ENHANCING VULNERABILITY MANAGEMENT FOR IOT DEVICES WITH BUG BOUNTY PROGRAMS AND RESPONSIBLE DISCLOSURE

Limon de Jesus, Gianluca

TU Delft, 2019

Enhancing Vulnerability Management for IoT Devices with Bug Bounty Programs and Responsible Disclosure

Master thesis submitted to Delft University of Technology
in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE
in Management of Technology
Faculty of Technology, Policy, and Management

by

Gianluca Limon De Jesus
Student number: 4756797

To be defended in public on August 26th, 2019

Graduation Committee

Chairperson	: Dr. M. Janssen, Section ICT, TU Delft
1st Supervisor	: Dr. A.Y. Ding, Section ICT, TU Delft
2nd Supervisor	: Dr. M.R. Alfano, Section Ethics, TU Delft
1st External Supervisor	: H. Velema, Senior Manager, Deloitte
2nd External Supervisor	: S. Seijmonson, Senior Consultant, Deloitte

This page is intentionally left blank

Executive Summary

The Internet of Things (IoT) will soon impact the lives of thousands of people as numerous IoT devices are emerging in the consumer market. Consumers goods consist of products designed for the consumption of final consumers. Even though IoT applications are expected to improve people's lives, security is often lacking in current IoT devices. Vulnerabilities in these type of products pose serious risks to the security and privacy of consumers. Compared to traditional electronics, IoT devices are endowed with internet connectivity that can be exploited by hackers in remote attacks. Several attacks on IoT products that can threaten the security of a large of number actors have already been observed. To minimize the risk of attacks, developers and vendors need to identify vulnerabilities in time before any malevolent individual can exploit them.

In recent years, as part of vulnerability management practices, many organizations have started to implement crowdsourced security methods such as Bug Bounty Programs (BBPs) and Responsible Disclosure Policies (RDPs). BBPs and RDPs are programs that involve the participation of ethical hackers in the security processes of organizations, reporting vulnerabilities to companies in exchange for monetary rewards or recognition. These methods present the benefit that thousands of hackers can work together with companies to identify and patch vulnerabilities. Empirical research suggests that BBPs and RDPs effectively augment existing vulnerability management practices by companies. However, the application of these programs in the field of IoT has never been studied.

There are many questions open regarding the potential and future adoption of Bug Bounty Programs and Responsible Disclosure Policies. The research aim is to study and expand the literature on security practices for IoT, focusing on the application of BBPs and RDPs, and to conduct an interview-based investigation with experts in order to provide practical recommendations for companies to enhance vulnerability management practices for IoT consumer goods. For this research, the literature on IoT security and security practices is confronted with empirical data from expert interviews. The empirical data was gathered during an internship at Deloitte in the Netherlands. In total, 19 interviews with cybersecurity experts from different companies in the field were collected for this thesis.

The results are employed to generate recommendations for companies to improve their vulnerability management practices with the use of BBPs and RDPs. The recommendations are directed to companies developing, manufacturing, and commercializing consumer IoT devices that want to enhance the security of their products. The main contributions of this research consist of practical and tangible security recommendations for companies to tackle IoT vulnerabilities in consumer goods, which will help enhance the overall IoT security practices. Moreover, our findings raise attention on the societal risks derived from the unsafe deployment of vulnerable IoT products into the consumer market. We create awareness on the IoT security challenge, and present a call for further actions from companies, consumers, and regulators in the IoT domain.

Keywords: IoT Security, Vulnerability Management, Bug Bounty Programs, Responsible Disclosure, Ethical Hacking, Crowdsourced Security Methods.

This Page is Intentionally Left Blank

Table of Contents

Chapter 1 – Introduction

In recent times, due to advancements in the Internet of Things (IoT), numerous IoT devices are emerging in the consumer goods market (O'Neill, M. 2016). Even though IoT is expected to improve people's lives, security is often lacking in current IoT devices. Vulnerabilities in these type of products pose serious risks to the security and privacy of consumers (McFadden et al., 2019, O'Neill, M. 2016). In order to prevent any damage to people from the use of IoT, developers and vendors have the central role to enhance the security of this type of products.

One solution to minimize the risks connected with insecure IoT products is to identify and patch vulnerabilities in time before they can be exploited. Over recent years, as part of security practices, many organizations have started to implement so-called Bug Bounty Programs (BBPs) to identify vulnerabilities. BBPs involve external security researchers, known as "ethical hackers" or "white hats", reporting vulnerabilities to companies in exchange for monetary rewards (Zhao et al., 2016). Organizations allow security researchers to perform ethical hacking on their systems to identify flaws that their internal security teams do not identify (Finifter et al., 2013). Empirical results indicate that BBPs significantly contribute to security of organizations (Zhao et al., 2017). However, at the moment, BBPs are mainly implemented to identify vulnerabilities in software applications, such as websites (HackerOne, 2018). There is very limited information regarding the adoption of BBPs to test the security of IoT. A possible obstacle to the adoption of BBPs for IoT is that hackers need to have physical access to a device to test the hardware. The need of physical proximity prevents the scalability of BBPs online as in the case of software applications.

An additional practice that involves the participation of ethical hackers identifying and reporting vulnerabilities to companies to coordinate a secure disclosure of security flaws is Responsible Disclosure Policy, known also as Responsible Disclosure (RD). RDPs, are rules and guidelines that firms establish to allow external security researchers to hack their systems without facing legal actions (Cavusoglu et al., 2005; HackerOne, 2018). In particular, RDPs are there to avoid episodes where a vulnerability is found and publicly disclosed before companies have patched the security flaw. The risk is that a malicious individual could exploit such information in the meantime. The difference between RD and BBPs is that typically RD does not involve a monetary reward or bounty (HackerOne, 2018). Both BBPs and RD are part of a particular category of Ethical Hacking, defined by Zhao et al., in 2016, as Crowdsourced Security. Crowdsourced security methods are increasingly being adopted as different studies and empirical cases effectively demonstrate their ability to augment existing security practices (Zhao et al., 2017; Gartner Inc., 2018). Moreover, several commercial crowdsourced security platforms have emerged (e.g., HackerOne, ZeroCopter, BugCrowd) and successfully facilitate the process of managing these programs for organizations, broadening the appeal of crowdsourced security (Zhao et al., 2016).

At the moment, it is not clear whether BBPs and RDPs are in use in the field of IoT, and if there are barriers for their application in this domain. In this study, we expand the literature on security practices for IoT, focusing on the application of BBPs and RDPs. Furthermore, we conduct an interview-based investigation with experts, in order to provide practical recommendations for companies to enhance vulnerability management practices for consumer IoT products. The results are used to generate recommendations to improve vulnerability management practices with the use of BBPs and RDPs. The recommendations are directed to companies developing, manufacturing, and commercializing consumer IoT devices that want to enhance the security of their products.

1.1 Problem Definition

The advent of IoT will soon impact the lives of thousands of people. By 2020, over 20 billion IoT devices are expected to be deployed worldwide (Gartner Inc., 2017, Zhang et al., 2017). In particular, the consumer segment already accounts for an estimated 60% of the total installed base of IoT devices (McFadden et al., 2019). Consumers goods consist of products bought for the consumption of final consumers rather than by companies to manufacture other goods. Compared to traditional electronics, IoT products are endowed with internet connectivity and are often part of complex networks of connected devices. In this context, insecure products can compromise the security of an entire network (Lee, & Lee, 2015). As a result, it is easier to perform scalable attacks on IoT with much serious consequences than attacks on normal devices, (Zhang et al., 2017).

There are different problems determining the general lack of IoT security. One of the reasons for the current state of security practices for IoT is the existence of a multi-actor problem. In fact, there are vendors, manufacturers, integrators, and platform suppliers establishing a value chain of different companies behind every IoT product (Höst et al., 2018). According to Pen Test Partners, 2018, most firms mistakenly assume that someone else in the supply chain addressed the product security. The same behavior is reported by Höst et al., 2018, stating that companies in advanced phases of the value chain tend to rely on product manufacturers for the identification of vulnerabilities. In the end, none of the actors in the value chain considers security. Additionally, there is a lack of guidance and industry standards among organizations to promote a secure deployment of IoT products (Pen Test Partners, 2018).

Furthermore, the majority of entrepreneurs focus on the business potential of IoT without considering the technological implications. In order to address IoT product security, firms need to have an understanding of different aspects such as hardware, firmware, APIs, and communication protocols. Frequently, companies investing into IoT, in particular startups, lack all this knowledge (Zhang et al., 2017). Nevertheless, Pen Test Partners, 2018, reports that companies still keep on developing a good business plan, forecast the cash flow, and start investing money or go to the financial market for funding. Right after, suppliers are contracted, prototypes developed, and production starts. Following some months, the new product hits the market but nobody has paid any attention to security. In this respect, a related problem is that technological, societal, and competitive pressure are all pushing enterprises to be constantly innovative. As a result, IoT applications are growing and spreading. However, the pace of innovation is not in line with the development in terms of product security (Höst et al., 2018). Competitive pressure is causing IoT products to be part of hyper-accelerated development cycles that frequently leave security unaddressed (Lee, & Lee, 2015).

As a consequence of the aforementioned problems, security practices are often lacking in current IoT deployment. The commercialization of poorly tested devices presents the risk that IoT products can be easily targeted in cyber-attacks (McFadden et al., 2019). In particular, Zhang et al., 2017, describe that IoT devices in the consumer market, present higher chances to be vulnerable compared to the industrial IoT counterparts that are usually protected by enterprise firewalls and managed by professionals. There are several cases of attacks on consumer IoT products already reported. In many cases, these attacks generate severe threats not only to the device’s owner but to third parties as well, determining a societal menace. For instance, in 2015, hackers demonstrated that they could remotely take control of a Chrysler jeep via its network-connected entertainment system, while a person was driving (O’Neill, 2016). The previous security flaw could have been used, for instance, in the case of a terroristic attacks. Moreover, vulnerable products have been exploited to compromise the security of large networks and to perform scalable attacks. In 2016, a massive attack left much of the East Coast of the United States without Internet connection. In that occasion, a hacker exploited frequently used username and passwords, set as default by developers and manufacturers, to take control of millions of CCTV cameras and routers. All the devices were connected to create an army of small computers to produce a massive Distributed Denial of Service (DDoS) attack (Fruhlinger, 2018). DDoS attacks are explained in section 2.1. The previous case demonstrates how vulnerabilities in consumer IoT can be used to perform network attacks on larger organizations and institutions. There are several other cases of dangerous attacks already reported. The risks resulting from unsafe IoT devices raise concerns about a precarious future related with IoT technology (O'Neil, 2016).

In conclusion, as companies increasingly race to get IoT devices to the market, security is often left behind, resulting in vulnerable devices that are easy targets for hackers. Several attacks have already been demonstrated. The number of attacks will increase if security is not properly addressed. Companies need to invest in security practices in order to identify vulnerabilities before attacks increase in the future. Crowdsourced security methods, in particular, Bug Bounty Programs and Responsible Disclosure, can effectively contribute to the security practices of organizations. Crowdsourced methods present the benefit that thousands of hackers work together with companies to identify vulnerabilities at a lower cost compared to conventional vulnerability identification practices, such as Pen Testing (Synax, n.d.). In particular, BBPs have proved to be highly cost-effective tools for organizations to identify and patch vulnerabilities in the software domain (Laszka et al., 2017; Finifter et al., 2013). As a result, this practice has gained increasing attention from the industry and the academic world. Nevertheless, the adoption of BBPs and RD for IoT security is still limited, and there are many questions open regarding their possible application in this field. Therefore, the aim of this research is to analyze and expand the literature on security practices for IoT, focusing on the application of BBPs and RD in order to provide practical recommendations for companies to enhance their security practices.

1.1.2 Knowledge Gaps

Theoretical research, as well as empirical work, has indicated the benefits that Crowdsourced Security can provide in the field of vulnerability management for product security. BBPs and RDPs present a remarkable potential to enhance enterprise security practices. However, the current literature of Crowdsourced Security is still very limited. In particular, research investigating how organizations can harvest the potential of crowdsourced methods for IoT security is lacking. At the moment, the following knowledge gaps exist:

- A compelling study that investigates security practices for IoT products and that identifies best practices for vulnerability management by companies is missing.
- Research investigating the adoption of crowdsourced security methods by companies in IoT is absent. In particular, the state of adoption, benefits, limitations, and barriers for the adoption of BBPs and RDPs need to be determined.

- Practical recommendations for companies to leverage BBPs and RDPs to enhance vulnerability management in IoT are also missing.

1.1.3 Problem Statement

The thesis problem statement is as following:

The pace of innovation of IoT products in the consumer market is not in line with the implementation of security measures. The insecure state of consumer IoT devices poses serious risks for the security of people and society. For this reason, developers, manufacturers, and vendors of IoT products have the central role to enhance IoT security. Crowdsource security methods have the potential to significantly contribute to current security practices for IoT. In particular, practical recommendations for organizations to leverage Bug Bounty Programs and Responsible Disclosure Policies to increase the current state of IoT security are missing.

1.2 Scientific and Practical Relevance

1.2.1 Scientific Relevance

The scientific world has identified the need to improve IoT security practices (Asplund & Nadjm-Tehrani, 2016). Initial research on BBPs and RDPs, has proved the validity of these methods as a means to enhance the vulnerability management process of companies. However, the current literature of crowdsourced security methods is still very limited, as they have only recently gained the attention of the scientific public (Kuehn & Muller, 2014). Our research continues the study of crowdsourced security and expands the current literature by investigating the possible application of BBPs and RDPs in the context of IoT security practices. In particular, the conjunction of IoT security practices and crowdsourced security methods constitutes a novel field of investigation.

1.2.2 Practical Relevance

In the near future, IoT will have a major impact on people’s lives. At the moment, security is the main concern for the successful implementation of this technology. IoT networks of connected devices will operate through automated processes while supporting sensitive data but several episodes proved the poor security of IoT devices. Companies need to invest in security practices in order to increase the security of IoT products. Crowdsourced security methods, in particular, Bug Bounty Programs and Responsible Disclosure Policies, can effectively contribute to the security practices of organizations. Our research offers important insights and recommendations for improving security practices for IoT, in particular by introducing a novel practice to test security and manage vulnerability disclosure with crowdsourced methods. Moreover, our study creates awareness on the risks resulting from the commercialization of insecure IoT products in the consumer market, and raises attention on the need to improve security for IoT.

1.2.3 Relevance to The Management of Technology

The MOT program educates students as technology managers and responsible decision makers (TU Delft, n.d.). In particular, the program covers how to deal with corporate social responsibility and how to prevent threats from the design of technology. In this respect, IoT is one of the main trends in future technology. In order to design secure IoT products, firms need to have an understanding of different technological aspects. However, the majority of entrepreneurs focus on the business potential of IoT without considering the technological implications. Moreover, firms face trade-offs between security and other business drivers, such as time-to-market, functionality, and costs, that hinder the implementation of security practices. The way in which companies will shape the design of this technology will have a major impact on people's life. The present security state of IoT products poses several risks for people, company’s reputation, and society at large. Technology managers need to consideration the implications consequent to the design of IoT products. Our research analyzes the reasons behind the current lack of IoT product security. Furthermore, recommendation for companies are defined to increase the integration of security into IoT products, in order to improve the future design of this technology.

1.3 Research Objectives and Questions

The objective of this research is to provide practical recommendations for companies to enhance vulnerability management practices for IoT consumer products. The deliverable consists of:

- Analysis on the current state of IoT security practices, including the reasons for the lack of security.
- Analyses on the possible application of Bug Bounty Programs and Responsible Disclosure Policies, including the current state of adoption, benefits, limitations, barriers and best practices.
- Practical security recommendations for companies to leverage BBPs and RDPs, in order to enhance vulnerability management practices in IoT.

We note that this study does not intend to cover all the potential causes for the lack of security practices in IoT, nor to provide an absolute solution to cure the IoT security problems. Instead, our focus is to provide practical and tangible recommendations to enhance IoT vulnerability management with crowdsourced methods, in order to augment the overall IoT security practices.

1.3.1 Main Research Question

The thesis main research question is the following:

- MRQ. How can developers, manufacturers, and vendors of consumer IoT products enhance vulnerability management practice with Bug Bounty Programs and Responsible Disclosure?

The aim of this research is to provide practical recommendations for companies to enhance security practices for consumer IoT products with crowdsourced security methods. The main research question investigates how companies can leverage on BBPs and RDPs to enhance their security practices. In particular, the answer to the main research question provides practical insights and recommendations for companies to leverage crowdsourced security methods to enhance vulnerability management.

1.3.2 Sub-Questions

- SQ1. What is the current state of security practices by developers, manufacturers, and vendors of consumer IoT products?

The answer to the first sub-question generates an overview of the current state of security practices for IoT consumer products. In particular, we focus on security practices used by companies for vulnerability management. Additionally, we investigate whether there is any difference in the security attitudes between different types of companies. The findings from this question are important to understand how BBPs and RDPs can fit and improve current security practices by organizations.

- SQ2. What are the reasons for the lack of security practices by developers, manufacturers, and vendors of consumer IoT products?

In order to understand the potential of crowdsourced security methods, we investigate the reasons determining the current lack of security in IoT products. In fact, the reasons responsible for the lack of security practices could undermine effectiveness adoption of crowdsourced methods.

- SQ3. What is the current state of Bug Bounty Programs and Responsible Disclosure in IoT, including the rate of adoption, benefits, limitations, and potential barriers?

There is very limited information regarding the adoption of RD and BBPs for IoT. For this reason, we investigate whether companies are already implementing these methods to test IoT products. Subsequently, we analyze benefits, limitations, and possible barriers for RD and BBPs in IoT. In particular, a possible obstacle to the adoption of BBPs is that hackers need to have physical access to a device to test the hardware.

- SQ4. What are the potential best practices for companies to enhance the vulnerability management of IoT products?

The answer to the fourth sub-question provides general recommendations on the best security practices that companies can follow to increase the security of IoT products. The objective is to assess whether crowdsourced security methods are considered by security experts as best practices and to understand how BBPs and RDPs can be combined with conventional security practices.

- SQ5. How can companies leverage Responsible Disclosure and integrate it with conventional security solutions to enhance the vulnerability management of IoT products?

The fifth sub-question addresses the way in which companies can adopt RD as part of vulnerability management practices. The aim is to analyze the potential of RD as a security practices for IoT and to develop practical recommendations for companies to implement such programs and integrate it with conventional security practices.

- SQ6. How can companies leverage Bug Bounty Programs and integrate them with conventional security solutions to enhance the vulnerability management of IoT products?

The last sub-question investigates the viability of adopting BBPs for testing the security of IoT products. The results from the interview-based analyses are used to generate recommendations on the best practices for companies to leverage on BBPs and integrate them with conventional security practices for IoT products.

1.4 Research Method

The thesis methodology consists of qualitative research based on literature survey and expert interviews. Chapter 3 is entirely dedicated to the presentation of the research methodology. In order to answer the research questions, the development of novel theory was needed, leading to the choice of qualitative research. The strategy to collect the data is based on semi-structured interviews with cybersecurity experts from different companies in the field.

1.4.1 Qualitative Research

In contrast with quantitative research that typically seeks causal determination, qualitative research is used to generate understanding and conclusions on uncertain phenomena (Hoepfl, 1997). Qualitative research does not have a standard structure and is commonly based on interviews and surveys methods (Smith, 2015). Limitations of these methods are that the researcher is closely involved this creates room for bias (Bouwman, 2018). In addition, findings from qualitative research lack generalizability. The thesis methodology is largely based on the Streubert and Carpenter model (1999), defining the steps of a qualitative research cycle (see Figure 1).

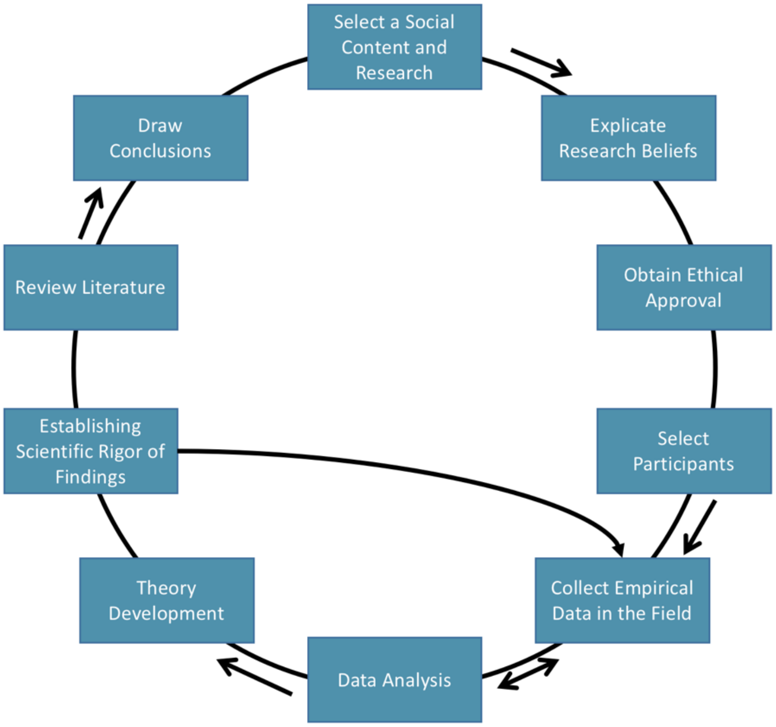

Select a Social Content and Research
Explicate Research Beliefs
Obtain Ethical Approval
Select Participants
Collect Empirical Data in the Field
Data Analysis
Theory Development
Establishing Scientific Rigor of Findings
Review Literature
Draw Conclusions

Figure 1. The Qualitative Research Cycle (Streubert, & Carpenter, 1999).

1.4.2 Expert Interviews

The data collection method consists of semi-structured interviews with experts. Many qualitative studies use semi-structured interviews with a small sample of population members to explore the diversity of perceptions and behaviors in the population (Jansen, 2010). Semi-structured interviews entail that the interviewer prepares a series of questions and lists them on a general interview plan. Typically, the structure of the questions is repeated across the interviews, however, questions might be asked to the interviewee in a different order. In addition, the list of questions might change between interviews, as additional themes become relevant or questions are left out (Höst et al., 2018)

1.4.3 Research Approach

The research approach for this thesis consisted of three main phases: Preparation, Data Collection, and Results Evaluation. Each phase incorporated different sub-stages. The preparation phase was dedicated to the development of the research proposal and to conduct the literature review. The data from the literature was then used to design the questionnaires for the semi-structured interviews during the second phase of the study. The data collected during the interviews were analyzed and evaluated in order to draw conclusions in the last phase. In the Data Collection phase, the interview protocol was derived from the literature, and the experts for the interviews were selected. After the data collection the data was coded and analyzed. In the last phase, results were evaluated and the conclusions drawn. The research approach's overview is portrayed in Figure 2.

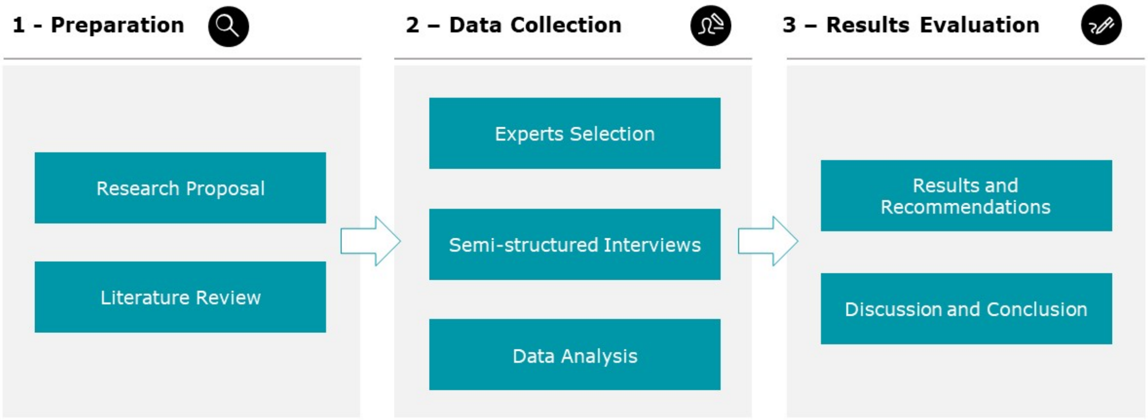


Figure 2. Research Approach.

1.4.4 Reader Guide

The report structure consists of six chapters (see Figure 3). In Chapter 1, the research topic is introduced and the research problem, objective, and questions described. Following, in Chapter 2, we present the literature review. At first, background information on IoT security is presented. Then, the literature concerning crowdsourced security methods is discussed. In Chapter 3, we cover the research methodology. In Chapter 4, the main results from the expert interviews are reported. Subsequently, in Chapter 5, the results are combined with the literature review facts to generate a research discussion. Lastly, in Chapter 6, the thesis conclusions and reflections are stated.

Chapter 1
Introduction
Chapter 2
Literature
Review
Chapter 3
Methodology
Chapter 4
Results
Chapter 5
Discussion
Chapter 6
Conclusions

Figure 3. Thesis Outline.

Chapter 2 – Literature Review

In the previous chapter we introduced the research topic. Moreover, the research problem, objectives, and questions were defined. In this chapter, we present the literature review on the main themes mentioned in the Introduction and Problem Definition sections. In particular, two are the main topic areas investigated: The IoT Security Challenge and Crowdsourced Security Methods. The scientific reports included in the literature review on The IoT Security Challenge and Crowdsourced Security were published between 2014 and 2019, and between 2005 and 2019, respectively.

