’.

Post experiences some issues such as **managerial gaps** related to internal **communications** that could lead to frustration/resistance outside BBP team.

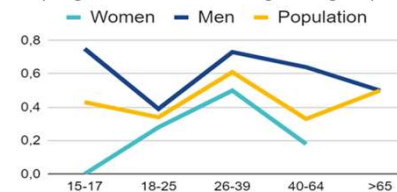
Customers perception

- **Age (26-39 y.o. most aware) and gender (M>F) bias** in **awareness** of the public of the existence of bug bounty programs
- Effect of bug bounty programs on **customers trust** for a company : **78%** ↗ ; 20% ~ ; 1,4% ↘
- 46% concerned by risks for their **data privacy** in bug bounty programs

Regarding Swiss Post:

- Only **16% aware of BBP at Swiss Post**
- 62% of Swiss residents **expect the Post to take part to a BBP**, and 93% think it **increases their security**

Awareness of the existence of bug bounty programs for different age subgroups



Risk Analysis and Risk Mitigation

STRENGTHS

- Support from CISO
- Commitment and support from the security team
- Developers open to learning from hackers
- Outsourcing to 3rd party platform
- Visibility within the BBP community

RECOMMENDATIONS

- Improve internal communication
- Provide more accessible and simple info for general public
- Define business KPIs to access BBP performances

RISKS

- Fail to restructure to integrate BBP
- Limited/loss of top management commitment without performance indicators
- Negative customer perception
- Inadequate cyber-security to enable digital transformation

GAPS

- Internal communication
- Business performance indicators
- Compensation for internal staff to process BBP

Conclusions

- Bug bounty program needed to **support cybersecurity** and to **enable digital transformation**
- Need of the **company culture** to **adapt** to embrace the new challenges.
- Necessity to **educate the public** to refine their perceptions of the risks resulting from bug bounty programs

References

- Pawaskar, S. (2019). The Cybersecurity Challenge in the Age of Digital Transformation. Vol 1, Issue 4.
- Nofal, H. (2019). The unspoken truth: The role of cybersecurity in breaking the digital transformation deadlock [White paper].
- Ali, F. A. B. H. & Dr Jali, M. Z. (2018) J. Phys.: Conf. Ser. 1018 012012
- Kaplan, J. & Richter, W. & Ware D. (2019). Cybersecurity: Linchpin of the digital enterprise. McKinsey & Company
- Malladi, S.S. & Subramanian, H. C. (2018). Bug Bounty Programs for Cyber-Security: Practices, Issues and Recommendations.
- Al-Banna, M. & Benattallah, B. & Shlagwein, D. & Barukh, M.C. & Bertino, E. (2018). Friendly Hackers to the Rescue: How Organizations Perceive Crowdsourced Vulnerability Discovery in Twenty-Second Pacific Asia Conference on Information Systems, Japan
- Maillart, T. & Zhao, M. & Grossklags, J. & Chuang, J. (2017). Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs.
- Kuehn, A. & Mueller, M. (2014). Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities [Working Paper]. TPRC Conference Paper
- Luna, D. & Allodi, L. & Cremonini, M. (2019). Productivity and Patterns of Activity in Bug Bounty Programs: Analysis of HackerOne and Google Vulnerability Research. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19), Canterbury, United Kingdom. ACM, New York, NY, USA, 10 pages.



Gender repartition of “Yes” and “No” answers to the question “Were you already aware of the existence of such programs?”