Firstly, background information on IoT is presented. Following, the literature concerning the current state of vulnerable IoT devices in the consumer good market is reported. For the first sections, academic papers were mainly adopted together with some industry reports. Section 2.1, covers a portion of the literature addressing the causes behind the current lack of security practices by companies and the main problem areas. We note that this study does not intend to cover all the potential vulnerabilities in IoT nor to provide an proper analyses to the reason for the current state of IoT security practices. Instead, our focus is to provide practical recommendations to enhance the overall IoT security practices.

The main focus of our investigation is the literature addressing the intersection between Crowdsourced Security and IoT security practices. In particular, the chapter presents a comprehensive analysis on Ethical Hacking and Crowdsourced Security methods. We analyze the current studies regarding Bug Bounty Programs and Responsible Disclosure Policies. However, the academic work on these topics is still limited. For this reason, the major part of the literature on BBPs and RDPs was gathered from company reports, such as HackerOne’s. Moreover, for industry-specific insights both on IoT security and crowdsourced methods, we utilized Deloitte's research tools, including reports from Gartner and internal materials.

2.1 The Security Challenge for IoT

The Internet of Things (IoT) is recognized as one of the most important areas in future technology (Lee, & Lee, 2015; Deloitte, 2019). The term IoT envisions an extended network of Internet-connected devices interacting and exchanging data collaboratively to achieve complex applications. Deloitte, 2018, defines IoT as a suite of technologies and applications that equip and connect devices to generate information, provide instant data analysis, and accomplish smart action (Deloitte, 2018). In this respect, an IoT device can be any dedicated physical object with embedded technology, that communicates, senses, or interacts with the external environment.

- ### *Drivers for IoT Adoption*

IoT applications are rapidly growing and expanding to several fields. Gartner predicts over 20 billions internet-connected ‘things’ by 2020, resulting in approximately 3 connected devices per human on the planet (Gartner Inc., 2017). Digicert, a technology company based on digital security, identifies the main drivers behind the fast IoT expansion by defining the concept of “digital transformation wave” (Digicert, 2018). The digital transformation (DT) seeks to optimize firms’ operational performance and customer experience through IoT technologies in a way that was previously impossible for companies. Four are the major advantages that companies seek from IoT applications as presented in Figure 4.

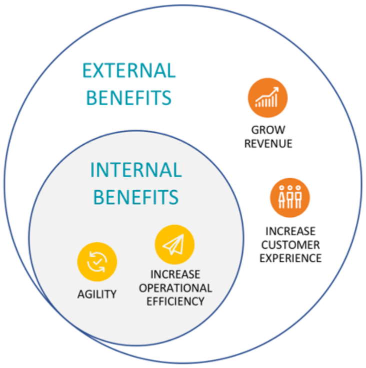
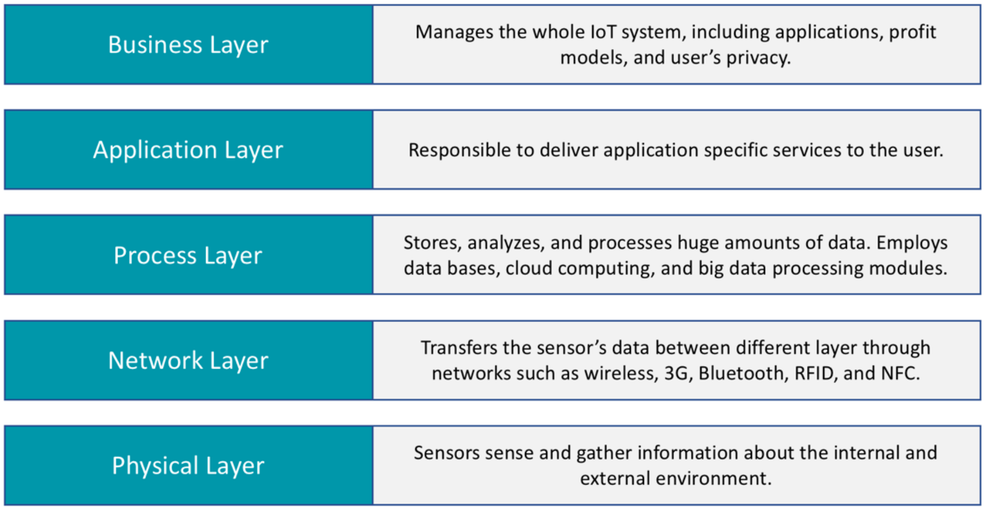


Figure 4. Drivers for the Increasing Adoption of IoT (Digicert, 2018).

The IoT Architecture

A typical IoT architecture (see Figure 5) consists of different layers including Physical Layer, Network Layer, Process Layer, Application Layer, and Business Layer (Khan et al., 2012). IoT architectures adopt different components, such as sensors, smart gateways, data centers, cloud solution, software, and user interfaces to perform complex tasks (Höst et al., 2018; Lee, & Lee, 2015). Moreover, common IoT processes include: collecting data, processing information, communicating to the cloud, and creating final applications (Pawar, & Ghumbre, 2016). As a result, an IoT architecture consists of a very complex system that involves the integration of many different components, protocols, and technologies.



Business Layer	Manages the whole IoT system, including applications, profit models, and user’s privacy.
Application Layer	Responsible to deliver application specific services to the user.
Process Layer	Stores, analyzes, and processes huge amounts of data. Employs data bases, cloud computing, and big data processing modules.
Network Layer	Transfers the sensor’s data between different layer through networks such as wireless, 3G, Bluetooth, RFID, and NFC.
Physical Layer	Sensors sense and gather information about the internal and external environment.

Figure 5. Classic IoT Architecture (Eureka!, 2018).

2.1.1 Vulnerable Devices in The Consumer Goods Sector

In this section, we present the literature concerning the security state of consumer IoT. The consumer market consists of products that are purchased by individuals for personal use rather than manufacturers to produce other goods. Examples of consumer IoT products are smart-home devices, smart phones, voice assistants, medical devices, and cars. According to Gartner, as reported by McFadden et al., 2019, consumer IoT accounts for an estimated 63% of the total installed base of IoT devices (See Figure 6). In this respect, several studies in the literature describe that the majority of consumer IoT devices lack security.

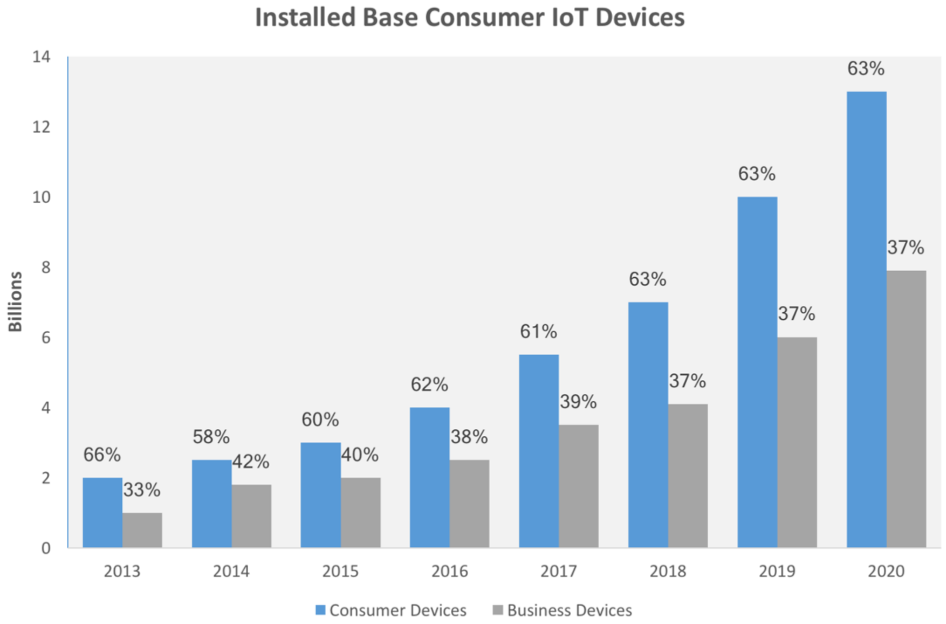


Figure 6. Installed Base of Consumer IoT Devices (McFadden et al., 2019).

Vulnerable IoT Devices

The literature indicates that security is often lacking in IoT. In 2015, Lee & Lee, found that several types of IoT devices missed essential security measures such as data encryption, secure web interfaces, firmware updates, and software protection. A study from Hewlett Packard (HP), in 2014, revealed that approximately 70% of the most commonly used consumer IoT devices, including TVs, webcams, home thermostats, door locks, and home alarms, were affected by serious vulnerabilities. HP found a total of 250 security flaws in 10 devices that were tested, with an average of 25 vulnerabilities per device. Moreover, 80% of tested devices failed to require a password with sufficient complexity, and 70% did not encrypt communication. A significantly data is that 90% of tested devices contained at least one piece of personal consumer data that could be exposed (Hewlett Packard, 2014).

Furthermore, in 2017, Zhang et al., developed a study on the severity of vulnerable IoT devices in relation with the ease of performing scalable attacks. The research describes that consumer IoT devices are more vulnerable compared to the industrial counterparts that are commonly managed by professionals and protected by enterprise firewalls. In particular, the study performs a panoramic data collection on consumer IoT attacks reported from 2010 to 2016, both in the literature and online. In total, information about 107 unique IoT attacks was collected. Among the incidents, 31 were described in academic papers, and 76 in web reports. The data set is available online and updated periodically by the authors. The results indicate that during the years the counted attacks on consumer IoT have increased from almost zero incidents reported on the web in 2010, to hundreds of episodes in 2016. The results show that the majority of the attacks during the last years were registered in the field of home automation. In particular, the number of episodes in home automation between 2014 and 2016 remained approximately constant around 15 episodes per year, whereas the attacks reported on other areas such as wearable technology, smartphones, and vehicles, decreased. The majority of attacks reported by the study might indicate that home automation is the field where products are more insecure. The research results are presented in Appendix 9.

Risks Resulting from Vulnerable IoT Devices

In 2019, McFadden et al., conducted a comprehensive study assessing the state of security on consumer IoT devices. They concluded that the recent IoT growth has been accompanied by increasing concerns about security and privacy as security is often lacking in consumer IoT devices. The exploitation of the vulnerabilities in this type of products can cause direct threats to the safety and privacy of users and third parties. In particular, insecure IoT products can be used to spread malware or launch large scale attacks (McFadden et al., 2019). As stated by O'Neill, 2016, the growing volume of network-connected IoT devices has enabled for novel attack methods and attack targets for hackers. Bertino and Islam, 2017, reported that the large number of insecure IoT devices constitutes an easy and attractive target for hackers. In particular, IoT are at higher risks of exposure for six major reasons from the system and device perspective (Bertino & Islam, 2017):

- IoT systems do not have well-defined perimeters as they can continuously change.
- IoT systems are highly heterogeneous with respect to communication medium and protocols.
- IoT systems often include devices not designed to be connected to the Internet or for being secure.
- IoT devices can often autonomously control other IoT devices without human supervision.
- IoT devices could be physically unprotected and/or controlled by different parties.
- The large number of devices increases the security complexity.

In this context, the large number of vulnerable IoT devices is attractive target to create so-called "botnets". A botnet is a network of infected devices or that are used for various malevolent purpose, such as Distributed Denial of Service (DDoS) attacks (Bertino & Islam, 2017). A DDoS is a cyber-attack meant to shut down a device or network, to prevent the access of the intended owner (Technopedia, n.d.). Moreover, the number of malware families targeting IoT has recently multiplied (Symantec, 2016). A malware is a software designed to damage or gain unauthorized access to a computer system that can be used to create botnets. In this respect, weak IoT systems are an easy target. Malware can take over IoT devices and add them to botnets. In most cases, the infection of a device might go unnoticed. Malware can propagate among different devices, such as home routers, security cameras, printers, but also industrial control systems (Bertino & Islam, 2017, Symantec, 2016). The recurrent problem with IoT products is that default passwords are almost never changed, making it easy for hackers to gain access to the device. As previously described in Chapter 1, in 2016, a massive attack left much of the East Coast of the United States without Internet connection. In that occasion, a hacker exploited frequently used username and passwords, set as default by developers and manufacturers, to take control of millions of CCTV cameras and routers. All the devices were connected to create a botnet from an army of small computers to produce a massive Distributed Denial of Service (DDoS) attack (Fruhlinger, 2018). These types of attack can cause substantial harm at a local, national, or even global scale (McFadden et al., 2019).

The Reasons for The Lack of Security

There are different studies in the literature investigating the reasons for the lack of security in IoT. In this section, we cover some of the studies about this topic. Subsequently, in Chapter 5, we expand the discussion by comparing the reasons stated by scholars with the interview results.

In 2018, Pen Test Partners, a cybersecurity services company, conducted an analyses regarding the reasons why the security of consumer IoT devices is poorly addressed. As already mentioned in Chapter 1, they identified a multi-actor problem. The cause of the problem is that there is a value chain of different companies behind every IoT product and most firms mistakenly assume that someone else in the supply chain addressed the product security. The same behavior is reported by Höst et al., 2018, stating that companies in advanced phases of the value chain tend to rely on product manufacturers for the identification of vulnerabilities. A second problem recognized by Pen Test Partners, is that the investment required for the production phase determines a very limited budget left for security. A further issue according to the company, is that once products are on the market, there are security flaws that cannot be fixed through product updates. For this reason, the products remain insecure in the hands of consumers. Additionally, there is a lack of standards and guidance for IoT security (Pen Test Partners, 2018). Lastly, Pen Test Partners reports the case of firms that simply do not consider product security.

Another comprehensive study on the security of consumer IoT products was performed by McFadden et al., in 2019. The authors conclude that weak IoT security is rooted in economic factors rather than technical ones. Specifically, they identify 3 economic factors determining the lack of security measures:

- **Asymmetric information:** Consumers are not able to recognise IoT products with good security from those with poor security. Therefore, manufacturers are not rewarded by consumers for investing in effective security measures.

- **Misaligned incentives:** The costs of an IoT device security breach are suffered by the device owner and not the manufacturer or the service provider. As a result, manufacturers do not have strong incentives to incorporate effective security in their products.

- **Externalities:** Compromised devices can be used to conduct attacks on third parties. The costs are again suffered by the attack target and not the manufacturer or the service provider.

Another problem is rooted in the lack of understanding of the technological implications of IoT. Gartner indicates that IoT security might be beyond the understanding of average IT manager's skill set (Gartner Inc., 2017). In order to address IoT product security, companies and technology managers need to have an understanding of different technical aspects such as hardware, firmware, APIs, and communication protocols. Frequently, companies investing into IoT, in particular startups, lack all this knowledge (Zhang et al., 2017). In particular, Zhang et al., 2017, point out that several IoT products are the results of an increasing number of startup companies that entered this market. According to the researchers, the vast majority of startups accounts for less than 10 employees and their obvious priority is to develop functional rather than secure products (Zhang et al., 2017).

Conclusively, according to O'Neill, 2016, companies race to get IoT products to market and do not take the time to consider the security of their devices. As reported also by Lee and Lee, 2015, there is technological, societal, and competitive pressure pushing enterprises to be constantly innovative. In this context, investing in security might be perceived as a costly and time-consuming obstacle. In particular, the literature describes that enterprises targeting end-users do not have security as a priority and are generally driven by time-to-market (Zhang et al., 2017).

2.1.2 Main Problem Areas

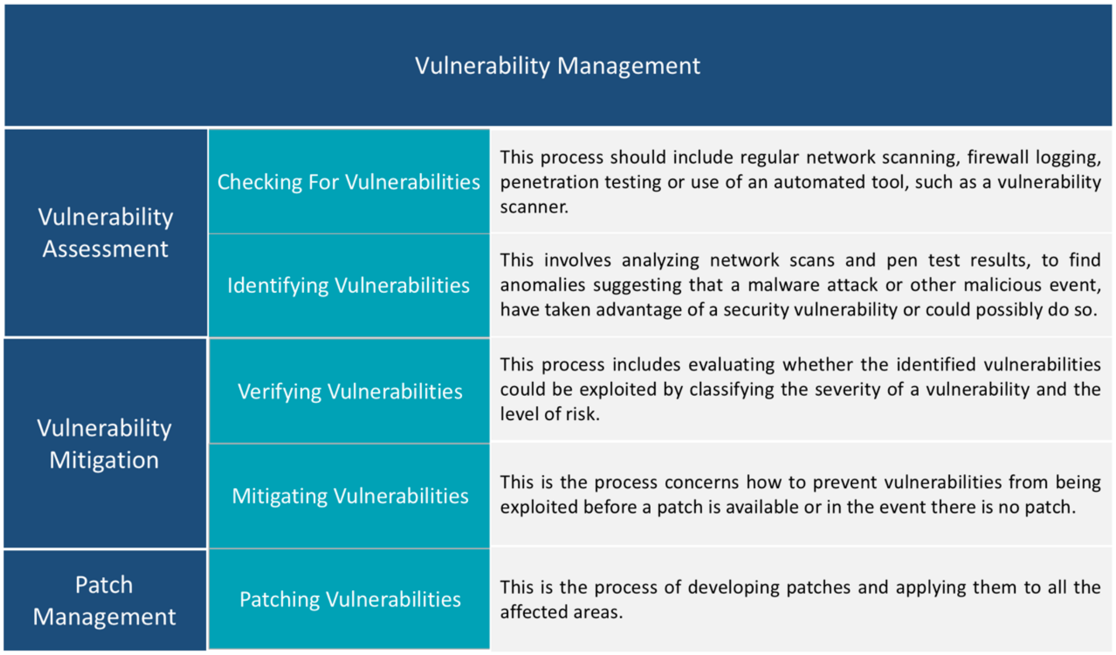
The literature presents a broad number of academic works covering the main challenges for IoT security. Typically, the main problem areas reported by scholars consist of Confidentiality, Integrity, and Availability (CIA), Access Control, Privacy, Trust, Communication, Authentication, and Implementation flaws (Mahmoud, et al., 2015; Pawar, & Ghumbre, 2016; Zhang et al., 2017). In this context, The Open Web Application Security Project (OWASP), provides a unified list concerning the principal IoT security weaknesses to consider by manufacturers, enterprises, and consumers. Table 1., describes the top ten vulnerabilities according to the OWSAP Top Ten 2018, in combination with the vulnerability impact from the OWASP Top Ten 2014.

Table 1. OWASP Top IoT Vulnerabilities (OWASP, 2018; OWASP, 2014).

Vulnerability	Security Weakness	Impact
Weak, Guessable, or Hardcoded Passwords	Use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software	Insecure credentials can grant unauthorized access to deployed systems, data loss or corruption, and can lead to complete device takeover
Insecure Network Services	Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information	Insecure network services can result in data loss or corruption, denial of service or facilitation of attacks on other devices or allow unauthorized remote control
Insecure Ecosystem Interfaces	Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the Device. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering	Insecure Ecosystem Interfaces allows the compromise of the device or its related components
Lack of Secure Update Mechanism	The lack of ability for a device to be updated presents a security weakness. This includes lack of firmware validation on the device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.	Unsecured update mechanisms could lead to compromise of user data, control over the device and attacks against other devices
Use of Insecure or Outdated Components	Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms and the use of third-party software or hardware components from a compromised supply chain	Insecure software, firmware, and hardware components could lead to compromise of user data, control over the device and attacks against other devices
Insufficient Privacy Protection	User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission	An insecure collection of personal data along with a lack of protection of that data can lead to compromise of a user's personal data
Insecure Data Transfer and Storage	Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing	Lack of transport encryption can result in data loss and could lead to the complete compromise of the device or user accounts
Lack of Device Management	Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities	Lack of Device Management prevent IT personnel to remotely manage, track, troubleshoot and secure devices
Insecure Default Settings	Devices or systems shipped with insecure default settings or lack the ability to make the the system more secure by restricting operators from modifying configurations.	Insecure default settings can result in data loss or corruption and can lead to the complete compromise of the device/user accounts
Lack of Physical Hardening	Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device	Insufficient physical security could lead to compromise of the device itself and any data stored on that device

2.2 Vulnerability Management

Vulnerability management is a pro-active approach, in the area of cybersecurity practices, with the objective of ensuring that vulnerabilities are identified and fixed across the product's lifecycle. The main phase of the vulnerability management process consists vulnerability assessment, vulnerability mitigation, and patch management. Each phase includes different steps as reported in Figure 7. In particular, insights from TechTarget and from the Deloitte cyber security capability model (see Appendix 3), were used as an inspiration to create the process overview.



Vulnerability Management		
Vulnerability Assessment	Checking For Vulnerabilities	This process should include regular network scanning, firewall logging, penetration testing or use of an automated tool, such as a vulnerability scanner.
	Identifying Vulnerabilities	This involves analyzing network scans and pen test results, to find anomalies suggesting that a malware attack or other malicious event, have taken advantage of a security vulnerability or could possibly do so.
Vulnerability Mitigation	Verifying Vulnerabilities	This process includes evaluating whether the identified vulnerabilities could be exploited by classifying the severity of a vulnerability and the level of risk.
	Mitigating Vulnerabilities	This is the process concerns how to prevent vulnerabilities from being exploited before a patch is available or in the event there is no patch.
Patch Management	Patching Vulnerabilities	This is the process of developing patches and applying them to all the affected areas.

Figure 7. The Vulnerability Management Process.

In the next sections, the main Ethical Hacking methods for vulnerability management are described. We define two categories of ethical hacking consisting of Conventional and Crowdsourced Security Methods. Among conventional methods, we cover only Pen Testing given that this is the most established method, as used widely in the IT industry. However, there are also other methods in this area, such as Red Teaming. Subsequently, we present an extensive analyses of crowdsourced security methods. In particular, we define Bug Bounty Programs and Responsible Disclosure Policies as the main crowdsource approaches. In order to avoid any confusion to the reader, we present a relation tree diagram (see Figure 8), to display the relation between the different security concepts and methods that are discussed.

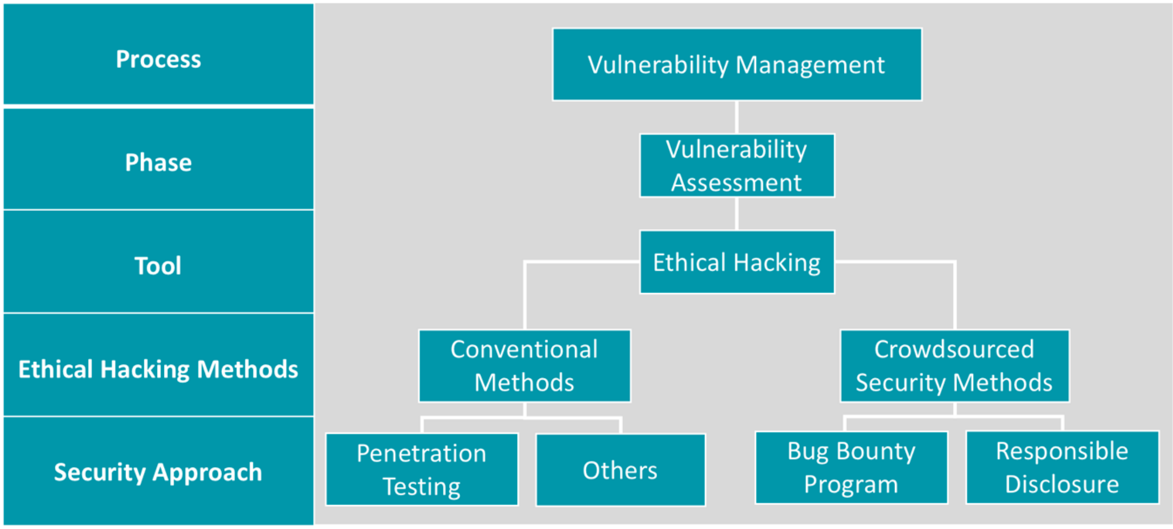


Figure 8. Ethical Hacking Methods for Vulnerability Assessment.

2.2.1 Ethical Hacking

The term hacking, refers to unauthorized intrusion into a computer or a network. Therefore, the figure of the hacker has typically a negative connotation. However, ethical hacking envisages security experts, called also “white hats” or simply “security researchers”, who attack a computer system on behalf of its owner in order to identify vulnerabilities to prevent other malicious hackers from exploiting them (Chandrika, 2014). Ethical hackers, hack without malicious intent, only to report vulnerabilities to improve the security of products and organizations. There are two main methodologies, that we cover in this research, in which companies can adopt ethical hacking: Penetration Testing and Crowdsourced Security Methods.

Chandrika, in 2014, describes that with modern technology any system, website, app, and device, that is based on internet connectivity, can potentially be hacked. Despite significant progress in software engineering practices, most often software remains insecure (Zhao et al., 2017; Choi, et al., 2010; Cavusoglu et al., 2005). The rise of cyber-crime is leading organizations to deploy hack-preventing strategies to protect their systems. In this context, governments and firms are finding in ethical hackers powerful allies to fight security threats. The following, are the main benefits of ethical hacking as identified by the EC-Council, 2019:

- Preventing data from being stolen and misused by malicious attackers.
- Discovering vulnerabilities from an attacker’s point of view to fix weak points.
- Implementing a secure network that prevents security breaches.
- Protect networks with real-world assessments.
- Gaining the trust of customers and investors by ensuring security.
- Defending national security by protecting data from terrorism.

Moreover, according to the CEO of EC-Council, “*Government agencies and business organizations today are in constant need of ethical hackers to combat the growing threat to IT security. A lot of government agencies, professionals and corporations now understand that if you want to protect a system, you cannot do it by just locking your doors*” (EC-Council, 2019).

Penetration tests

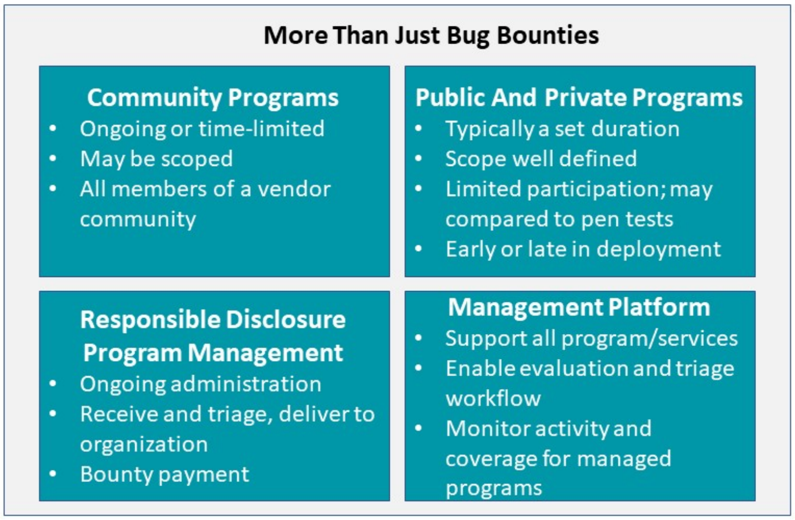
Penetration Testing, or simply Pen Test, is a subclass of ethical hacking that comprises a set of methods and procedures designed to test and protect an organization's security (Baloch, 2014). Pen tests involve different phases including the identification of entry points, attempting to break in, and reporting back the discovered security flaws (Rouse, n.d.). Pen tests are commonly adopted by companies, as part of vulnerability management practices to identify vulnerabilities. Traditional penetration tests can be performed by certified pen testing firms, independent ethical hackers, and consultants. In most cases, companies hire pen testers to perform regular hacks. However, as reported by Baloch, in 2014, penetration tests demand a great deal of money out of a company's budgets. In fact, these services are commonly paid per hour regardless of the result (Synac, n.d.). Moreover, Bugcrowd, a major commercial crowdsourced security platform, believes that pen tests alone are no longer sufficient for effective risk reduction (Bugcrowd, 2018). According to Bugcrowd’s experts, 2018, the following are the major limitations of pen testing:

- Traditional pen testing is performed by one or two pen testers, using a standardized methodology. It is unrealistic that this approach alone can find all of the vulnerabilities.
- Traditional pen tests are periodic point-in-time exercises. With today’s Agile and DevOps environment, applications are constantly changing and updating. Testing once or twice a year, results in leaving new code untested for months.
- The output of a pen test is a long report that requires companies to go through thousands of findings with little context on remediation advice.
- Pen tests are expensive.

Crowdsource Security Methods

As an alternative to Pen Testing, companies can nowadays adopt Crowdsourced Security Methods. In this research, we consider principally two methodologies of crowdsourced security: Responsible Disclosure Policies (RDPs) and Bug Bounty Programs (BBPs). These methods involve the participation of large numbers of ethical hackers, reporting vulnerabilities to companies in exchange for rewards that can consist of money or uniquely recognition. Empirical studies indicate that RDPs and BBPs effectively contribute to vulnerability management practices, and typically result in more cost-effective deals for organizations (Laszka et al., 2018; Gartner Inc., 2018; Finifter et al., 2013). Moreover, several of the main tech companies, such as Google and Facebook, are increasingly relying on these methods to enhance their security (Zhao et al., 2017). As a result, the adoption of crowdsourced methods by organizations is growing. Granter Inc., predicts that by 2022, approximately 50% of companies will employ BBPs and related services as security testing practices (Gartner Inc., 2018). In 2018, Gartner Inc. presented their first report addressing the emerging topic in technology of "Bug bounties and Crowdsourced Security Testing

Methods"(Gartner Inc., 2018). Gartner reports that crowdsourced security testing methods have confirmed their ability to effectively augment existing security testing applications. Gartner identifies at least four different categories of crowdsourced security methods (see figure 9), that are extensively presented in Appendix 8. Community Programs and Public and Private Programs, refer both to BBPs applications. Responsible Disclosure is a category on its own. Management Platforms can be used to manage both BBPs and RDPs.



More Than Just Bug Bounties

Community Programs
- Ongoing or time-limited
- May be scoped
- All members of a vendor community

Public And Private Programs
- Typically a set duration
- Scope well defined
- Limited participation; may compared to pen tests
- Early or late in deployment

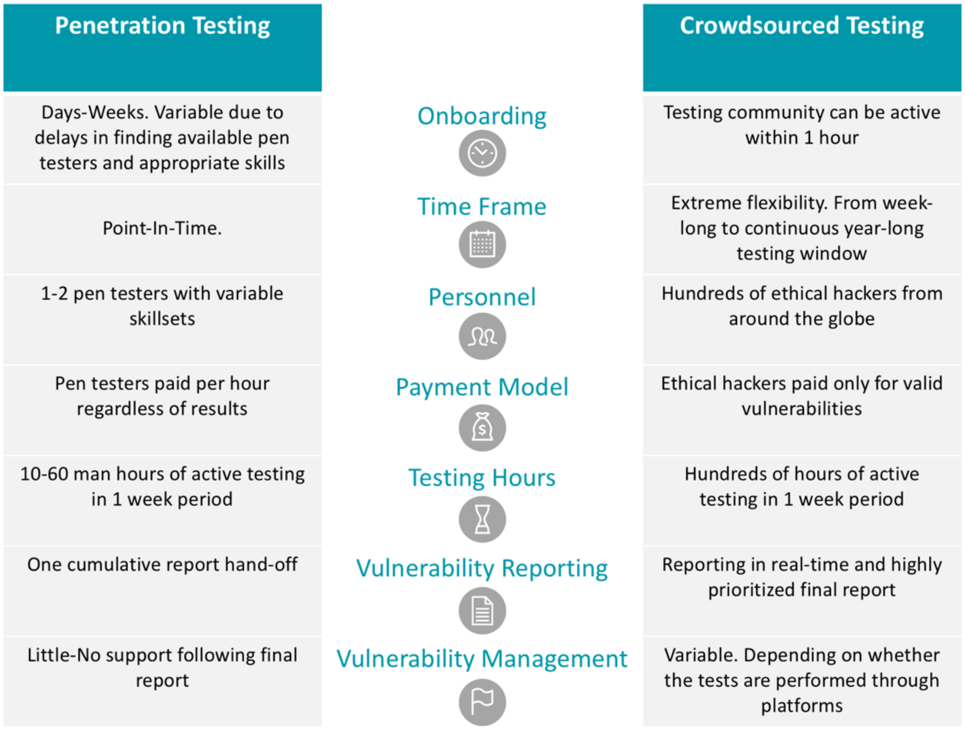
Responsible Disclosure Program Management
- Ongoing administration
- Receive and triage, deliver to organization
- Bounty payment

Management Platform
- Support all program/services
- Enable evaluation and triage workflow
- Monitor activity and coverage for managed programs

Figure 9. Crowdsourced Security Testing Methods (Gartner Inc., 2018).

Comparing Penetration Testing and Crowdsourced Security Methods

In this section, we present a comparison of pen tests and crowdsourced methods based on the literature. Penetration tests consist of one or two people conducting security tests for a limited period of time, at the expense of a fixed cost. Crowdsourced methods, allow potentially thousands of hackers working on a security target (Gartner Inc., 2019). As reported by Laszka et al., 2018, Edmundson et al., in 2013, conducted an experiment where security researchers were requested to identify a series of security vulnerabilities present in a code. The results indicated that none of the participant was able to accomplish this task alone. However, when the researchers collected a random sample of 50% of the participants, the probability of finding all of the security flaws increased to 95%. As a result, security researchers cooperating together have increased chances to identify vulnerabilities. For this reason, Bugcrowd, believes that BBPs and RDPs introduce a more effective and efficient way to identify and manage vulnerabilities (Bugcrowd, 2018). Moreover, instead of a point-in-time test, crowdsourced methods enable continuous testing. A further difference is that conversely to pen tests, hackers are only paid the moment that a valid vulnerability is reported. The benefits of crowdsourced methods over conventional pen tests, are presented in Figure 10.



Penetration Testing		Crowdsourced Testing
Days-Weeks. Variable due to delays in finding available pen testers and appropriate skills	Onboarding	Testing community can be active within 1 hour
Point-In-Time.	Time Frame	Extreme flexibility. From week-long to continuous year-long testing window
1-2 pen testers with variable skillsets	Personnel	Hundreds of ethical hackers from around the globe
Pen testers paid per hour regardless of results	Payment Model	Ethical hackers paid only for valid vulnerabilities
10-60 man hours of active testing in 1 week period	Testing Hours	Hundreds of hours of active testing in 1 week period
One cumulative report hand-off	Vulnerability Reporting	Reporting in real-time and highly prioritized final report
Little-No support following final report	Vulnerability Management	Variable. Depending on whether the tests are performed through platforms

Figure 10. Comparing Traditional Pen Testing with Crowdsourced Methods (Synax, n.d.).

2.3 Crowdsource Security Methods

In this section, the literature on Responsible Disclosure Policies and Bug Bounty Programs is presented. In particular, the academic work on these topics is still very limited. For this reason, the majority of the literature, specially concerning RDPs, was gathered from company reports.

2.3.1 Responsible Disclosure Policies

Responsible Disclosure Policies (RDPs), known also as Coordinated Vulnerability Disclosure (CPD) or simply Responsible Disclosure (RD), consist of rules and guidelines from companies that allow individuals to report vulnerabilities to organizations (Hackerone, 2018). In particular, they provide clear guidelines on how to report a potential security flaws to companies and set a procedure for a controlled and responsible disclosure of vulnerabilities. Cavusoglu et al., 2005, described that most of the software vulnerabilities are typically discovered by benign users. In this context, individuals might feel responsible for reporting the vulnerability to the vulnerability owner organization. However, several times, companies lack a dedicated channel for individuals to report vulnerabilities. According to HackerOne, 2018, in such situation, three different events might happen:

- **Failed disclosure:** After looking for and not finding an appropriate contact, the hacker gives up. As a result, the vulnerability is not reported and remains. HackerOne, 2018, indicates that approximately 1 in 4 of discovered vulnerabilities are not reported by hackers because companies lack a RDP.
- **Vulnerability is reported but information is lost:** Even in the cases where a vulnerability is correctly reported, the information can get lost. Firms that have multiple contact points, including customer support lines, emails, and social media pages, and lack a RDP, can very easy lose track of a reported vulnerability. Eventually, only in some cases the security team will be informed about the vulnerability.
- **Full disclosure:** After looking for and not finding an appropriate contact, the hacker will release the information publicly online without coordinating with the company. Besides the reputational repercussion for the company, there is the risk that malicious hackers exploit the vulnerability to cause damage before the company is able to release a patch.

Consequently, without a RDP, reporting vulnerabilities might result in a very complex process both for ethical hackers and companies (see Figure 11).

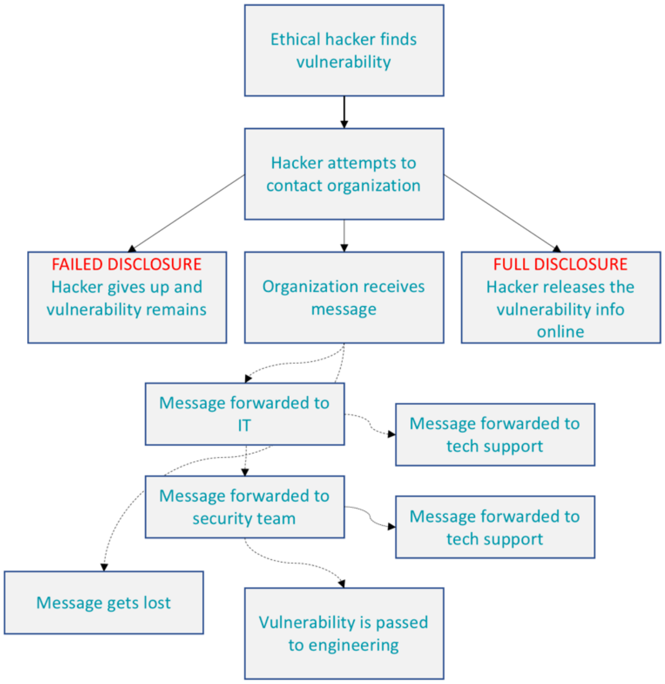

Ethical hacker finds vulnerability
Hacker attempts to contact organization
FAILED DISCLOSURE
Hacker gives up and vulnerability remains
Organization receives message
FULL DISCLOSURE
Hacker releases the vulnerability info online
Message forwarded to IT
Message forwarded to tech support
Message forwarded to security team
Message forwarded to tech support
Message gets lost
Vulnerability is passed to engineering

Figure 11. The Chaotic Process of Reporting a Vulnerability Without a RDP (Hackerone, 2018).

Benefits of Responsible Disclosure Policies

In other to solve the aforementioned issue, organizations had to create a safe channel to coordinate with ethical hackers. As a consequence, companies started to provide rules for submitting vulnerabilities to their security team, and to allocate resources to follow the process (HackerOne, 2018). Due to RDPs firms benefit from nearly free advice of ethical hackers to enhance their security. RDPs effectively improve the vulnerability management process of reported vulnerabilities. The improved process with a RDP compared to the case of Figure 11, is shown in Figure 12.

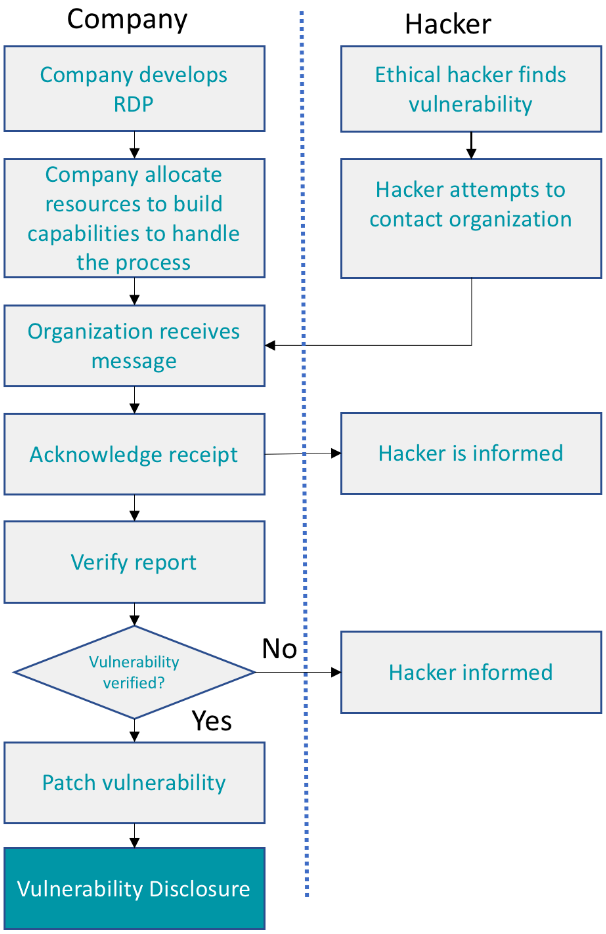

Company
Hacker
Company develops RDP
Company allocate resources to build capabilities to handle the process
Organization receives message
Acknowledge receipt
Verify report
Vulnerability verified?
No
Yes
Patch vulnerability
Vulnerability Disclosure
Ethical hacker finds vulnerability
Hacker attempts to contact organization
Hacker is informed
Hacker informed

Figure 12. Responsible Disclosure Process Flow (Hackerone, 2018).

A responsible disclosure process results in an easy win both for companies and researchers. According to Bugcrowd, n.d., a responsible disclosure policy is the first step from companies to protect themselves from an attack and from the premature release of vulnerability to the public. HackerOne, 2018, claims that no organization is too small or too large to benefit from a RDP. Moreover, a RDPs are easy to set up and cheap relatively to maintain. The simplest versions require only of an online page that states what type of security flaws are within the testing scope and a dedicated contact address to report the findings (Bugcrowd, n.d.). In most cases, companies do not pay any monetary reward to researcher for their assistance but provide them with a token of appreciation or public recognition. On the other hand, a benefit for ethical hackers is that RDPs should protect researchers from companies' legal actions for breaking the security of their systems. For this reason, it is important for organizations to include a declaration to reassure ethical hackers that, when acting in good faith, there will be no legal action against them (Hackerone, 2018).

Rate of Adoption of Responsible Disclosure Policies

Even though RDPs has the potential to improve organizations' security practices, the data collected presents that RDPs are implemented by very few organizations. Every year, HackerOne realizes a survey study to investigate the adoption of RDPs among the Forbes Global 2000 List, covering the world's most valuable public companies. The results from 2017, indicate that 93% of organizations do not have any public RDP, or any channel to report vulnerabilities (Hackerone, 2018). Therefore, only 7% of the sample seemed to adopt RDPs. From this data, we deduce that the rate of adoption of RDPs among companies is still very limited. Moreover, HackerOne, in 2018, published a report presenting the current state of policies to support the adoption of RDP in EU member states. The results, present that very few countries have an advanced state of policies for RDP as depicted in Figure 13 (Hackerone, 2018). According to the report, The Netherlands was the first country to activate policies to support RDPs. The Dutch policies offer full protection to hackers, while for instance France, offers only limited protection to researchers. Ten other EU countries are developing some kind of policy. All the other countries have little or absent national related activity on RDPs.

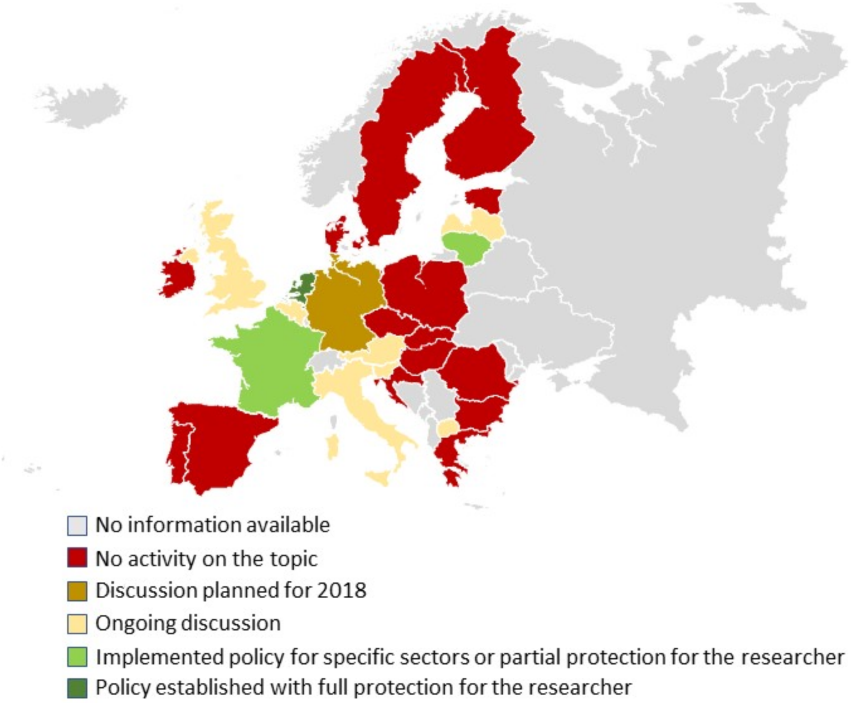

⬜ No information available
🟥 No activity on the topic
🟫 Discussion planned for 2018
🟨 Ongoing discussion
🟩 Implemented policy for specific sectors or partial protection for the researcher
🟩 Policy established with full protection for the researcher

Figure 13. RDP Policies in Europe: A Mapping of the State of Play by Country (HackerOne, 2018).

2.3.2 Bug Bounty Programs

Bug Bounty Programs (BBPs), known also as Bug Bounties, are crowdsourced security testing programs that monetarily reward ethical hackers who successfully discover and report vulnerabilities to companies (Zhao et al., 2016). Organizations offer bounties to enhance vulnerability management, and to prevent zero-day vulnerabilities (Finifter et al., 2013). Research upon BBPs has been conducting only recently, companies, such as Google, started adopting them in 2010 (Kuehn & Mueller, 2014; Finifter et al., 2013).

Previously to that period, in 2008, Just et al., conducted research on software vulnerability tracking, suggesting the importance of rewarding researchers that were communicating vulnerabilities to companies. Moreover, the study suggested the idea of introducing researcher's reputation as part of vulnerability tracking programs, and to provide tools and rules for reporting bugs in a structured way (Just et al., 2008). All of the prior elements are now fundamentals of BBPs.

There are two different approaches to Bug bounties: Public and Private programs (Gartner Inc., 2018; Zhao et al., 2017; Laszka et al., 2018). Public programs essential allow entire communities of ethical hackers to participate. They typically consist of large scale BBPs and can be both time-limited or ongoing. Organizations such as Facebook and Google, typically allow everyone to participate (Zhao et al., 2017). On the other hand, Private programs are invite only a selected sub-group of hackers, are generally scoped to specific targets, and are limited in time (Gartner Inc., 2018). Private programs tend to take place through commercial bug bounty platforms where hackers are selected based on reputation, skills, and experience. According to Zhao et al., 2017, private BBPs have a much higher percentage to provide valid reports.

Moreover, companies can decide to launch independent BBPs, or to rely on the services of commercial bug bounty platforms that facilitate the process of building and maintaining BBPs for organizations (Laszka et al., 2016, Zhao et al., 2016). Commercial platforms are becoming critical components for RDPs and BBPs, as they match the security services of ethical hackers with the demand of organizations. Typical features of these platforms include: tracking the progress of researchers, assessing code coverage, controlling the program's scope, handle financial transactions, serving as a point of contact for conflicts between white hackers and companies or even law enforcement, and providing real-time information on the stratus of discovered vulnerabilities to both researchers and companies (Laszka et al., 2018; Gartner Inc, 2018). Platforms also allow companies for the selection of skillful individuals for Private BBPs based on rankings Zhao et al., 2017. In this respect, scholars have tried to define the main differences between independent and platform based BBPs. Zhao et al., 2017, found that BBPs hosted on platforms have a higher rate of valid reports due to better identification practices for participants, that can be used for quality-control policies.

Lastly, we present all the possible approaches identified from the previous literature for BBPs in the following table:

Table 2. Overview of the Possible Approaches for BBPs.

	Public Programs	Private Programs
Independent	Public and Independent	Private and Independent
Platform-Based	Public and Platform-Based	Private and Platform-Based

Bug Bounty Programs and Responsible Disclosure

BBPs present numerous elements in common with Responsible disclosure. The main difference between the two is that BBPs constitute an actual invite from companies to hackers to hack their systems in exchange for monetary rewards. RDPs are not proactive invites for researchers to hack, but are rather there to coordinate the disclosure of security flaws that ethical hackers might identify independently. Moreover, RDPs do not generally offer monetary rewards to hackers (Bacchus, 2017). BBPs and RDPs, today, allow hackers to report vulnerabilities in a regulated manner to companies. Moreover, emerging platforms, such as HackerOne or ZeroCopter, is boosting the adoption of crowdsourced security services (Zhao et al., 2016)

Benefits and Limitations of Bug Bounty Platforms

There are different benefits that BBPs offer to companies to enhance security. In particular, the advantages of crowdsourced security over pen testing previously presented in section 2.2.1 apply to BBPs. Finifter et al., 2013, suggested that BBPs are a more costed-effective method to identify vulnerabilities compared to conventional methods. Moreover, BBPs have the advantage of engaging with broad communities of hackers resulting in greater chances to discover different types of vulnerabilities given the disperse skillset of the participants (Finifter et al., 2013). The previous result was demonstrated by Edmundson et al., 2013, with an experiment where security researchers were requested to identify a series of vulnerabilities in a code. None of the participant was able to accomplish the task alone. However, when the researchers collected a random sample of 50% of the participants, the probability of discovering all of the security flaws increased to 95% (Laszka et al., 2018). Further empirical research describes that hackers experience increasing difficulties to find vulnerabilities in companies participating in BBPs, suggesting that BBPs effectively contribute to increase security (Zhao et al., 2017).

While empirical results present that BBBs have a significant potential to contribute to security, there are also several obstacles for companies in running these programs. In particular, the key challenge for companies is presented by a substantial number of invalid reports submitted by of hackers. Research describes that there is abundant noise that companies need to manage resulting from low-value reports (Lazka et al., 2016). In 2018, Laszka et al. presented that the percentage of invalid reports commonly ranged between 35% and 55%. Another challenge consists of efficiently distribute valuable but scarce hacker effort across organizations over time. Multiple hackers taking part into BBPs partially compete with each other resulting in duplicate reports of same vulnerabilities. However, in those cases, only the first submission is rewarded. BugCrowd, in 2015, described that approximately 40% of the submissions were duplicates.

Rate of Adoption of Bug Bounty Programs

In recent years, Bug Bounty Programs are becoming a significant part of organizations' security ecosystem. Companies are increasingly launching independent BBPs or are joining platforms that facilitate the management of these programs (Laszka, et al., 2016). Even institutions, including the U.S. Department of Defense and the European Commission, are adopting BBPs to enhance their security (Finifter et al., 2013; Hackerone, 2019). According to Gartner Inc., 2018, BBPs have demonstrated their ability to effectively augment existing security testing activities and support the effective management of vulnerabilities. In addition, commercial crowdsourced security platforms, such as HackerOne and Bugcrowd, are promoting the adoption of BBPs (Laszka et al., 2016; Zhao et al., 2017; Finifter et al., 2013). Gartner Inc., predicts that by 2022, BBPs and crowdsourced methods will be employed by more than 50% of enterprises up from less than 5% today (Gartner Inc., 2018). However, the majority of the current bug bounties is directed towards website vulnerabilities, and more in general software applications (HackerOne, 2018). According to data collected by HackerOne, 2018, less than 2% of the hackers registered on their platform research security flaws in IoT (see Figure 14). From this data, we conclude that the rate of adoption of BBPs for IoT devices is marginal.

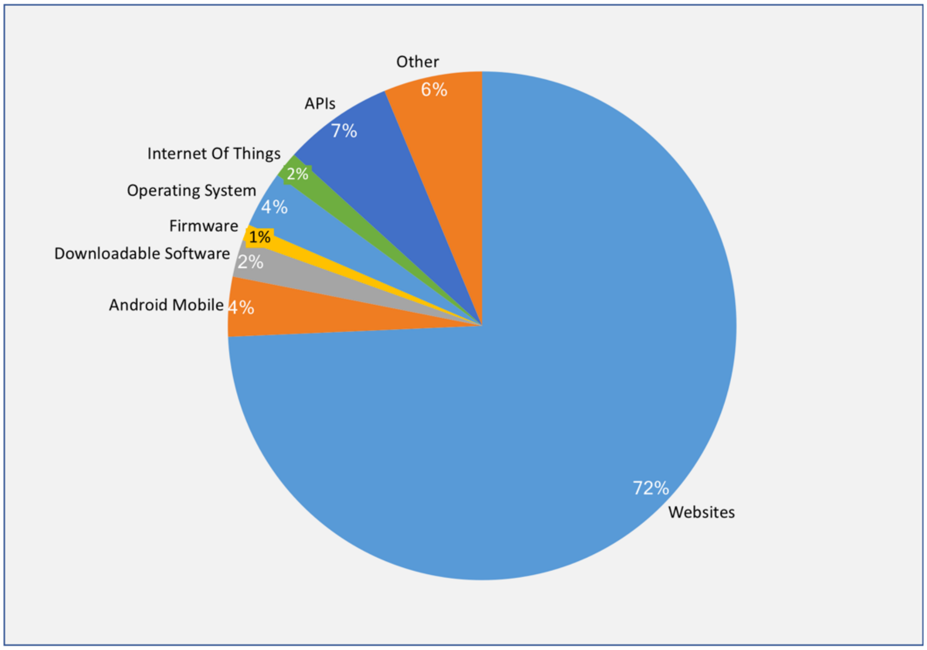


Figure 14. What Hackers on HackerOne Hack for Bounties (HackerOne, 2018).

Best Practices for Bug Bounty Programs

In 2017, HackerOne, presented the "Bug Bounty Field Manual", a report that describes how to plan, launch, and operate a successful BBP (Bacchus, 2017). In this respect, the crowdsource security company advises organizations to follow a five stage process for BBPs:

- **Assessment:** Companies need to assess the bug bounty approach that is best according to their capabilities. HackerOne offers an assessment questionnaire to help companies in this step. Moreover, before starting a BBP, companies should already be active with vulnerability management practices to ensure that a sufficient amount of vulnerabilities have been previously identified and fixed.

- **Preparation:** Companies stating a BBP will have more vulnerabilities to manage. For this reason, organizations need to ensure a solid process to evaluate and fix the vulnerabilities. At the same time, they have to allocate sufficient resources to support the ongoing program.

- **Champion Internally:** Companies need to define a BBP leader that will be responsible for the success of the program. Together with the leader, the company has to create a bug bounty team to take charge of related processes.

- **Launch:** Before launching the program, companies have to consider whether they want to offer a public or private program. Subsequently, the company has to define the scope of the program. The advice for organizations new to BBPs, is to start with small programs. Moreover, it has to be decided whether to adopt the assistance of a platform or launch an independent BBP.

- **The Post Bounty:** Once the company has been able to successfully manage the first BBP, the next step is to scale up. This entails more hackers, a broader scope, and increasing rewards. It might seem counterintuitive but organizations should aim to find more vulnerabilities to reach overtime almost complete coverage. In addition, security only improves when bugs are fixed, not when they are found. For this reason, it is important for companies to identify the internal vulnerability owner that can provide a solution to the vulnerability.

2.4 Chapter Conclusion

Vulnerable IoT products that support sensitive data from individuals are becoming lucrative targets for hackers that seek to steal such information or to perform network attacks. Under these conditions, attacks on IoT systems can result in major safety risks. In particular, the literature indicates that insecure IoT products can be used to spread malware or launch large scale attacks. There are different studies investigating the reasons for the lack of security in IoT. Among the main reasons, research reports the presence of a multi-actor problem due to the involvement of several firms in the value chains for IoT products, where firms mistakenly assume that someone else in the supply chain addressed the product security. Another major problem is rooted in the lack of understanding of the technological implications of IoT by companies. In this context, the rise of cyber-crime is leading organizations to deploy hack-preventing strategies to protect their systems.

In order to boos security, firms and governments are finding in Ethical Hacking a powerful tool to fight security threats. Ethical hacking envisages security experts who attack a computer system on behalf of its owner, in order to identify vulnerabilities. In particular, our investigation focused on Crowdsourced Security Methods. Specifically, we examined the literature regarding two main methodologies of crowdsourced security: Responsible Disclosure Policies (RDPs) and Bug Bounty Programs (BBPs). These methods involve the participation of large numbers of ethical hackers, reporting vulnerabilities to companies in exchange for rewards that can consist of money or uniquely recognition. The academic work on these topics is still limited. For this reason, the majority of the literature that we analyzed regarding RDPs and BBPs originated from company reports. Empirical studies indicate that RDPs and BBPs effectively contribute to vulnerability management practices, and typically result in more cost-effective deals for organizations. Moreover, crowdsourced methods have the advantage of engaging with broad communities of hackers resulting in greater chances to discover different types of vulnerabilities given the disperse skillset of the participants. However, even though BBPs and RDPs have a remarkable potential to improve vulnerability management, few companies are implementing these methods. Additionally, the data depicts that less than 2% of hackers participating in BBPs research security flaws in IoT.

From the literature analyses, we concluded that the research concerning the adoption of crowdsource security methods for IoT is still scarce. In particular, the state of adoption, benefits, limitations, and barriers for adopting BBP and RDPs in IoT needs to be further investigated. In the following chapters, we dive into this yet unexplored area, by carrying out a qualitative investigation to explore how to apply crowdsource methods for improving IoT vulnerability management. The next chapter covers the research methodology for our study.

Chapter 3 – Research Methodology

The objective of this research is to investigate a possible application of crowdsourced security methods to derive recommendations for enhancing the vulnerability management of IoT. However, based on our extensive literature review, there are insufficient studies on this subject. For this reason, we decided to conduct an exploratory research based on a qualitative approach. Qualitative research seeks for understanding of new phenomenon and it is generally used to generate possible conclusions and theories (Hoepfl, 1997). In this chapter, we present the research methodology that was adopted as part of our investigation to collect and analyze the data. Given the exploratory nature of this study, our research consists of extensive literature survey (covered in the previous chapter) and semi-structured interviews with industry experts.

3.1 Semi-Structured Interviews

Qualitative research does not have a standard structure. Frequently, this types of study are based on interviews and surveys methods (Smith, 2015). In particular, many qualitative studies use semi-structured interviews with a small sample of population members to explore the diversity of perceptions or behaviors in a population (Jansen, 2010). Semi-structured type of interviews inquires a series of prepared questions listed on a general interview plan (see Appendix 1 for our interview guide). The structure of the questions is typically repeated across the interviews, but questions might also be asked in a different order. In addition, the list of questions might change between interviews as additional themes become relevant to be asked or questions are left out (Höst et al., 2018). The final intent of semi-structured interviews is that all questions should be asked and framed in similar terms. The reason is to allow a cohesive set of data to emerge to be compared in the data analysis. However, in the semi-structured interview method the researcher is closely involved with participants, and this can alter the objectivity of the data (Bouwman, 2018). For this reason, findings from this type of research tend to lack generalizability. In order to reduce the risk of data contamination for this study, we repeated the same structure across the interviews. Moreover, we recorded the interview answers to preserve the original information for the data analyses.

3.2 Data Collection

In this section, we describe the data collection methodology. Our study is based on two types of data. Descriptive data, gathered with desk research for the literature survey, and empirical data, derived from semi-structured interviews with industry experts.

3.2.1 Desk Research

Desk research was conducted to gather the descriptive data for the literature survey. In particular, the collected data was clustered into two main categories: The IoT Security Challenge and Crowdsourced Security Methods. Most of the academic papers for this study were found with the Google Scholar search engine. For industry-specific insights both on IoT security and crowdsourced security, we utilized Deloitte's research tools, including internal material and reports from Gartner. In addition, the data was complemented with material from a wide range of other sources including company reports, online articles, and videos. The scientific reports included in the literature review on The IoT Security Challenge and Crowdsourced Security were published between 2014 and 2019, and between 2005 and 2019, respectively.

The desk research process was carried out with human inspection. At first, we focused on articles published by scholars on IoT security. Filters were adopted to perform specific queries on the search engine. Keywords associated with our research corresponded to IoT security, IoT security challenges, IoT security measures, and IoT and crowdsourcing. As a next step, we identified the most relevant papers on security challenges and practices, and excluded the others. Regarding the data addressing real case examples of vulnerable IoT devices, we included a large number of online reports by security firms and security blogs. For the literature on crowdsourced security, we acknowledged that there is a limited number of academic work addressing this subject. In particular, scientific investigation on RDPs is scarce. We included in our analyses the majority of the academic papers currently published on RDPs and BBPs, and we further complemented this data with reports released by cybersecurity companies, in particular, HackerOne and BugCrowd.

3.2.2 Expert Interviews

The main results of this research are based on the data gathered from expert interviews that were conducted during an internship period at Deloitte in the Netherlands. The data collection methodology described in this section was used to gather empirical data to answer the thesis research questions.

- *Interview Protocol*

In order answer to the research questions, we collected the opinion of cybersecurity experts in the field of IoT security hacking and ethical hacking practices, including crowdsourced methods. During a preparation phase, earlier to the expert selection, an interview protocol was developed including the interview questionnaire. The questions are divided similarly to the literature review, in two categories, covering IoT security practices and ethical hacking methods for vulnerability management in IoT. In particular, the interview protocol was inspired by the survey design of two related works found in the literature, namely Attitudes and Perceptions of IoT Security in Critical Societal Services – By Asplund & Nadjm-Tehrani, (2016), and Security Vulnerability Management for IoT Systems – an Interview Study, by Höst (2018), (see Appendix 2 and 3).

The questionnaires were structured in two main blocks for a total of 14 questions. The first group covered the topics concerning IoT security risk, security perception, measures from companies, and advice on possible best practices. The second, focused on responsible disclosure, bug bounty programs, and the adoption of crowdsourced security methods in the IoT domain. The interview guide is displayed in Appendix 1. In particular, the literature indicated that companies lack awareness on the importance of IoT security. For this reason, we tried to validate this condition by asking experts on the way that companies perceive security and the measures that they adopt to manage vulnerabilities. Moreover, guidelines on best practices for vulnerability management were scarce in the literature, thus we investigated what are possible best practices according to the experts. Given the research gap where the adoption of crowdsource security methods in IoT is still left open, the second group of questions investigated the application of crowdsourced security methods in IoT, including the state of adoption, benefits, limitations, barriers, and possible best practices for adopting BBP and RDPs.

The data gathering took part in one round of semi-structured interviews with industry experts. We repeated the same structure across the interviews, and when additional themes become relevant to be asked, more open discussions are applied. The majority of the interviews were realized as face-to-face with the experts, and in the rest of the cases consisted of remote video interviews. All of the interviews were recorded with the consent of experts, in order to preserve the integrity of the data and to allow the researcher to listen to the audio files in the data analysis. Each interview lasted for approximately 30 to 45 minutes.

Experts Selection

In this section, we discuss the interviewees selection process. It is typically not possible to investigate the behavior of an entire population. For this reason, a sampling method is adopted to allow the deduction of conclusion about a population, based on a sample of the population members (Ben-Shlomo et al., 2013). We adopted a nonprobability sampling technique, specifically a judgment sampling, where only a limited number of elements in a population have the chance to be selected based on their expertise in the subject investigated (Sekaran, 2000).

In our study, we define an "expert" as an individual with considerable knowledge on IoT security hacking, including ethical hacking practices and crowdsourced methods. During an internship period at Deloitte in the Netherlands, we firstly identified interview candidates from the network of professionals within Deloitte Global. A list of possible participants was developed from the employee profiles listed on the Deloitte international network portal, connecting more than 186,000 Deloitte personnel. By adopting profile filters, 17 experts were selected based on their experience with IoT security, ethical hacking, and crowdsourced security methods. The Deloitte professionals that we identified have different years of project experience in IoT security and ethical hacking, as they mentioned on their profiles. Moreover, the experts hold experience in different industries and have different roles and levels within the company. After the selection phase, an email was sent to all the candidates, including a description of the research, its objectives, and an invite to participate in an interview. In the end, among the 17 candidates, only 10 decided to take part in the study.

In addition to the previous group, 6 additional security experts from 8 other companies agreed to participate in our research. Initially, the companies were selected based on the literature. We decided to directly contact many of the firms operating in the field of crowdsourced security that we had encountered in the literature review, such as HackerOne, Pen Test Partners, Intigriti and other organizations. Eventually, some experts from these companies decided to take part in our interviews. Similarly to the first group, all of the participants have a background in IoT security and ethical hacking. In particular, three people come from a vulnerability coordination and bug bounty platform, three from penetration testing companies, and two from a hardware security conference and training organization. Additionally, one interview was done with members of a multinational company that develops and sells IoT consumer products worldwide. At the end of the data collection phase, we were able to consult with 19 experts, coming from 9 different companies, spread across 5 different European countries. All the relevant information regarding the interview participants is displayed in Table 3. The name of the companies (except Deloitte) and in general of all the interviewees is kept anonymous for privacy reason.

Table 3. Interview Participants.

Expert	Company	Position	Years of Experience	Focus industry	IoT Security Expertise	Ethical Hacking Expertise
A	Deloitte – The Netherlands	Senior Consultant, Risk Advisory	4 years, 5 months	Primary: Financial Services Secondary: Government and Public Services	High	Low
B	Deloitte – The Netherlands	Senior Consultant, Risk Advisory & Ethical hacker	3 years, 7 months	General Consultancy	High	Medium
C	Deloitte – The Netherlands	Manager, Risk Advisory	6 years, 3 months	Primary: Energy, Resources and Industrial Products and Services	High	Low
D	Deloitte – The Netherlands	Senior Consultant, Risk Advisory	2 years, 9 months	General Consultancy	High	Medium
E	Deloitte – The Netherlands	Senior Consultant, Risk Advisory & Ethical Hacker	1 year, 11 months	General Consultancy	Medium	High
F	Deloitte – The Netherlands	Senior Manager, Risk Advisory	1 year, 4 months	General Consultancy	High	High
G	Deloitte – The Netherlands	Manager, Risk Advisory & Ethical Hacker	3 years, 10 months	Primary: Technology, Media and Telecom	High	High
H	Deloitte – Hungary	Senior Manager, Consulting	3 years, 8 months	Primary: Technology, Media and Telecom	High	Low
I	Deloitte – Germany	Senior Consultant, Risk Advisory	0 years, 8 months	General Consultancy	Medium	Low

J	Deloitte – United Kingdom	Senior Manager, Risk Advisory	0 years, 7 months	Primary: Financial Services, Banking	High	Medium
K	Bug Bounty Platform A – The Netherlands	CEO	Not Mentioned	Cyber Security	Medium	High
L	Bug Bounty Platform B – Belgium	Advisor	1 year	Cyber Security	Medium	High
M	Bug Bounty Platform C – The Netherlands	Team Member & Ethical Hacker	Not Mentioned	Cyber Security	Medium	High
N	Penetration Testing Company A – The Netherlands	CEO, & Ethical Hacker	Not Mentioned	Cyber Security	High	High
O	Penetration Testing Company B – United Kingdom	Co-founder, & Ethical Hacker	Not Mentioned	Cyber Security	High	High
P	Hardware Security Organization – The Netherlands	Co-founder	Not Mentioned	Cyber Security	High	High
Q	Hardware Security Organization – The Netherlands	IT Team Member	Not Mentioned	Cyber Security	Medium	High
R	Automated IoT Security Analyses Platform – The Netherlands	Co-founder	Not Mentioned	Cyber Security	Medium	None
S	Multinational Electronics Company – The Netherlands	IT Team Members	Not Mentioned	Conglomerate	Medium	Low

3.2.4 Sampling Method

According to Sekaran (2000), for certain studies, judgmental sampling is the only meaningful way to investigate a specific phenomenon. Accordingly, we focused on a sample of experts that could provide us with the information sought by our research. As a result, subjects were selected on the basis of their expertise. In our case, as previously mentioned, we defined an "expert" as an individual with considerable expertise in the field of cybersecurity, specifically on IoT security hacking, ethical hacking practices, and crowdsourced methods. Moreover, IoT Security and Crowdsource Security have only recently become a subject of exploration in the academic and professional domain. We argue that judgmental sampling was the only viable sampling method for obtaining the right information sought by our research. The main benefit of this sampling technique, is that it allowed us to reach substantial results on the investigated field by employing a small sample of the population and limited resources. In addition, it is worth noting that our sample is based on a population of security experts working as security advisors. Consequently, our research takes the point of view of experts that are generally providing solutions to companies that face security problems. Therefore, the generalizability of our findings to the entire population should be done with care.

- *The Deloitte Bias Risk*

In this qualitative study, one limitation is that only experts that were conveniently available participated in the interviews. Within judgmental sampling, there is a risk of selection bias. There is clearly a lot of input from Deloitte in the case of this thesis that can lead to bias. In fact, 76% of the empirical data collected (13 interviewees out of 17), originates from interviews with Deloitte employees. The potential bias can compromise the opportunity for generalization the research conclusions. However, as we will present in Chapter 5, most of the results from the Deloitte interviews were confirmed by the interview findings with the other companies' experts. Moreover, the results present general insights on the research topics. We believe that there is no commercial dependency and interest on the application of crowdsourced security methods for IoT from Deloitte, as the company does not provide advice on these matter. Most of the experts' knowledge on ethical hacking comes from private life interests or previous working experiences, as stated by many interviewees. In addition, the research was conducted with a high degree of independency from the researcher.

3.3 Reliability, Validity, and Generalizability

According to Sekaran (2000), conclusions derived from qualitative research need to be plausible, reliable, and valid. In the case of qualitative research, reliability and validity have a different connotation from the definitions used in quantitative investigation. These principles are addressed in this section.

3.3.1 Reliability and Validity

In qualitative research the concept of reliability is based on category reliability and inter-judge reliability (Kassarjian, 1977). The first, refers to the researcher's ability to formulate competent definitions of categories to classify the qualitative data. The latter is based on the degree of consistency between codes processing the same data. Similarly to the reliability case, the principle of validity is divided in internal and external validity. Internal validity that measures the accuracy to represent the data collected. External validity is the degree of generalizability of the findings to other contexts and settings (Sekaran, 2000). In order to ensure validity, Sekaran, 2000, describes the following two methods:

- **Supporting generalizations by counts of events:** In order to respect this principle, the conclusion of our research are based on the most frequent codes registered from the expert interviews.

- **Ensuring representativeness:** In order to ensure representativeness, Sekaran, advices the selection of deviant cases to provide a strong theory test. In our study, we included cases that could contradict our theory. In particular, with did not based the data collection exclusively on crowdsourced security experts. Instead, we included the input of industry competitors, namely Penetration Testing Companies A and B.

3.3.2 Generalizability

In scientific investigations, generalizability refers to the wider range of applicability of the results and conclusions, from one to other settings (Sekaran, 2000). In our case, the applicability of our findings is based on the authority of the sample that was selected for the interviews. Due to the fact that the experts that participated in the research were predominantly from the Netherlands (13 experts), and more in general all from Europe, the results should be generalized with care to other countries and the whole security industry. In fact, security practices are different among countries. Some countries are advanced whereas others are still learning. In the western world, cybersecurity is generally mature but there are still many regions where responsible disclosure and bug bounties are just too sophisticated methods at the moment. For this reason, the recommendations are directed to companies belonging to the western cybersecurity industry that are developing, manufacturing, and commercializing consumer IoT devices. Nevertheless, several of the proposed recommendations might be also generalized to all firms that want to improve their security by implementing BBPs and RDPs that are mature enough in terms of security practices. We believe that the public will be able to determine the extent to which the findings and recommendations can be generalized and applied.

3.4 Data Analyses

In qualitative data analyses, there are few well-established rules and guidelines to analyze the data (Sekaran, 2000). In the following sections, we discuss our approach, based on the work of Miles & Huberman, (1994). The approach consists of three main steps: Data reduction, Data display and Drawing of conclusions.

3.4.1 Data Reduction

Data reduction consists of the process of coding and categorizing the data (Sekaran, 2000). Typically, this phase is very important because by coding and categorizing the data, the researcher can start to notice patterns and relationships in the data.

At first, all the audio recordings of the interviews were transcribed and converted into written documents. Subsequently, the next step consisted of coding the data. Coding is defined as the creative and iterative process of labeling words, sentences or entire paragraphs to reduce and rearrange the data in a meaningful way. Once the codes were generated from all the transcripts, we conclude the data reduction process with the Categorization. As a result, the codes were organized and categorized in different groups. For our research, the coding and categorization were realized adopting ATLAS.ti, a computer program for the qualitative analysis of large bodies of textual data. The tool was very handy and allowed us to structure and optimize the overall reduction process.

Moreover, as part of the data reduction, 2 of the 19 interviews conducted, were excluded from the data analysis because not sufficiently relevant. The reason is that two of the companies, namely Automated IoT Security Analyses Platform and Multinational Electronics Company, did not have the required expertise in IoT security and ethical hacking as the other ones in our study. In the end, 17 transcripts were included in the data analyses.

3.4.2 Data Display

Data display refers to the method of presenting the data, which is also important to identify patterns in the data. There are many different ways to data display. The most common ones include tables, charts or graphs each of them containing the most relevant information. In the end, the main purpose of the data display is to facilitate the eventual drawing of conclusions. From the coding process, we extrapolated categories and created conceptual groups on an Excel file. The file categorizes all the participants to the interviews. During the data analyses, we were able to determine the frequency in the data for each category counting the number of experts that were referring to the same conclusion. The full coding table is visible in Appendix 4.

3.4.3 Drawing Conclusions

The final step of the data analyses was drawing conclusions from the qualitative data. Drawing conclusion can be considered as the essence of qualitative research because it is the point where a researcher provides an answer to the research question (Sekaran, 2000). After the identification of common themes in the data reduction, we linked the categories, compare them, and thought of contrasts also with the data in the literature. Finally, after all these steps, we attempt to provide a logical explanation for the observed patterns and to determine our conclusions. In the next chapter, we present the results from the data analyses.

Chapter 4 – Results

In this chapter, we present the results of the interview analyses. The results are based on the identification of common themes and concepts from the data reduction. In particular, we determined key codes and categories by counting the frequency of different experts referring to the same concept. In order to provide more insights and transparency on the interview analyses, we present a results overview in Table 4. In section 4.1, we present the results on the current state of IoT security practices, including the reasons for the lack of security practices. Following, section 4.2 presents the findings on crowdsourced security methods, including the current state of adoption, benefits, limitations, and barriers for RDPs and BBPs in IoT. Finally, in section 4.3, we describe the results concerning the practical recommendations for companies to leverage BBPs and RDPs, in order to enhance vulnerability management practices in IoT, and some additional recommendations to boost IoT security practices. In order to preserve the anonymity of the participants, we do not use the real names of the experts, but we refer to them with descriptive names (see Table 3). Moreover, the results described in this chapter will be used to answer our research questions in Chapter 5.

Table 4. Results Overview.

High-Level Category	Concept/Code	Counts (out of 17)	Percentage
State of IoT Security Practices And Security Problems	▪ IoT security is not properly implemented	10	59%
	▪ Awareness on the importance of IoT security is missing both from industry and consumers	7	41%
	▪ Incentives for companies to implement security are scarce	7	41%
	▪ Hardware security is a problem for IoT	4	24%
	▪ Hardware security cannot be updated once products are on the market	7	41%
	▪ There are technical problems for IoT security	3	18%
	▪ Companies focus on functionality, time to market, and costs, leavening security unaddressed	9	53%
	▪ Companies care on security only if reputation is at stake	4	24%
	▪ Companies are not security mature	3	18%
	▪ Consumer demand for secure products is inadequate	6	35%
	▪ Consumer IoT goods is more vulnerable than other IoT sectors	6	35%
	▪ There is the need for more regulation	7	41%
	▪ Companies now care more about security	4	24%
	▪ Budget is Not the problem	4	24%
Bug Bounties	▪ BBPs effectively enhance security practices	9	53%
	▪ BBPs in IoT are already happening	5	29%
	▪ Monetary incentives are fundamental	5	29%
	▪ Protect company reputation	5	29%
	▪ Clear policies and resources from companies are required	7	41%
	▪ Adoption of BBPs will increase in the future	7	41%
	▪ Hardware is the main problem	9	53%

Obstacles for The Adoption of BBPs in IoT	▪ Hardware hacking skills are scarce	3	18%
	▪ Incentives for hackers on IoT are missing	2	12%
	▪ Budget is Not the problem	4	24%
	▪ Companies are not security mature enough	2	12%
	▪ Companies do not understand BBPs	3	18%
	▪ Companies do not trust hackers	4	24%
Solutions for BBPs in IoT	▪ Conferences	4	24%
	▪ Create events	9	53%
	▪ Hackathons	9	53%
	▪ Private in-house BBPs	7	41%
	▪ Using crowdsourced platforms to identify hackers for private in-house BBPs	2	12%
	▪ Increasing incentives for hackers	6	35%
	▪ Adopting BBPs for testing IoT software	3	18%
Responsible Disclosure Policies	▪ It is not a testing method	2	12%
	▪ It is a testing method	3	18%
	▪ Coordinates the disclosure of vulnerability found by ethical hackers	6	35%
	▪ Requires clear policies	6	35%
	▪ Incentives for hackers to engage with RDP are missing	3	18%
	▪ Companies sue hackers	7	41%
	▪ Adoption of RDPs will increase in the future	7	41%
Security Recommendations for IoT, integrating BBPs and RDPs	▪ Design secure products in the development phase	7	41%
	▪ Offer BBP after security maturity	6	35%
	▪ Adopt BBPs after pen tests	4	24%
	▪ Adopt a combination of BBPs and Pen tests	7	41%
	▪ Adopt pen testing to test security	7	41%
	▪ Implement secure design practices	4	24%
	▪ Adopt code reviews	3	18%
	▪ Follow OWASP/security guidelines	2	12%
	▪ Every type of company should offer BBPs	5	29%
	▪ RDPs should be in use by every company	9	53%
	▪ The use of crowdsourced platforms is recommended	3	18%

4.1 The State of Security Practices in The IoT Consumer Sector

The main result is that there is a general lack of security practices for IoT, as the literature suggests. In particular, the experts believe that the driver for security in consumer products is missing, at this moment. However, as a few experts point out, security practices always vary from company to company. The results also suggest that some companies are starting to care more about security.

4.1.1 Security in IoT Consumer Good Sector

The results from the expert interviews suggest that security is not properly implemented by developers, manufacturers, and vendors of consumer IoT products. In particular, 10 out of 17 experts believe that security is not properly implemented by most companies in the consumer goods sector (see Figure 15). However, not all the experts agree on this view. In particular, expert C explains that the attention on security always varies from company to company.

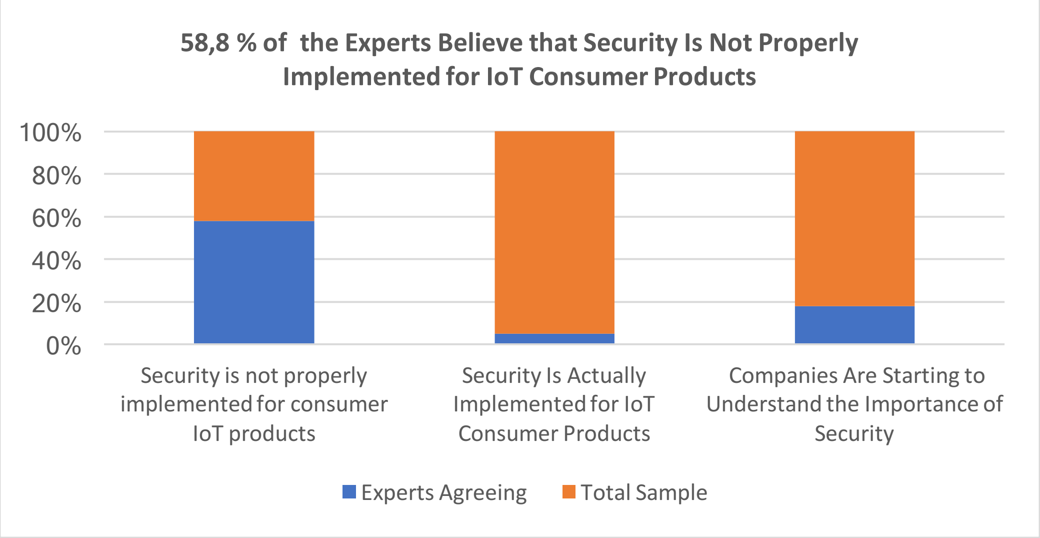


Figure 15. Security in IoT Consumer Goods.

Different Attitudes and Perceptions from Type of Company

In this section, we try to understand whether there is a difference in security attitudes by firms, based on factors such the size, age, or industry of the company. The main result is that the size of a company does not seem to affect the level of security, whereas age and industry might do so. Few experts believe that technology startups, even lacking the resources of bigger companies, understand better the importance of security. On the other hand, old established companies in certain industries, such as banking or medical, that want to move into IoT, might face bigger challenges to recognize the importance of security given that they lack deep technical knowledge.

Moreover, experts report that there are sectors where companies are more likely to address security given the higher risk of facing reputational repercussions by product security incidents. These include IoT products in the area of medical devices and cars. However, according to experts, consumer goods are not part of the previous sectors. In particular, expert C mentions: "*I do not see any driver for security in consumer IoT products at this moment*". The results present that 6 of the experts consider that consumer goods are more exposed to vulnerabilities than other sectors. Expert G points out that the main problem is presented by "cheap devices".

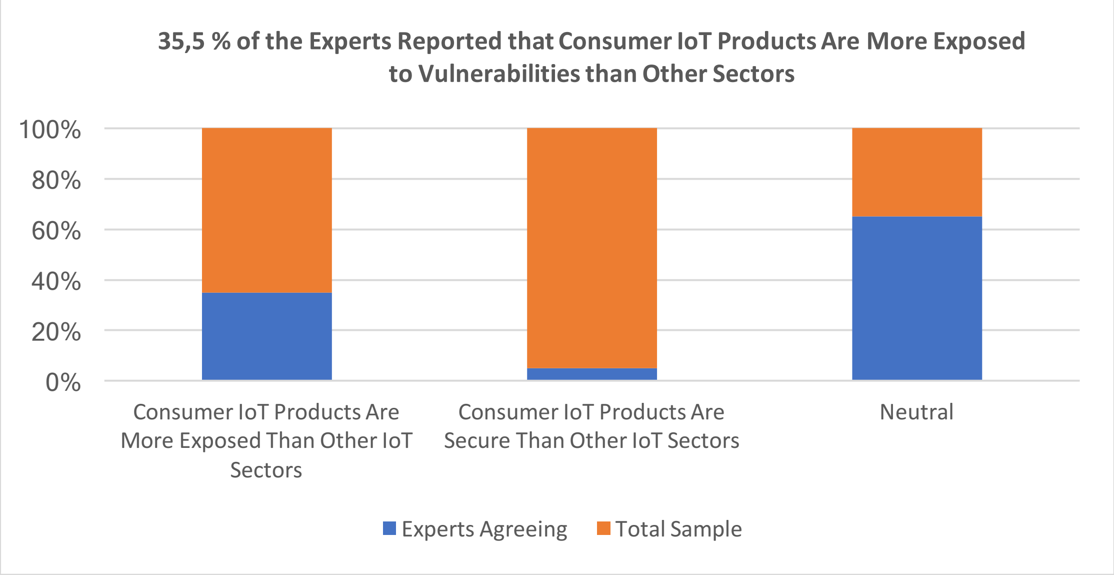


Figure 16. Consumer IoT Products Are More Exposed to Vulnerabilities than Other Sectors.

Contrary to the opinion of the previous experts, J believes that companies in the consumer IoT market, in particular startups, are actually aware of the importance of security: "*Retail companies that produce end-products for consumers, such as Fitbit, or other IoT powered end products, they quite understand that security is relevant and they understand that something about security must be done. I see also new companies that emerged recently, usually startups built by younger people, they understand security and privacy implications, although they might not have a security and privacy expert on the team. They do understand that something should be done about security*".

We conclude this sub-section by presenting the aforementioned findings in Table 5.

Table 5. Attitudes and Perceptions on IoT Security from Type of Company.

Different Attitudes and Perceptions on IoT Security from Type of Company		
Result	Description	Interview Quote
Company Size Is Not a Security Driver	The results do not suggest a strong correlation between the size of a company and level of security. Therefore, it is not the case that a big company equals big budget for security.	"*If you compare a startup to a multinational, then the big firm will probably have more resources to invest in security.* But *we cannot always say that a big company equals big budget for security because we have seen in the past that this does not hold true. Very often big*

		companies will realize the importance of security only after an accident.” (expert D).
Some Sectors Are More Security Driven than Others	The results indicate that there are some categories of IoT consumer goods, such as medical devices and cars, for which security is better addressed. Furthermore, IoT products that are adopted in sensitive environments require for security implementations. As an example, the experts mention that the military and baking sectors present high-security standards on IoT products.	"*Cars are increasingly becoming IoT. The lifespan of a car can easily reach 20 years. Those cars need to have security patches available for all those years. Therefore, companies need to be able to provide security updates” (expert H).*
The Consumer IoT Sector Is Not Security Driven	The results present that consumer goods are more exposed to vulnerabilities than other sectors. Expert G points out that the main problem is presented by "cheap devices".	"*I do not see any driver for security in consumer products at this moment*” (expert C). “*When you have very cheap devices, they will not have any kind of security. The reason is that for companies to set a low price, also the production costs have to be low” (expert D).*

Vulnerability Management Practices by Companies

Lastly, we describe the results on the vulnerability management practices by companies. Experts describe that the most common practice for vulnerability management is pen testing. However, some experts consider that pen testing is not sufficient. Expert C, explains that: “*Pen testers tend to focus on major risk drivers and they do not look to all the attack factors*”. Additionally, to pen testing, there are other security practices that firms should implement, such as code reviews. However, the experts do not see much of these practices across companies.

In contrast to the previous opinion, expert J believes that many IoT companies have recently started to implement different security measures: "*During the last decade a lot of things have improved. From security assessed after the market launch to the initial stages of the product development. There are a lot of companies that do, such as code reviews. There are even more companies starting to think about how to define security requirements and tests against those requirements. And there are even a few companies that started thinking about security and privacy as their competitive advantage*”.

Some Companies Now Care About Security

Few experts indicate that the previous situation might be changing as companies become more aware of the security value. As mentioned by expert I: “*There is a huge lack of security and most companies are not fully aware of the importance of security. But nowadays this is changing*”. Furthermore, expert J presents a very unique opinion on this topic. He believes that the current view on IoT security shared by most of the experts is outdated: “*I think there is the idea for which consumers are not paying for security. Therefore, companies cannot invest in it. If they do, products will be more expensive and they will go out of the market. I think that is a traditional view. But in many cases that is changing, especially in consumer* *products. I think there are a lot of customers who start asking about security and if the vendors don't provide it then they go out of the market*".

4.1.2 Causes for the Lack of Security in Consumer IoT Products

The results indicate that companies lack the incentive to invest in security. The reason for the lack of incentive comes from the attitude of consumers, that fail to demand companies for secure products. In order to have secure products, customers need to realize that is also their behavior that will determine the level of security of IoT products. Moreover, companies fail to understand the importance of security practices and have premature security measures in place. The lack of regulation is also one of the reasons limiting the action of firms. In the end, the results indicate that the current lack of security is largely caused by the combined unawareness on the value of security, from both companies and consumers. Furthermore, a technical problem is that companies cannot fix vulnerabilities in the hardware once the products are on the market. Normally, after a vulnerability is identified, companies are able to release software updates to improve the security of a device. In the case of IoT, it is often not possible to do the same to fix vulnerabilities in the hardware. We present the aforementioned results from the data analyses more in detail in Table 6, followed by the interview data.

Table 6. Causes for the Lack of Security in Consumer IoT Products.

Causes for the Lack of Security in IoT	
Cause / Sub-Cause	Description
1) Companies Lack Incentives to Invest in Security	The results indicate that firms lack the incentives to invest in security. According to expert H: "*The main problem is that incentives are currently missing”.* There are several problems described by the experts that negatively impact security practices.
1.a) Security Does Not Pay Off for Companies	According to the majority of the interviewees, companies do not invest in security because they do not perceive it as beneficial in terms of returns. According to expert H: “*IoT manufacturers do not want to create secure products. The reason is that security is not something that pays back. It only costs money, but actually, the client does not pay for it*”.”
1.b) Companies Focus on Time-To-Market	Companies that want to stay on top of the market need to be first commercializing new ideas. For this reason, security is left out of development and production phases. Expert K describes: “*The problem with IoT is that most of the companies want to be fast at developing products, to be the first ones on the market. For this reason, most often security is just cut out*”.
1.c) Companies Focus on Functionalities	Due to the growing number of IoT products on the consumer market, companies need to develop better features than competitors to attract consumers. As mentioned by expert B: “*The problem in IoT is that now there are more and more devices that are available for people. This causes issues that companies will spend more time implementing nice features, rather than look into product security*”.
1.d) Companies Focus on Cost Reduction	In other to be competitive on the market, companies need to manage costs. According to expert F: "*Security is not a leading criterion for product development. Firms rather look for the cheapest solution and not even think about security. I think that's the problem*”.

2) Companies Are Not Security Mature	A second main problem is that companies have very limited expertise in security practices. Experts mentioned that most of the companies are not “mature” in terms of security and they do not test the security of their device. According to expert I: "*The problem is that most of the companies are still in a very immature. So they have some kind of security process, but they still need to improve*”. According to expert J, maturity is defined as: “*Having the device tested and knowing that most of the bugs are already solved*”.
3) Hardware-Related Problems	The results indicate the hardware is one of the most important elements affecting the degree of security in IoT. There are two main problems involving the hardware. Firstly, it is difficult for companies to release vulnerability patches for IoT devices once they are in the market. Secondly, companies forget testing hardware security.
3.a) Hardware Patches Are Problematic	One of the major obstacles for IoT security is that several hardware vulnerabilities are unfixable. According to expert H: “*In IoT security, it is infinitely more complicated to fix bugs, because there is usually no way to install security updates and patches*”.
3.b) Companies Do Not Test Hardware Security	Due to the problem 3.a), companies should test hardware security before the product launch. However, the results suggest that companies are not aware of the importance of testing the hardware. As expert B mentions: “*I think right now companies do not invest in securing the hardware*”.
4) Consumers Do Not Demand Secure Products	According to many experts, consumers underestimate security. Expert C mentions: "*An issue when it comes to consumer IoT products, is that consumers do not care that much about security. If someone wants to buy a webcam, they will not spend 2 euros to have an encrypted product. Consumers will buy the cheapest device".*
5) Regulation Is Missing for Consumer IoT	Experts describe that there is no regulation on consumer IoT products. Expert O reports: “*There is no regulation. We are reliant on protecting the data based on the GDPR, that is useful. Some European state laws that are useful as well. But there are no strict regulations around the Internet of Things security”.*
6) Lack of Security Awareness and Understanding	Experts indicate that the current lack of security in IoT is mainly the result of the absence of security awareness both from companies and consumers. According to expert O: “*There are all sorts of reasons behind the poor security in IoT, but fundamentally, it all comes down to a lack of understanding and awareness on the importance of security*”. As expert D, claims: “*Awareness. It all starts with awareness. Until companies and people will not realize that they need security, then we will never have security in IoT.*

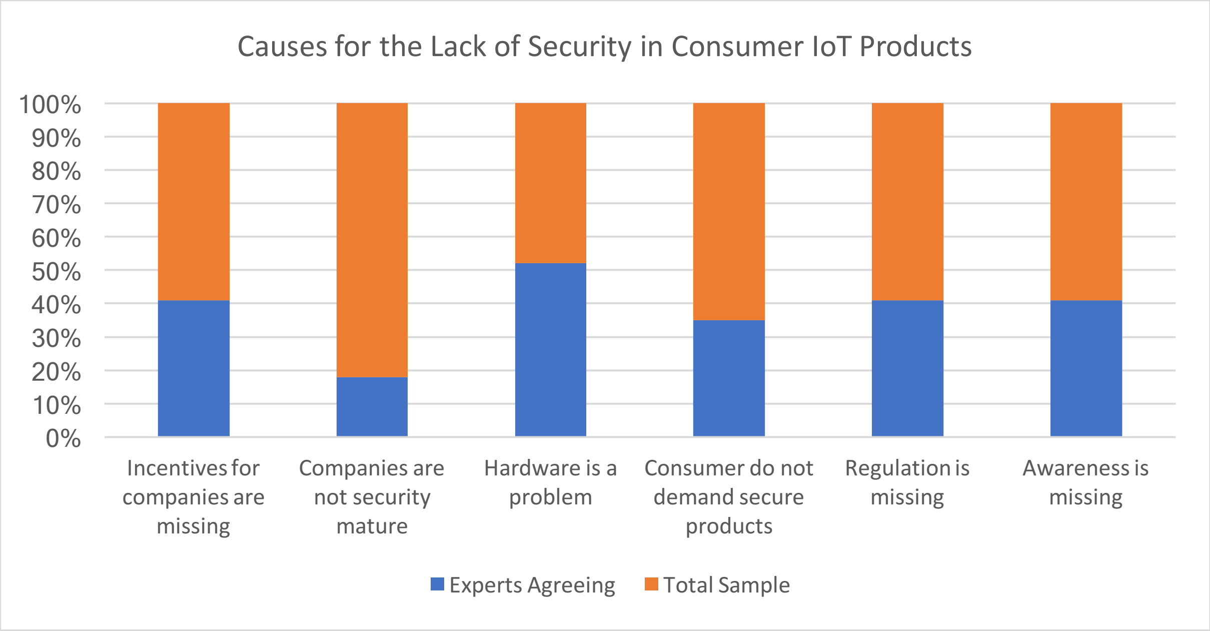


Figure 17. Causes for the Lack of Security in Consumer IoT Products.

Before moving forward, we share the opinion of expert F, on the current lack of security in IoT. He believes that the lack of security in IoT is the result of a recurrent problem in the digital world. He explains that the current lack of security is in part a cyclical problem of digital technologies. According to him, every time there is a new technology security will always be neglected. The expert believes that this is also the case with IoT: "*We started with computers with no security, then over the years, security increased and companies became mature. So right now we are very security savvy on computers. Then mobile phones came, and we started all from zero again. There was no protection and problems started to occur. So people thought there was a need for security and they started implementing it. But now there is IoT, and we have the same issue again*".

4.2. Crowdsourced Security Methods in IoT

This section presents the result analyses on crowdsourced security methods, including the current state of adoption, benefits, limitations, and barriers for RDPs and BBPs in IoT. In particular, the results add little information to the literature findings on the current state of adoption of RDPs and BBPs in IoT. However, we were able to confirm that the adoption of BBPs for IoT is still minimal. The data that we collected on this subject regards expert G's opinion: "*Bug bounties in IoT are already running right now. However, my calculated guess is that only 2% of the entire bug bounty is done for IoT. So it is not a large amount*".

The results concerning the benefits and limitations of RDPs and BBPs expand the findings described in Chapter 2. Regarding the reasons for the limited adoption of crowdsourced methods, the results provided us with several new insights. Among the main reasons that we identified, some companies still do not understand or see the benefits of crowdsourced methods. In particular, some of them are still very aggressive against ethical hackers that report vulnerabilities. Moreover, we also identify the "hardware obstacle" as one of the main barriers for the scalability of BBPs in IoT. However, the interview results provide also with several innovative solutions to allow BBPs in the IoT domain.

4.2.1 Benefits and Limitations of Responsible Disclosure and Bug Bounty Programs

- *Benefits and Limitations of Responsible Disclosure Policies*

Experts identify many benefits from responsible disclosure. In particular, they believe that companies, ethical hackers, and society all benefit from RD. According to expert C, responsible disclosure is a quick win for companies to get free advice and avoid some reputational damage. Moreover, RD helps to attract people that want to test your security. Ethical hackers benefit from it because it guards them against the risk of legal persecution. Society benefits because zero-day vulnerabilities are prevented. However, the experts also indicate that a limitation of RD is that researchers may lack incentives to engage with it. According to expert E: "*The problem of responsible disclosure is that it pays you nothing for your time, but still it expects you to provide details about the vulnerabilities you find"*. A second limitation mentioned by few experts is that RD is not supposed to be considered as a security testing method. For this reason, it cannot ensure security coverage like pen testing or other methods does. According to them, RD is more of a tool for companies to engage with the researcher and to prevent that people disclose vulnerabilities that they find. Expert I, claims: "*Responsible disclosure policy is not related about identified vulnerabilities, but to avoid possible incidents and episodes where you disclose a vulnerability without any kind of patch or remediation.*

- *Benefits and Limitations of Bug Bounty Programs*

According to the majority of experts, BBPs are very beneficial tools for companies to test security. In this respect, many are the advantages mentioned. In particular, experts believe that BBPs are a great way for companies to engage with the population of security researchers. Expert I, affirms that companies can really use BBPs to improve their security by incentivizing people to detect vulnerabilities in their systems. In addition, by finding vulnerabilities before they are exploited, companies can protect their reputation and avoid having to pay for any damage to consumers in the case they get hacked. Expert I claims: "*I think if you pay a bounty it will be always cheaper than actually having to pay the fines or the repercussion that might happen after a company is hacked*". Moreover, several interviewees stated that BBPs provide cheaper and more accurate results than pen tests. Expert Q reports: "*Bug bounty programs give companies almost a free pen test from several people and a fresh perspective on how to hack their product*". According to expert D: "*With bug bounties, there is always going to be high chances that researchers find some vulnerabilities. Because if you have a hundred people, and passionate people because they would not be there otherwise, then you will have more results than a pen test*". In particular, experts consider that companies can save a lot of money if they properly understand how to combine pen testing and bug bounties. Lastly, ethical hackers can make a living out of bounties. Therefore, BBPs consists of a lucrative work for many individuals.

Regarding the limitations of BBPs, the results present scarce information. Instead, there are several insights on the obstacles preventing the application of BBPs and more in general of crowdsourced security in IoT. We present these findings in the next section. Before moving forward, we summarize the results on the benefits and limitations of RDP and BBP in Table 7.

Table 7. The Benefits and Limitations of Responsible Disclosure and Bug Bounty Programs.

	Benefits of Responsible Disclosure
For Companies	▪ Prevents irresponsible disclosure
	▪ Helps to attract people that want to enhance your security
	▪ Companies benefit from almost free advice
	▪ Protects reputation
For Ethical Hackers	▪ Guards against the risk of legal persecution
For Society	▪ Zero-day vulnerabilities are prevented
	Limitations of Responsible Disclosure
For Companies	▪ Is does not ensure security coverage
	▪ Incentives are not sufficient to attack hackers
For Ethical Hackers	▪ It pays researchers nothing for their time but still expects them to provide detailed reports
	Benefits of Bug Bounty Programs
For Companies	▪ Allow to effectively engage with security researcher communities
	▪ Provide an almost inexpensive form of pen testing
	▪ Protect companies' reputation and to avoid financial repercussions from security incidents
For Ethical Hackers	▪ Allow to making a living out of bounties

4.2.2 The Reasons for the Limited Adoption of Responsible Disclosure and Bug Bounties in IoT

The interview results generated numerous insights on the reasons for the limited adoption of RDPs and BBPs in IoT. Among the main reasons that we identified, there are companies that still do not understand crowdsourced ethical hacking. Crowdsource security has only recently gained the attention of the cybersecurity industry, and it seems to be still too radical as an approach for many companies. Some others do not see the benefits of crowdsourced methods. In particular, some firms are still very aggressive against ethical hackers that report vulnerabilities. Moreover, in certain firms lack the capabilities to manage these type of programs or are not mature enough in terms of security practices.

Looking into more specific IoT problems, the results describe that ethical hackers lack incentives for participating in RDPs and BBPs for IoT. In this respect, we identify one of the main barriers for the scalability of BBPs in IoT, consisting of the "hardware obstacle". The security of IoT products depends to a large extent on the hardware security. For this reason, in the case of BBPs for IoT products, researchers need to have physical access to the device to test the hardware. The problem is that for practical reasons companies cannot provide physical devices to all of the researches willing to participate in BBPs. At the same time, researchers miss sufficient incentive to buy the products themselves for testing them. In addition, in order to hack IoT, hardware hacking skills are needed. However, the experts state that there are limited people with such skills at the moment. The previous obstacles could also be a reason for the minimal employment of bug bounties in the field of IoT. The results from the data analyses are presented in more detail in Table 8, followed by the interview data.

Table 8. The Obstacles to the Adoption of RD and BBPs in IoT.

Obstacles to the adoption of RD and BBPs in IoT	
Companies Do Not Understand Crowdsourced Security	Experts consider that many companies fail to understand that in order to protect their products and reputation, they can benefit from external help. As expert C claims: "*Firms want to protect their product and the company reputation. But they don't realize that it's better for them to be open rather than close to external help*". In particular, BBPs seem to be still too radical as an approach. According to expert O: "*Companies still do not understand how to use bug bounty. It is quite too progressive. The whole idea of rewarding people to break their products requires quite a lot of forwarding thinking*". Sometimes, companies are also scared of hackers. Expert K describes: "*People are still scared of hackers. That's mostly what we see. And it's mostly a board decision in the companies. So somebody in the company wants to try bug bounty and he goes up to the board, but they say: 'What? No way! We do a pen test. We don't know who are these hackers".* In the worst cases, companies even take legal action against the hackers reporting vulnerabilities to them.
Companies Are Not Security Mature	The results describe that security maturity is a major problem. Several companies are not ready to adopt crowdsourced security, in particular BBPs in IoT. Expert F mentions: "*I think the biggest issue is that the world of IoT still is not prepared enough to do bug bounties. I don't think they are security savvy enough to be able to handle a bug bounty*".
Companies Lack Capabilities	The results suggest that companies might lack the capabilities to handle crowdsourced methods. In fact, according to expert K, there are many companies willing to use RD and BBPs, but it is difficult for them to handle the whole process.
Incentives for Researchers to Are Missing	Expert B describes that when companies want to start RD or offer a BBP for IoT, most researchers will not be interested in the program. In particular for BBPs, expert M believes that the problem is that ethical hackers are not really motivated to buy IoT products in order to hack them because they cannot be sure to get a reward. As expert D describes: "*Researchers don't have sufficient incentives. With bug bounties in IoT hackers have to buy a device and invest time, and then they don't know whether they will get any money back. They will not do that*". In addition, expert Q points out that in

	order to hack the hardware, the researcher has to disassemble the device. At that point the device becomes useless and to keep on testing the hacker needs to buy a new device.
Obstacles to the scalability of BBPs in IoT	
How to Test the Hardware Is the Main Problem	Bug bounties in IoT present a major obstacle compared to BBPs in software. Expert D describes: "*In a regular bug bounty the researcher has access to an URL, an API, etc. They can very easily start hacking. With IoT products is different. There is not only software running but also a hardware. So how do you get the hardware tested in a bug bounty? Hackers need to have the device itself. And I think that's the biggest issues*". In order to overcome such problem companies can deliver the hardware to people. However, there are also problems for companies to deliver the hardware to hackers. According to expert E: “*When it comes to bug bounties in IoT, the problem is how are companies going to deliver that hardware to all the researchers. It is not possible to provide the hardware to all the researchers because this will cost firms lots of money. In this case, they are not selling, but just sending products for free to these people*”.
Hardware-Hacking Skill Are Scarce	The results indicate that software hacking and hardware hacking are different practices that require very different skills. In order to test IoT security, researchers need both. However, most hackers are proficient in software hacking but not in hardware hacking. Expert J reports: “*The main issues is that IoT is a very specific field. So you do not always have people that know how to hack it*”. The main evidence is provided by expert K, the CEO of Bug Bounty Platform A: “*We have a lot of young hackers who do only web security. They have no clue on how to look into a physical device. So we need hackers capable of working with hardware. So the combination of software and hardware hacking skill will work perfectly in the future*”.

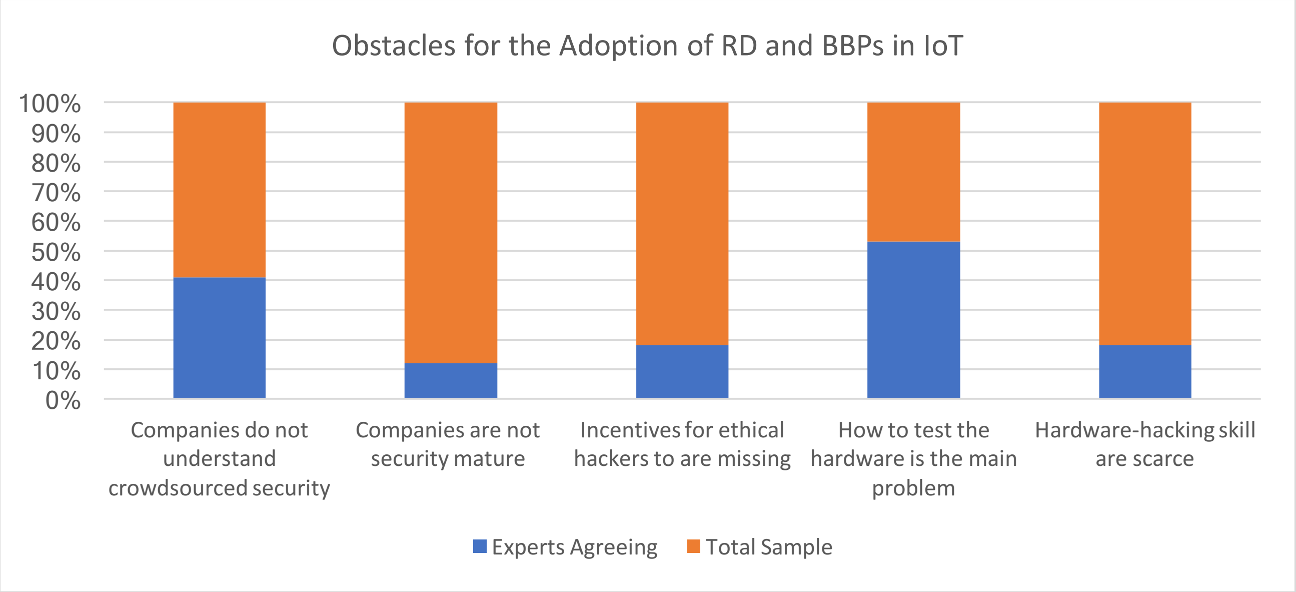


Figure 18. Obstacles for the Adoption of RD and BBPs in IoT.

4.2.3 Possible Solutions for The Adoption of Bug Bounty Programs in IoT

Previously, we described that the key problem that companies have to solve in order to adopt BBPs in IoT is how to provide hackers with the devices. In this section, we present possible solutions that experts have already experienced or that they believe would enable BBPs in IoT.

Even though companies cannot deliver the hardware to researchers individually, they can still try to create events for hackers to participate in bug bounties. In this case, they can set up events, such as hackathons, were hackers are invited to test the security of IoT products. Moreover, instead of organizing the events by themselves, companies can also join security conferences and invite participants to find vulnerabilities in their products in exchange for rewards. However, the previous two solutions do not allow companies to directly control who gets access to their devices. There might be some situations where companies have some critical assets, and they actually do want to select skillful individuals to test their technology. In this case, companies can set private BBPs where a limited number of hackers are selected to test the device. In the case of IoT, experts indicate that firms can set this type of BBPs to either invite researchers to private events or to send very trustworthy individuals some samples of the device to test. These are only some of the ways how BBPs sin IoT could be offered. In particular, we note that organizations have to be very creative to make BBPs viable in IoT. The solutions identified in this thesis are described in Table 9, followed by the interview data.

Table 9. Possible Solutions for The Adoption of Bug Bounty Programs in IoT.

Possible Solutions for The Adoption of Bug Bounty Programs in IoT	
Create Events Such as Hackathons	Even though companies cannot deliver the hardware to researchers individually, they can still try to create bug bounty events. As suggested by expert D, companies could also think of organizing hackathons to test the security of IoT devices, with actually rewards for participants: "*A very good idea is to invite people locally and organize a hackathon for the hardware. The hackathon can be in the company, or they just rent a location and provide some pizzas. And about the cost, I do not think companies need much budget for it*". Expert I, believes that hackathons are actually a very good way to test IoT devices.
Employ Security Conferences	Instead of creating events by themselves, companies can take their devices to security conferences where participants can try to hack them in exchange for rewards. As expert E describes: "*There are conferences with thousands or hundreds of researchers attending. Then firms could join those conferences to provide a number of IoT devices and then invite researchers who are already in the conference to hack on those devices. And if they find something they get a bounty. So companies don't need to send those IoT devices, there are no additional costs because the event is already set up during the conference, and they can take the products back after the conference*". According to expert Q, this practice is already there. He mentions: "*A solution for bug bounties is happening in conferences, where companies bring their products and then hackers can test it and be rewarded if they find vulnerabilities*".

Offer Private Bug Bounty Programs	Companies can invite an elite group of hackers to test IoT products in exchange for rewards per vulnerability. According to expert E, an additional benefit of this solution for companies is that hackers would also agree not to release any information regarding the program. The expert explains: *"If something critical is found or the company is concerned about its reputation, the private program means that nothing will be published. No one would know that there was a bug bounty program and no one would know about any vulnerability found in your application*". Moreover, we previously mentioned that shipping devices is not practical for BBPs in IoT. However, according to expert G, in the case of private BBPs, companies can try to send samples of products to small groups of hackers.
Provide More Incentives to Researchers	Experts believe that companies should provide more incentives if they want ethical hackers to engage with BBPs in IoT. For instance, they could return the cost of the product to hackers that find a vulnerability. However, expert K reports on this option: "*We have tried to motivate vendors to start a bug bounty program where hackers buy the device themselves, but on the first valid report, they refund the money of the product. This would be a very good motivation for people because then they can have that product for free. But it was really hard to convince vendors to do that*". Another suggestion for companies was to create a 'Hall of Fame' to give credit to hackers that successfully report vulnerabilities. The idea is that there are people that care about status even more than money, and this could promote the adoption of BBPs in IoT.
Employ Bug Bounty Programs to Test IoT Software	The results suggest that companies can still offer BBPs to test the software of IoT products. As expert J reports: "*Companies can still use bug bounties to test certain parts of devices over the internet. So you don't necessarily always need to have access to the IoT device".* There are still many advantages of testing the software of an IoT device, as expert E mentions: "*I have seen a company publishing the OS they used on the hardware and then asking top researchers to test it. The OS typically includes everything that needs to be tested. All libraries, all the source code, the web application, databases, etc. So to solve the hardware issue, this company didn't deliver the hardware, but they delivered the operating system that they used on that hardware. But this cannot work for all types of IoT devices*".

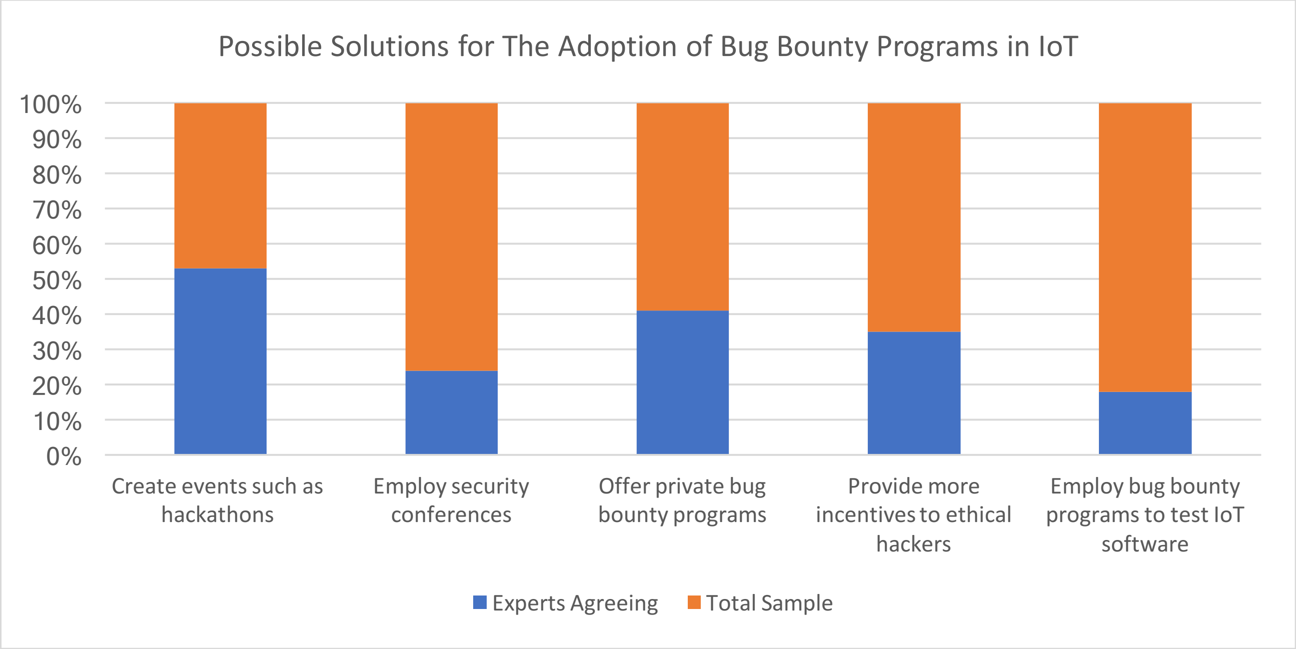


Figure 19. Possible Solutions for The Adoption of Bug Bounty Programs in IoT.

Limitations of The Proposed Solutions

According to expert J, the aforementioned solutions present several limitations: "*By limiting BBPs to only physical gatherings we out scope 70% or 80% of researchers that work on bug bounties from other countries. In my view, there is very few that can be done to solve this problem. To test IoT devices you need hardware hacking and you need access to the device. Also, very few people know how to hardware hacking. Moreover, few people are motivated to buying the device. The idea where you buy a device to test it, that is not really how bug bounties work. That is more someone who is really passionate about a certain device. But he is one in 10,000. At the moment, all the bug bounties and responsible disclosures are based on scalability and trying to get over as many researchers as possible*".

4.3 Integrating Bug Bounty Programs and Responsible Disclosure with Conventional Security Practices to Enhance IoT Vulnerability Management

In this section, we present the results on the best practices for companies to boost IoT vulnerability management and to integrate RDPs and BBPs among security practices. We start by describing the recommendations on possible best practices for vulnerability management in IoT. Subsequently, possible best practices for leveraging RDPs and BBPs in IoT are presented. Regarding BBPs in IoT, incentives for both ethical hackers and companies are the most crucial element. In this respect, companies shall take initiative to provide more incentives to researchers through the means of sharing hardware and setting up credit/reputation system to recognize active participation. In the implementation, BBP shall be applied after Pen Test to achieve a balance between cost and efficiency of detecting vulnerabilities.

4.3.1 Best Practices for Vulnerability Management in IoT

The main recommendation for companies is that security should be a parallel process of different practices, starting from the product design. Implementing security from a design stage makes it easier the process of vulnerability management because once those companies realize security from the beginning, it is less likely that they will face vulnerabilities. Secondly, experts advocate to always have some kind of security testing process. A possible best practice consists of using a combination of pen testing and bug bounties.

An ideal security process is highlighted by expert J: "Security should be a parallel process. You build in some tests in your software development life cycle, you do code reviews, you do secure design, and you have security requirements. Then whenever there is a release you do pen testing to make sure you follow a methodical process that validates that the security requirements are indeed implemented. But then in parallel with all of it, you also have a responsible disclosure policy on your website together with a bug bounty. This way you'll be able to cover other classes of vulnerabilities that pen testers missed."

A further recommendation from an organization perspective is to move the budget for security from IT to Risk. The recommendations identified are described in Table 10, followed by the interview data.

Table 10. Best Practices for Vulnerability Management in IoT.

Best Practices for Vulnerability Management in IoT	
Start with Security from the Design Phase	Companies should direct security efforts to the early stages of the development process of IoT products. Implementing security from a design stage facilitate vulnerability management because once security is executed from the beginning, it is less likely that firms will face vulnerabilities. As mentioned by expert I: "*The security level of IoT, will depend on what companies do in the development. I think that the most important point is that security in IoT should start from the design. If companies design secure products or just if they take into account the security during the whole development lifecycle, it is less likely that they will have security issues afterward and it will be easier to solve them*". This can be done by following secure design principles, such as the Secure Development Life Cycle (SDLC).
Testing Products for Vulnerabilities	Experts indicate to always have some kind of security testing practice, in particular, pen testing. There are different procedures that companies can apply to test security. As mentioned by expert J, among the security testing practices there are pen testing, red teaming, responsible disclosure, and bug

	bounties. A best practice consists of the combination of pen testing and bug bounties to test security. According to interviewee O: “*Manufactures should not be launching out products without a very thorough pen test. Additionally, bug bounties should be there to ensure that vulnerabilities that pen test missed are addressed*”.
Moving the Security Budget from IT to Risk	Keeping the budget for security within the IT is insufficient to cover the IoT vulnerabilities. Expert K reports: "*A lot of companies have their budget for security in IT. Hence, the IT department is responsible for securing everything within the company, such as networks, products, and websites. But the IT budget typically few. So it is very difficult to invest in IoT security. Instead, most of our clients, have put the security in the hands of the department responsible for risk. So if something goes wrong with security, that costs money, and they need to prevent it. By having security in the risk budget, it is much easier to get funds to secure and test IoT*”.

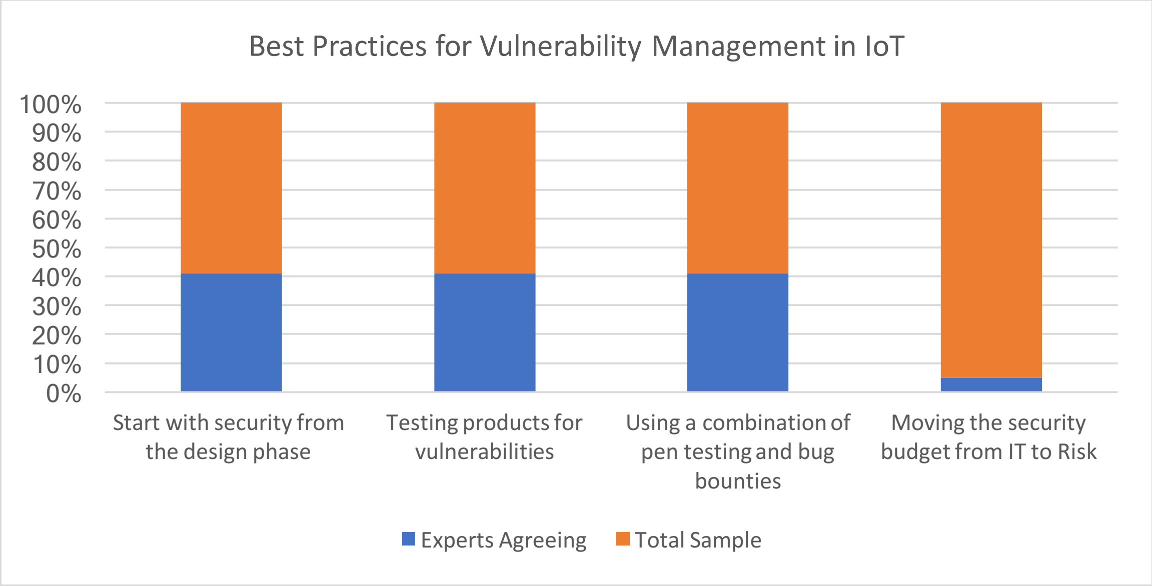


Figure 20. Best Practices for Vulnerability Management in IoT.

4.3.2 Leveraging Responsible Disclosure for Vulnerability Management in IoT

In this section we present the best practices for leveraging RDPs in IoT. The results indicate that experts recommend the implementation of RD to all type of companies, in particular for those dealing with IoT. According to expert C: *“Responsible disclosure definitely benefits companies. Especially with IoT technology. In IoT, there are too many relation and multiple places where you can make an error. This is unavoidable. So then as a company, you should be open for the feedback. It is free advice. And it really improves the quality of your products and protects your reputation*”. Moreover, expert B states: “*Responsible disclosure should definitely be there, regardless if it is IoT. Any company should have an email address in case somebody finds something wrong, so that the problem can be reported before someone exploits the vulnerability”.* Moreover, being open-minded is a condition to utilize crowdsource ethical hacking. The next step is to define policies for what happens after a vulnerability has been reported. In addition, companies need to define the internal processes to be able to accept and process the incoming reports.

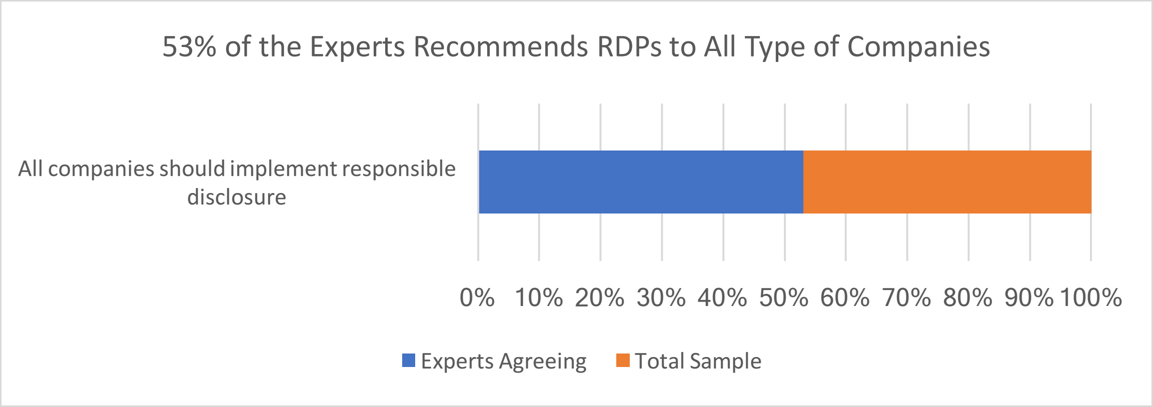


Figure 21. Experts Recommending Responsible Disclosure to All Type of Companies.

Elements of Effective Responsible Disclosure Policies

The interviewees report that in order to have an effective responsible disclosure, the first step is to be open-minded. Many companies nowadays still do not trust this practice and in particular the goodwill of the ethical hackers. Such behavior limits and hinders the effectiveness of RDPs. Secondly, companies need clear policies and clear rules. Finally, and most importantly, firms need to have a process to fix the problem.

Additionally, in order for responsible disclosure to work, companies have to make sure to communicate effectively with hackers. In order to manage the communication with security researcher, companies can also hire crowdsourced security platforms. K describes: "*We have security experts that are in charge of communicating with hackers. So if somebody submits something which is not relevant for our client, then we have an expert explaining to the hacker that this isn't relevant. And if it's serious, we help the client as well to fix the problem.*" Another important element that companies need to consider is to reward hackers for their effort in order for them to stay motivated on testing their security. The interview results are presented in Table 11.

Table 11. Best Practices for Responsible Disclosure.

Best Practices for Responsible Disclosure	
Be Open Minded	The first step for a company is to be open-minded. As expert C claims: "*Firms want to protect their products have to realize that it's better for them to be open rather than close to external help*".
Establish Clear Policies and Rules	It is important to define clear policies and rules. Expert D claims: "*Responsible disclosure is not as straightforward as just putting a website up. Companies really need to think about the process thought. They need to think about which type of vulnerability do they want to be informed. Who is going to take care of it, how much money do they want to spend on it, and how much time*".
Allocate Resources and Define Processes Around RD	Companies need to allocate sufficient resources and define processes to administrate the RDP. As expert J describes: "*If you are a company and you start a responsible disclosure on your website, then you also need to set up a process around it. You need a detection mechanism, a response procedure in place. If a company does not have this capacity, then it is useless*".

Patch the Vulnerabilities	Next to the process to analyze the reports, companies need to be able to actually fix the bugs. Expert A points out: "*If you disclose vulnerabilities without a patch, you will give possible attackers the time to exploit the vulnerability and to get access to users' data*".
Effectively Communicate with Researchers	In order for responsible disclosure to work, companies have to make sure to communicate effectively with hackers. Expert K reports: "*In most cases, hackers submit something but do not get any response. And then the hacker gets angry and releases the information. Then companies have a problem. But if you keep in contact with them, you can make it work*".
Reward Researchers	Companies need to reward hackers for their effort in order for these individuals to stay motivated. Benefits that companies can offer can be public recognition, objects, or even money. According to the expert G: "*There should be a benefit in responsible disclosure for the researcher. It can also be giving credit and recognition. People care for status, and that motivates people to keep on searching. Otherwise, only a much small subset of people will look at your security*".

Conditions to avoid

Before starting with responsible disclosure, companies should make sure to have some product security already in place. As explained by expert J: "*I have seen companies going wrong with responsible disclosure by putting on the market products which had a huge number of flaws. And then the responsible disclosure started sending them hundreds or thousands of scripts. I think that is when responsible disclosure is wrong. Because then you have to deal with answering thousands of people, go through long reports, and eventually also pay them money. So they should keep in mind that responsible disclosure is not a replacement to pen test or any of this. Pen tests or code review are still necessary steps*".

4.3.3 Leveraging Bug bounty Programs for Vulnerability Management in IoT

In the previous sections we presented that expert always recommends the adoption of RDPs. The results indicate that also BBPs are a best practice for the vulnerability management of companies. However, according to the experts, companies should already be active with vulnerability management practices before implementing a BBP.

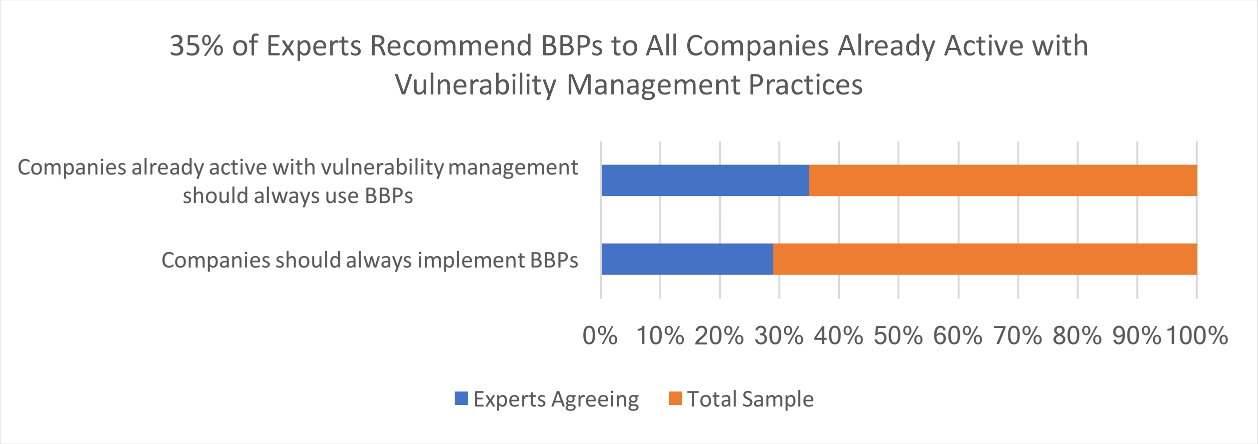


Figure 22. Experts Recommending the Adoption of Bug Bounty Programs to Companies.

Furthermore, the elements that were discussed for effective RD in the previous section, apply also in the case of BBPs: In order to have an effective BBP, organizations need to be open to the idea of having hackers testing their security. Companies need clear policies and rules for hackers. At the same time, they have to allocate sufficient budget and resources and define internal processes, to be able to accept and process the reports and actually fixing the vulnerabilities.

In this section we present additional guidelines that cover both technical and organizational aspects for an effective deployment of BBPs in IoT.

Integrating Bug Bounty Programs into IoT Security Practices

Before starting with BBP, companies should already be active with vulnerability management practices to ensure that a sufficient amount of vulnerabilities have been previously identified and fixed. Otherwise, BBP can turn into a very expensive and ineffective approach for companies to identify vulnerabilities. In the case of companies that developed a product and never tested it, the untested product will typically have many vulnerability issues. When BBP is used immediately on this product, hackers will start reporting a large number of vulnerabilities and for each vulnerability there is a price. It is possible that a company will pay a very high amount in a very short period of time, much more than what to be paid for a Pen Test. For this reason, the second recommendation is to adopt BBPs after pen testing.

Experts advise to start with pen testing, and then use BBPs to find additional vulnerabilities. With pen testing, companies pay a fixed amount and are able to find the major security flaws. For this reason, companies should do a pen test so that most of the bugs are eliminated upfront, and then have their product onto the bug bounty. Because if they rely completely on a bug bounty and they have pay for all the bugs, then a pen test might be cheaper.

Moreover, administrating a BBP can be very demanding for firms that have little experience with crowdsourced security, or in general with security practices. For this reason, experts recommend to companies not familiar with these topics, to start with the help of security platforms. Platforms, present the benefits that there is always an experienced researcher who helps companies to validate every type of vulnerability. Moreover, they have a reporting system where it is easier for companies to manage vulnerabilities. Platforms can also make this easier to attract hackers and to invite skilled researchers. Otherwise, firms have to ask themselves if they want to do all of this by themselves, instead of just paying a platform company.

Finally, experts recommend to all companies that have never adopted BBPs, to start with small trials. Particularly with the help of platforms. The recommendation for companies is to take a small tour around the different programs available on platforms such as HackerOne or BugCrowd. Then start BBPs in a controlled manner, setting a small budget and seeing what happens. In particular, interviewees believe that all companies should test security with BBPs, especially for consumer IoT devices that are part of the private life of people. The interview results are presented in Table 12, followed by the interview data.

Table 12. Best Practices for Integrating Bug bounty Programs into Security.

Best Practices for Integrating Bug Bounty Programs into Security

Be Already Active with Vulnerability Management Practices	Companies should be already active with vulnerability management practices and should trust their level of security before implementing a BBP. Otherwise, BBP can turn into a very expensive and ineffective approach for companies to identify vulnerabilities. Expert G states: “*If you have just designed a device and never tested it, starting a bug bounty program would not be my recommendation. Because people will identify a lot of vulnerabilities, and that will cost the company a lot. I think that is when bug bounties are wrong, because then they are more money than a pen test*”.
Adopt Bug Bounty Programs After Pen Testing	Expert's advice is to start with pen testing, and then use BBPs to find additional vulnerabilities. With pen testing, companies pay a fixed amount and are able to find the major security flaws. As expert E suggests*: "I would recommend in the first place pen testing, not a bug bounty. Companies should do a pen test so that most of the bugs are eliminated upfront, and then have their product onto the bug bounty. Because if they rely completely on a bug bounty and they have pay for all the bugs, then a pen test might be cheaper*”.
Small/Medium Enterprises Should Consider Starting with Platforms	Experts recommend the use of platforms to small and medium-size organizations or in general to all companies that do not feel confident administrating a BBP alone. Expert F states*: “Bug bounties are much more complicated than companies would think. In the case of platforms, there is always an experienced researcher who helps companies to validate every type of vulnerability. Moreover, they have a reporting system where it is easier for companies to manage vulnerabilities. Platforms can make this easier to attract hackers and to invite skilled researchers. For this reason, I think that for small and medium enterprises, they have to ask themselves if they want to do all of this, instead of just paying a company to do it for them*”.
Start with a Small Trial	Experts recommend to all companies that have never adopted BBPs, to start with small trials. Particularly with the help of platforms. As expert E suggests: “*I would recommend companies to just take a small tour around the different programs available on the platforms like HackerOne or BugCrowd. Start where it's all done in a controlled manner. Set a small budget and see what happens. I think that al companies should do something with bug bounties, especially for consumer devices that are part of the private life of people*”.

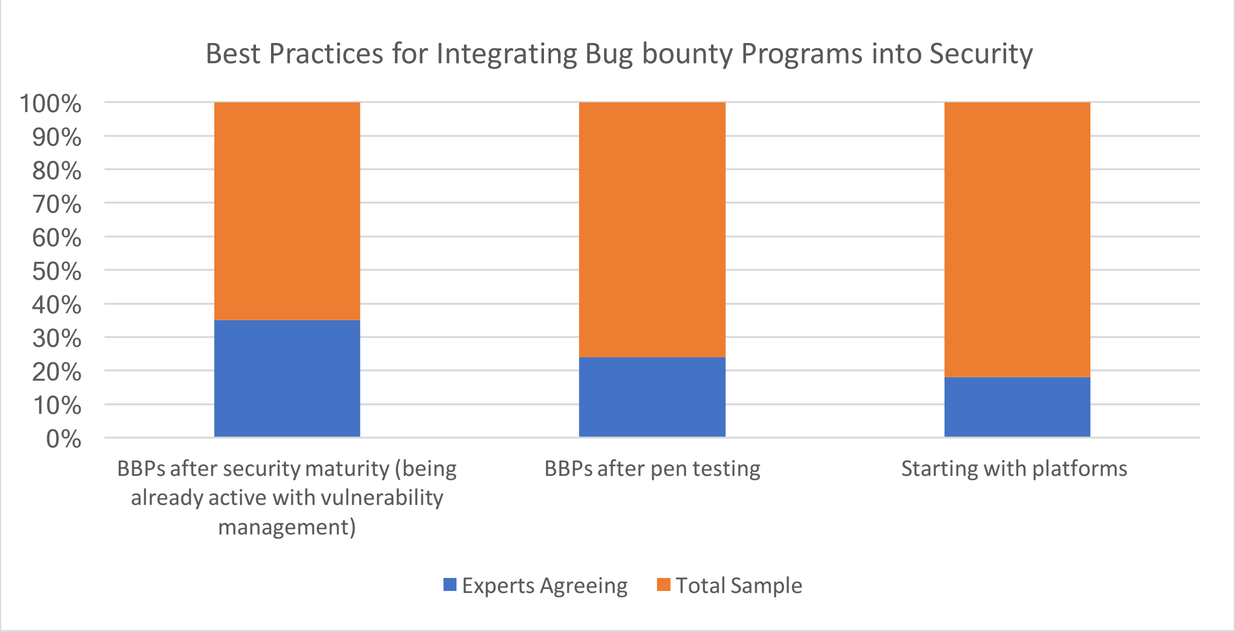


Figure 23. Best Practices for Integrating Bug bounty Programs into Security.

Chapter 5 – Discussion

The defined objective of this research is to derive tangible recommendations for companies developing, manufacturing, and commercializing consumer IoT products, by combining BBP and RD with existing security practices to further boost overall IoT security. In this chapter, an answer is provided to the research questions. By linking the categories, comparing them, and seeking contrasts with the data in the literature, we attempt to provide a logical explanation for the observed patterns and to determine our conclusions. We start by providing the answers for each of the sub-research questions that have been formulated in Chapter 1. Thereafter, we state the conclusion for the thesis main research question. This is followed by a discussion of the results.

5.1 The Current State of Security Practices by Developers, Manufacturers, And Vendors of Consumer IoT Products

In this section, we provide an answer to the sub-question (SQ1): What is the current state of security practices by developers, manufacturers, and vendors of consumer IoT products?

The literature presented in Chapter 2, describes that IoT devices are in most cases vulnerable, due to little security consideration of companies (Singh et al., 2016). In particular, Zhang et al., 2017, suggest that consumer IoT products, might be more vulnerable compared to industrial IoT devices. The same study also describes that enterprises targeting the consumer market, do not have security as a priority, but are generally driven by other business drivers. The interview results confirmed the literature results and provided additional insights.

The data analysis indicates that 58,8% of the interviewees believe that security is not properly implemented by developers, manufacturers and vendors of consumer IoT products. The interview data is reported in Figure 15, from Chapter 4.

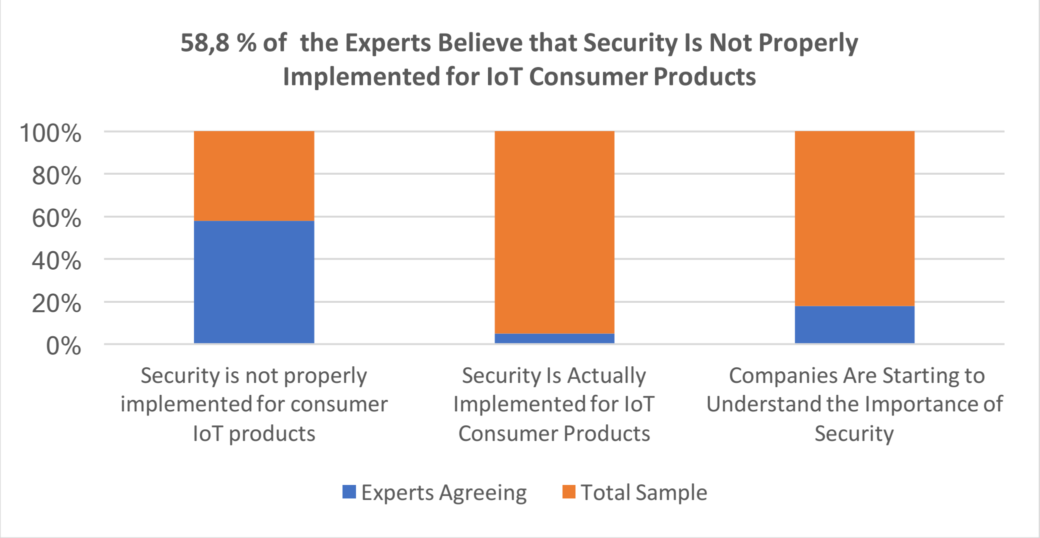


Figure 15. Security in IoT Consumer Goods.

Different Attitudes and Perceptions from Type of Company

However, not all the experts agree on this view. In particular, the interviewees suggest that the attention on security varies between companies.

The results indicate that firm's size, whether the company is a startup or a multinational, does not affect the level of company security practices. In this respect, Zhang et al., (2017), affirmed that most products in the IoT industry are produced by start-ups, which oftentimes lack sufficient resource to build security protection. One of the experts described a similar situation. Expert K reports: "*Most of the new IoT products are an idea of small teams that, after pitching the idea, obtain the support of an investor. At that point, for the startup, the issue is becoming the first one on the market. So the main focus in on mass production, cheap components, and as soon as they implement a functional software they launch it on the market without security*". However, the rest of the experts believe that being a small company does not prevent firms to invest in security. There are many practices, included crowdsourced security, that companies with limited resources can adopt even with little budget. We discuss some of these practices in the next sections.

On the other hand, company age and industry might affect the security attitude of firms. In fact, few experts believe that technology startups might understand the importance of security better than old established companies. Moreover, experts report that there are market sectors where companies are more likely to address security given the higher risk of facing reputational repercussions by product security incidents. These include consumer IoT products such as medical devices and cars. In addition, devices design to be adopted in sensitive environments, such as military and banking sector are also more secure. However, according to the experts, consumer goods are not security driven as the previous sectors. In particular, expert C mentions: "*I do not see any driver for security in consumer IoT products at this moment*". The results present that 35,5% of the experts consider that consumer goods are more exposed to vulnerabilities than other sectors (see Figure 16).

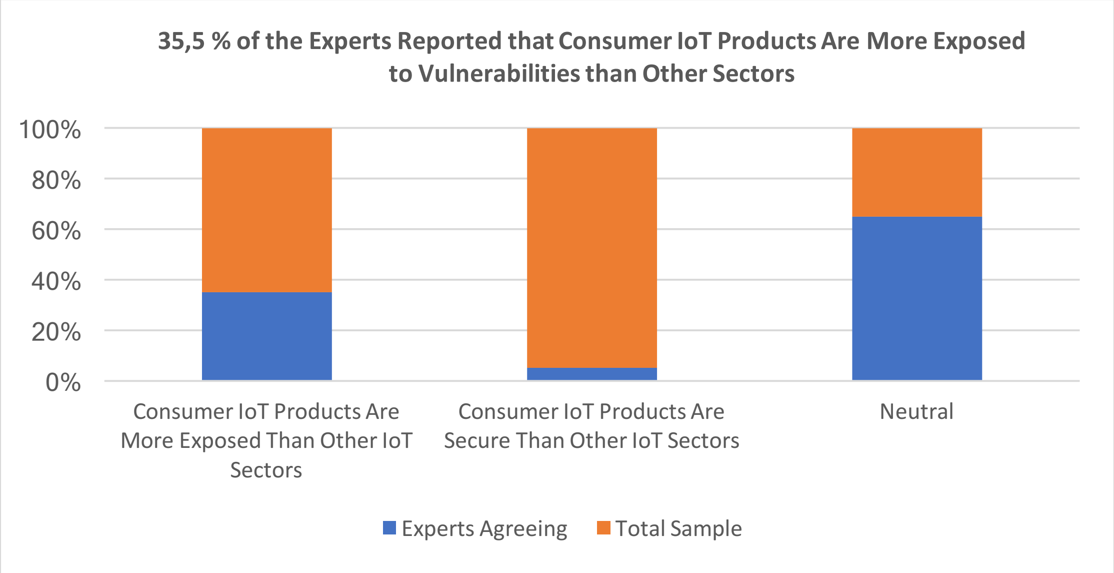


Figure 16. Consumer IoT Products Are More Exposed to Vulnerabilities than Other Sectors.

Lastly, few experts (24%) reported that nowadays the attitude of companies towards security might be improving. In particular, one of the experts, interviewee J, held a strong contrasting opinion on the security state of consumer IoT devices: "*I think there is the idea for which consumers are not paying for security. Therefore, companies cannot invest in it. If they do, products will be more expensive and they will go out of the market. I think that is a traditional view. But in many cases that is changing, especially in consumer products. I think there are a lot of customers who start asking about security and if the vendors don't provide it then they go out of the market*". However, we believe that the number of companies active with security in the consumer IoT market is still limited.

5.2 Causes for the Lack of Security in Consumer IoT Products

In this section, we provide an answer to the sub-question (SQ2): What are the reasons for the lack of security practices by developers, manufacturers, and vendors of consumer IoT products?

There are different studies that we identified in the literature investigating the reasons for the lack of security in IoT. The results from our interview study confirmed many of the literature findings and presented additional insights. In particular, the literature indicates the presence of a multi-actor problem due to the involvement of several firms in the value chains for IoT products, where firms mistakenly assume that someone else in the supply chain addressed the product security. Another major problem is rooted in the lack of understanding of the technological implications of IoT by companies. According to the expert interviews, the current lack of security in IoT is the result of the absence of security awareness both from companies and consumers. As stated by expert O: "*There are all sorts of reasons behind the poor security in IoT, but fundamentally, it all comes down to a lack of understanding and awareness on the importance of security*". We elaborate that the lack of awareness is the reason for added problems, such as companies failing to understand IoT security, the scarce security demand from costumers, and the lack of regulation on consumer IoT goods. As a consequence, we believe that sufficient incentives for companies to invest in security are missing. Our root-cause analysis is presented in Figure 24.

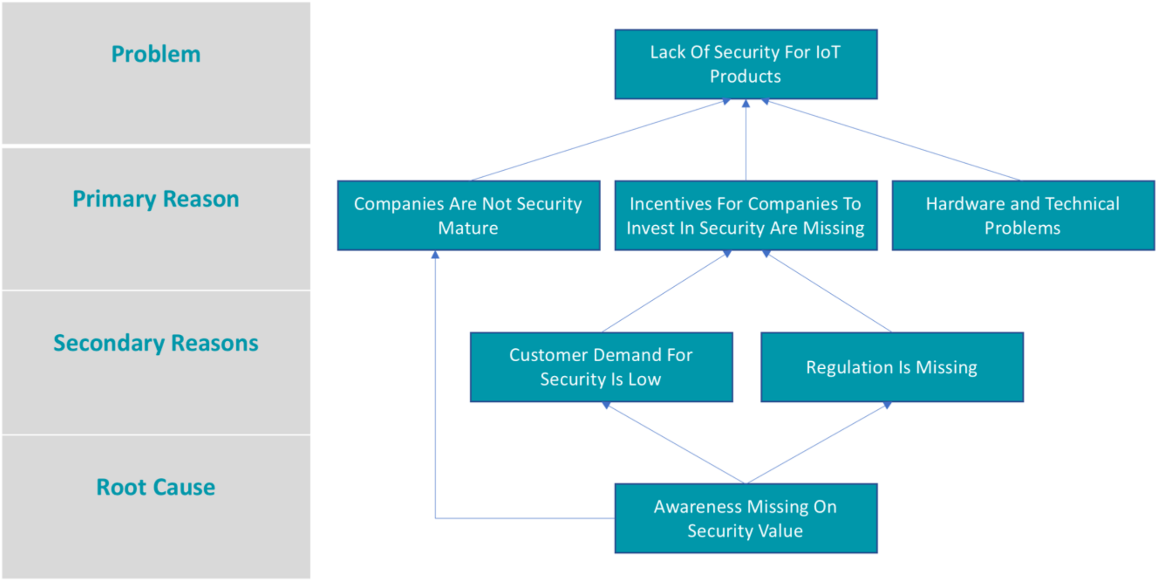

Problem
Primary Reason
Secondary Reasons
Root Cause
Lack Of Security For IoT Products
Companies Are Not Security Mature
Incentives For Companies To Invest In Security Are Missing
Hardware and Technical Problems
Customer Demand For Security Is Low
Regulation Is Missing
Awareness Missing On Security Value

Figure 24. Root Cause Analyses on the Reasons for the Lack of Security in IoT Products.

The Lack of Incentives to Invest in Security

Our analysis indicates that companies lack the incentive to invest in security. The reasons for the lack of incentive comes from the attitude of consumers, that fail to demand companies for secure products, and from the competitive pressure that pushes enterprises to be constantly innovative.

The same first issue is already reported by McFadden et al., in 2019. According to their research there is asymmetric information for which consumers do not recognize IoT products with good security. Therefore, manufacturers are not rewarded by consumers for investing in effective security measures. The interviewees, state that companies do not invest in security because they do not perceive it as beneficial in terms of returns. According to expert H: "*IoT manufacturers do not want to create secure products. The reason is that security is not something that pays back. It only costs money, but actually, the client does not pay for it*". In order to have secure products, customers need to demand and reward companies for secure IoT products.

A second problem recognized by Lee and Lee, 2015, is the technological, societal, and competitive pressure pushing enterprises to be constantly innovative. In this context, investing in security might be perceived as a costly and time-consuming obstacle. In particular, Zhang et al., 2017, describe that enterprises targeting consumer products do not have security as a priority and are generally driven by time-to-market, and that their priority is to develop functional rather than secure products. Accordingly, the experts report that companies that want to stay on top of the market need to be first commercializing new ideas. For this reason, companies focus on time-to-market as expert K describes: "*The problem with IoT is that most of the companies want to be fast at developing products, to be the first ones on the market. For this reason, most often security is just cut out*". Moreover, due to the growing number of IoT products on the consumer market, companies need to develop better features than competitors to attract consumers. As mentioned by expert B: "*The problem in IoT is that now there are more and more devices that are available for people. This causes issues that companies will spend more time implementing nice features, rather than look into product security*".

Companies Fail to Understand the Importance of Security

The empirical results describe that companies fail to understand the importance of security practices and have premature security measures in place. The reason might be rooted in the lack of understanding of the technological implications of IoT. Gartner indicates that IoT security might be beyond the understanding of the average IT manager's skill set (Gartner Inc., 2017). In order to address IoT product security, companies and technology managers need to have an understanding of different technical aspects. Frequently, companies investing into IoT, in particular startups, lack all this knowledge (Zhang et al., 2017). Moreover, our results present that companies might lack the required expertise to understand the security implications of IoT technology. The interviewees report that companies in IoT have very limited expertise in security practices. Experts mentioned that most of the companies are not "mature" in terms of security and they do not test the security of their device. According to expert I: "*The problem is that most of the companies are still in a very immature. So they have some kind of security process, but they still need to improve*".

The Hardware-Related Problems

According to Pen Test Partners, 2018, a further issue, is that once products are on the market, there are security flaws that cannot be fixed through product updates. For this reason, the products remain insecure in the hands of consumers. The same problem is reported in our expert interviews. According to expert H: "*In IoT security, it is infinitely more complicated to fix bugs, because there is usually no way to install security updates and patches*". Normally, in software security, after a vulnerability is identified, companies are able to release software updates to improve the security of a device. In the case of IoT, it is often not possible to do the same to fix vulnerabilities in the hardware. Moreover, the interview results indicate the hardware is one of the most important elements affecting the degree of security in IoT. For this reason, companies should test hardware security before the product launch. However, the results suggest that companies are not aware of the importance of testing the hardware. As expert B mentions: "*I think right now companies do not invest in securing the hardware*".

The Lack of Regulation

The lack of regulation is also one of the reasons limiting the action of firms. Pen Test Partners, 2018, reports that there is a lack of standards and guidance for IoT security. Accordingly, the experts' opinion collected describes that there is no regulation on consumer IoT products. Expert O reports: "*There is no regulation. We are reliant on protecting the data based on the GDPR, that is useful. There are some European state laws that are useful as well. But there are no strict regulations around the Internet of Things security".*

Finally, we present the results from the data analysis on the reasons for the current lack of security in consumer IoT products.

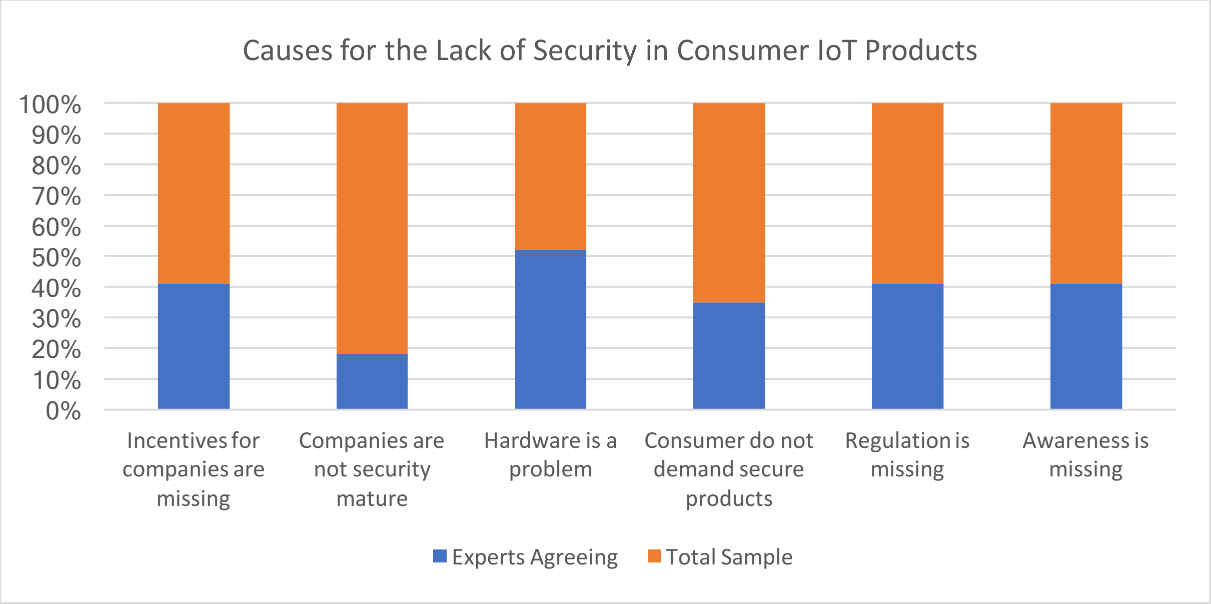


Figure 17. Causes for the Lack of Security in Consumer IoT Products.

5.3 Crowdsourced Security Methods in IoT

In this section we answer the sub-research question (SQ3): What is the current state of Bug Bounty Programs and Responsible Disclosure in IoT, including the rate of adoption, benefits, limitations, and potential barriers?

In order to boos security, firms and governments are finding in ethical hacking a powerful tool to fight security threats. However, from the literature analyses, we concluded that the research concerning the adoption of crowdsourced security for IoT is still scarce. In particular, the state of adoption, benefits, limitations, and barriers for adopting BBP and RD in IoT deserved a thorough investigation. The results from the expert interviews present several insights regarding this yet unexplored sphere.

5.3.1 Benefits and Limitations of Responsible Disclosure and Bug Bounty Programs

Empirical studies from the literature indicate that RDPs and BBPs cost-effectively contribute to vulnerability management practices of organizations. Crowdsourced methods have the advantage of engaging with broad communities of hackers resulting in greater chances to discover different types of vulnerabilities given the disperse skillset of the participants. In this section we present the results from the expert interviews on the benefit and limitations of these methods.

- *Benefits and Limitations of Responsible Disclosure*

The literature described that many vulnerabilities are typically discovered by benign users (Cavusoglu et al., 2005). In this context, individuals might feel responsible for reporting the vulnerability to the organization. However, several times, companies lack a dedicated channel for individuals to report vulnerabilities. In this case, we identified 3 possible scenarios from the work of HackerOne, 2018.

- **Failed disclosure:** After looking for and not finding an appropriate contact, the hacker gives up. HackerOne, 2018, indicates that approximately 1 in 4 of discovered vulnerabilities are not reported by hackers because companies lack a RDP.
- **Vulnerability is reported but information is lost:** Even in the cases where a vulnerability is correctly reported, the information can get lost. Eventually, only in some cases the security team will be informed about the vulnerability.
- **Full disclosure:** After looking for and not finding an appropriate contact, the hacker will release the information publicly online without coordinating with the company.

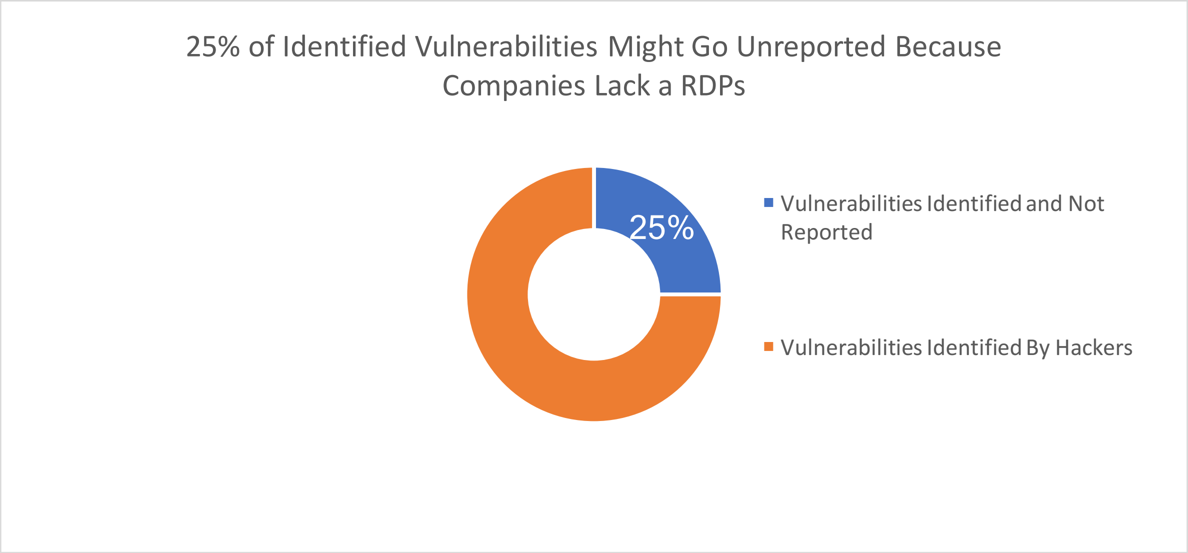


Figure 25. Vulnerabilities Not Reported by Hackers Because Companies Lack a RDP (Hackerone, 2018).

Consequently, without a RDP, reporting vulnerabilities might result in a very complex (see Figure 11). The main benefit of RD is providing a convenient solution to the aforementioned issue. As reported by HackerOne, 2018, with RDPs firms benefit from nearly free advice of ethical hackers to enhance their security. The interview results are in line with the previous statement. As expert C claims: *"I would personally say that responsible disclosure is a quick win to get free advice and avoid some reputational damage*". Experts identify many benefits from responsible disclosure. In particular, they believe that companies, ethical hackers, and society, all benefit from RD. Companies get free advice and avoid some reputational damage. Ethical hackers benefit from legal protection. Society benefits because zero-day vulnerabilities are prevented.

However, the results indicate that a limitation of RD is that researchers may lack incentives to engage with it. According to expert E: "*The problem of responsible disclosure is that it pays you nothing for your time, but still it expects you to provide details about the vulnerabilities you find"*. Moreover, according to some interviewees, RD is not supposed to be considered as a security testing method. For this reason, it cannot ensure security coverage like pen testing or other methods does.

Benefits and Limitations of Bug Bounty Programs

There are different benefits reported in the literature regarding BBPs. Finifter et al., 2013, suggested that BBPs are a more costed-effective method to identify vulnerabilities compared to conventional methods. Several interviewees stated that BBPs provide cheaper and more accurate results than pen tests. Expert Q reports: "*Bug bounty programs give companies almost a free pen test from several people and a fresh perspective on how to hack their product*". Moreover, BBPs have the advantage of engaging with broad communities of hackers resulting in greater chances to discover different types of vulnerabilities given the disperse skillset of the participants (Finifter et al., 2013). Our empirical results suggest the same. According to expert D: "*With bug bounties, there is always going to be high chances that researchers find some vulnerabilities. Because if you have a hundred people, and passionate people because they would not be* *there otherwise, then you will have more results than a pen test*". According to the majority of experts, BBPs are very beneficial tools for companies to test security. In addition, by finding vulnerabilities before they are exploited, companies can protect their reputation and avoid having to pay for any damage to consumers in the case they get hacked.

While empirical results present that BBBs have a significant potential to contribute to security, there are also several obstacles for companies in running these programs. Research describes that there is abundant noise that companies need to manage resulting from low-value reports (Lazka et al., 2016). In 2018, Laszka et al. presented that the percentage of invalid reports commonly ranged between 35% and 55%. Another challenge consists of efficiently distribute valuable but scarce hacker effort across organizations over time.

Table 7. The Benefits and Limitations of Responsible Disclosure and Bug Bounty Programs.

	Benefits of Responsible Disclosure
For Companies	▪ Prevents irresponsible disclosure
	▪ Helps to attract people that want to enhance your security
	▪ Companies benefit from almost free advice
	▪ Protects reputation
For Ethical Hackers	▪ Guards against the risk of legal persecution
For Society	▪ Zero-day vulnerabilities are prevented
	Limitations of Responsible Disclosure
For Companies	▪ Is does not ensure security coverage
	▪ Incentives are not sufficient to attack hackers
For Ethical Hackers	▪ It pays researchers nothing for their time but still expects them to provide detailed reports
	Benefits of Bug Bounty Programs
For Companies	▪ Allow to effectively engage with security researcher communities
	▪ Provide an almost inexpensive form of pen testing
	▪ Protect companies' reputation and to avoid financial repercussions from security incidents
For Ethical Hackers	▪ Allow to making a living out of bounties

5.3.2 The Adoption of Responsible Disclosure and Bug Bounty Programs in IoT

The data from the literature survey and the expert interview provided us with limited information on the adoption rate of RD and BBPs in IoT. The literature data presents that RDPs are implemented by very few organizations. Every year, HackerOne realizes a survey study to investigate the adoption of RDPs among the companies listed in the Forbes Global 2000. The results from 2017, indicate that only 7% of the organizations adopted RDPs. For RD, we were not able to collect any IoT specific data.

Regarding the adoption of BBPs, the literature describes that these programs are becoming a significant part of organizations' security ecosystem. Gartner Inc., predicts that by 2022, BBPs and crowdsourced methods will be employed by more than 50% of enterprises up from less than 5% today (Gartner Inc., 2018). However, the majority of the current bug bounties is directed towards website vulnerabilities, and more in general software applications (HackerOne, 2018). According to data collected by HackerOne, 2018, less than 2% of the hackers registered on their platform research security flaws in IoT (see Figure 14). Interestingly, from one of the interviews, the same rate of adoption was mentioned for BBPs in IoT. Expert G states: "*Bug bounties in IoT are already running right now. However, my calculated guess is that only 2% of the entire bug bounty is done for IoT. So it is not a large amount*". From our research, we conclude that the rate of adoption of BBPs for IoT devices is marginal.

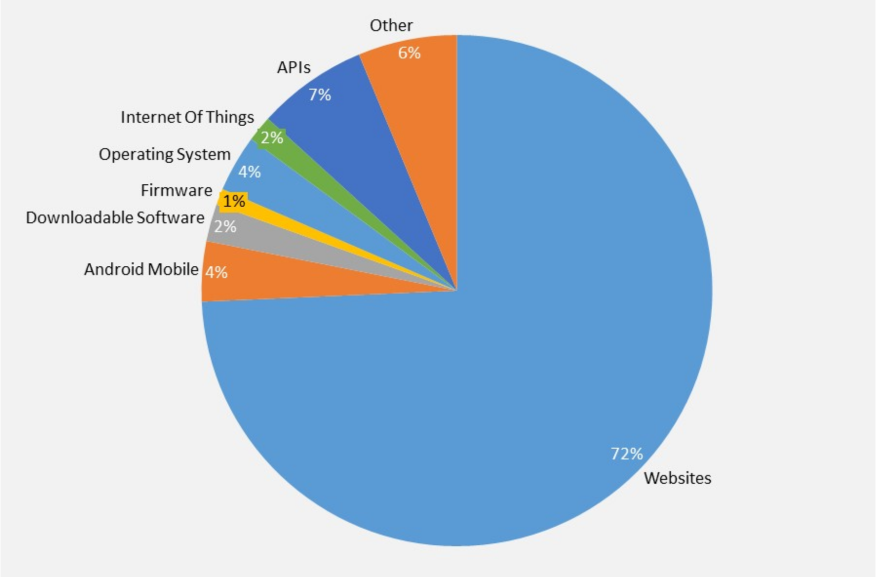


Figure 14. What Hackers on HackerOne Hack for Bounties (HackerOne, 2018).

5.3.3 The Reasons for the Limited Adoption of Responsible Disclosure and Bug Bounties in IoT

Regarding the reasons for the limited adoption of crowdsourced methods in IoT, we were not able to collect any data from the literature. However, the results provided us with several new insights.

The experts describe that there are companies that still do not understand or see the benefits of crowdsourced methods. Crowdsource security has only recently gained the attention of the cybersecurity industry, and it seems to be still too radical as an approach for many companies. In particular, some of them are still very aggressive against ethical hackers that report vulnerabilities.

Looking into more specific IoT problems, the results describe that ethical hackers lack incentives for participating in RDPs and BBPs for IoT. In this respect, we identify one of the main barriers for the scalability of BBPs in IoT, consisting of the "hardware obstacle". In the case of BBPs for IoT products, researchers need to have physical access to the device to test the hardware. The problem is that for practical reasons companies cannot provide physical devices to all of the researches willing to participate in BBPs. At the same time, researchers miss sufficient incentive to buy the products themselves for testing them. In addition, in order to hack IoT, hardware hacking skills are needed. However, the experts state that there are limited people with such skills at the moment. The previous obstacles could also be a reason for the minimal employment of bug bounties in the field of IoT.

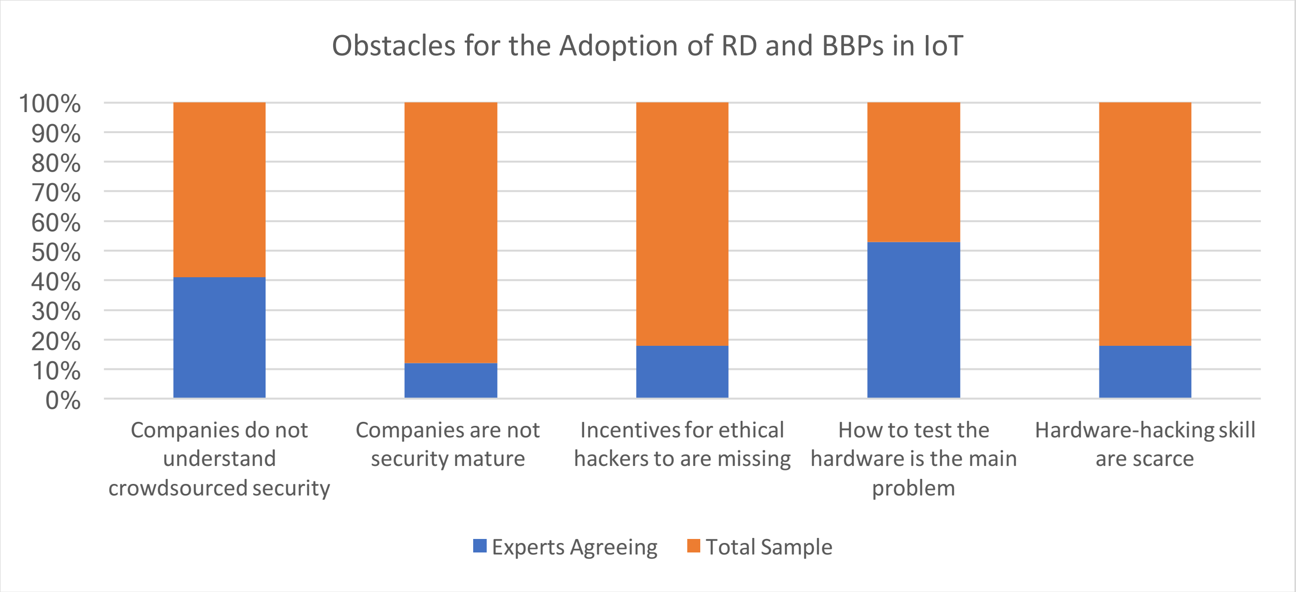


Figure 18. Obstacles for the Adoption of RD and BBPs in IoT.

Possible Solutions for The Adoption of Bug Bounty Programs in IoT

Previously, we described that the key problem that companies have to solve in order to adopt BBPs in IoT is how to provide hackers with the devices. Even though companies cannot deliver the hardware to researchers individually, they can still try to create events where hackers can join to participate in bug bounties. In this case, they can set up events, such as hackathons, where hackers are invited to test the security of IoT products. Moreover, instead of organizing the events by themselves, companies can also join security conferences and invite participants to find vulnerabilities in their products in exchange for rewards. However, the previous two solutions do not allow companies to directly control who gets access to their devices. There might be some situations where companies have some critical assets, and they actually do want to select skillful individuals to test their technology. In this case, companies can set private BBPs where a limited number of hackers are selected to test the device. Otherwise, companies can still use BBPs to test the software of IoT products. The identified solutions are listed in Figure 25.

- Create Events Such as Hackathons
- Employ Security Conferences
- Offer Private Bug Bounty Programs
- Provide More Incentives to Researchers
- Employ Bug Bounties to Test Software

Figure 25. Possible Solutions for BBPs in IoT.

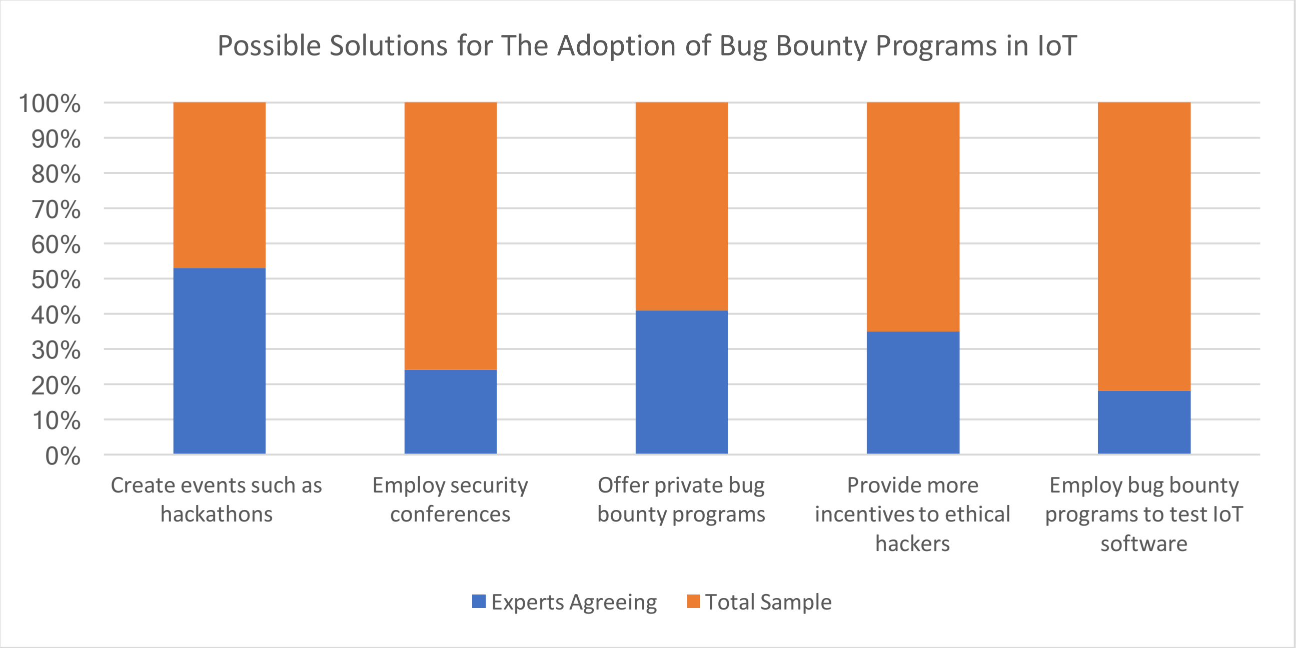


Figure 19. Possible Solutions for The Adoption of Bug Bounty Programs in IoT.

Limitations of The Proposed Solutions

The aforementioned solutions present limitations. At the moment, all the bug bounties and responsible disclosures are based on scalability and trying to get over as many researchers as possible. By limiting BBPs to only physical gatherings we out scope the majority of researchers that work on bug bounties from other countries, such as India. The experts state that there is very few that can be done to solve this problem. To test IoT devices researchers need access to the device. Also, very few people know how to hardware hacking. Moreover, few people are motivated to buying the device in order to participate in BBPs.

5.4 Integrating Bug Bounty Programs and Responsible Disclosure with Conventional Security Practices to Enhance IoT Vulnerability Management

In this section, we state the conclusion for the thesis main research question (MRQ): How can developers, manufacturers, and vendors of consumer IoT products enhance vulnerability management practice with Bug Bounty Programs and Responsible Disclosure?

In order to state the research conclusion, we provide an answer to the last 3 sub-research questions:

(SQ4). What are the potential best practices for companies to enhance the vulnerability management of IoT products?

(SQ5). How can companies leverage Responsible Disclosure and integrate them with conventional security solutions to enhance the vulnerability management of IoT products?

(SQ6). How can companies leverage Bug Bounty Programs and integrate them with conventional security solutions to enhance the vulnerability management of IoT products?

5.4.1 Best Practices for Vulnerability Management in IoT

In order to make the process of vulnerability management easier, the results describe that companies should implement security from the design. The overall idea, is that once those companies realize security from the beginning, it is less likely that they will face vulnerabilities.

Secondly, the experts recommend to always have some kind of security testing practice, in particular pen testing. There are different procedures that companies can apply to test security. As mentioned by expert J, among the security testing practices there are pen testing, red teaming, responsible disclosure, and bug bounties. A best practice consists of the combination of pen testing and bug bounties to test security. According to interviewee O: “M*anufactures should not be launching out products without a very thorough pen test. Additionally, bug bounties should be there to ensure that vulnerabilities that pen test missed are addressed*”. A further recommendation from an organization perspective is to move the budget for security from IT to Risk. In fact, keeping the budget for security within the IT is insufficient to cover the IoT vulnerabilities.

An ideal security process is highlighted by expert J: "*Security should be a parallel process. You build in some tests in your software development life cycle, you do code reviews, you do secure design, and you have security requirements. Then whenever there is a release you do pen testing to make sure you follow a methodical process that validates that the security requirements are indeed implemented. But then in parallel with all of it, you also have a responsible disclosure policy on your website together with a bug bounty. This way you'll be able to cover other classes of vulnerabilities that pen testers missed*".

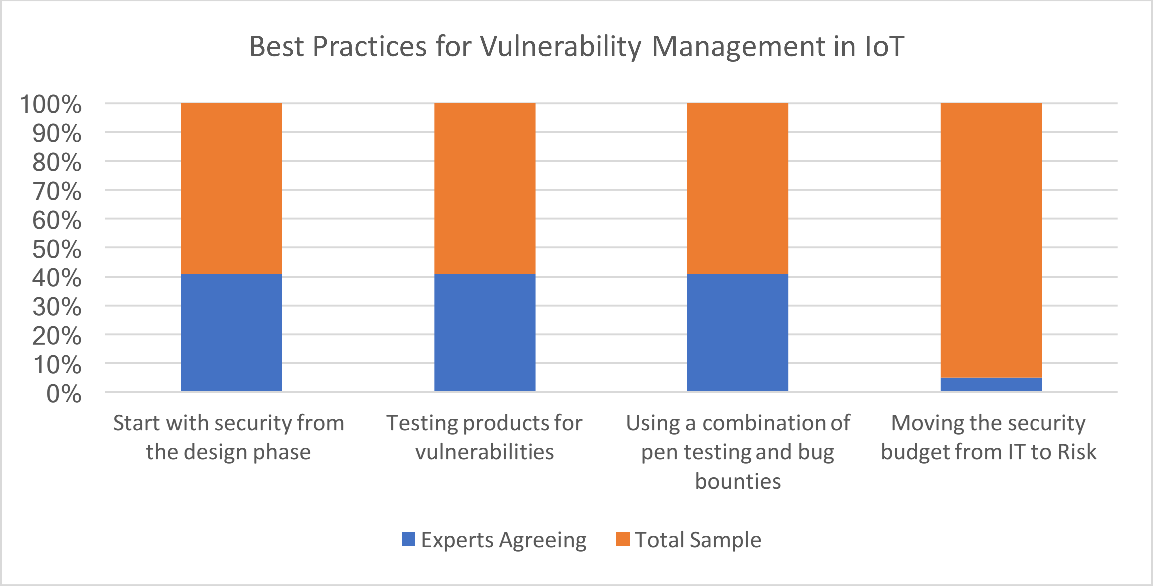


Figure 20. Best Practices for Vulnerability Management in IoT.

5.4.2 Leveraging Responsible Disclosure and Bug Bounty Programs for Vulnerability Management in IoT

In 2017, HackerOne, a report that describes how to plan, launch, and operate a successful BBP (Bacchus, 2017). The company suggests 5 stage process. In this respect, Preparation, Champion Internally, and The Post Program, apply also in the contest of RD:

- **Assessment:** Companies need to assess the bug bounty approach that is best according to their capabilities. Moreover, before starting a BBP, companies should already be active with vulnerability management practices to ensure that a sufficient amount of vulnerabilities have been previously identified and fixed.

- **Preparation:** Companies stating a BBP will have more vulnerabilities to manage. For this reason, organizations need to ensure a solid process to evaluate and fix the vulnerabilities. At the same time, they have to allocate sufficient resources to support the ongoing program.

- **Champion Internally:** Companies need to define a BBP leader that will be responsible for the success of the program. Together with the leader, the company has to create a bug bounty team to take charge of related processes.

- **Launch:** Before launching the program, companies have to consider whether they want to offer a public or private program. Subsequently, the company has to define the scope of the program. The advice for organizations new to BBPs, is to start with small programs. Moreover, it has to be decided whether to adopt the assistance of a platform or launch an independent BBP.

- **The Post Bounty:** Once the company has been able to successfully manage the first BBP, the next step is to scale up. In addition, it is important for companies to identify the internal vulnerability owner that can provide a solution to the vulnerability.

Many of the previously recommended practices are reported also in the expert interviews as presented in Table 11 and Table 12. In particular, the interviewees report that in order to have an effective RD or BBP, the first step is to be open-minded. Many companies nowadays still do not trust this practice and in particular the goodwill of the ethical hackers. Such behavior limits and hinders the effectiveness of crowdsourced security. Secondly, companies need clear policies and clear rules. Finally, and most importantly, firms need to have a process to fix the problem.

Table 11. Best Practices for Responsible Disclosure.

Best Practices for Responsible Disclosure	
Be Open Minded	The first step for a company is to be open-minded. As expert C claims: “*Firms want to protect their products have to realize that it's better for them to be open rather than close to external help*”.
Establish Clear Policies and Rules	It is important to define clear policies and rules. Expert D claims: "*Responsible disclosure is not as straightforward as just putting a website up. Companies really need to think about the process thought. They need to think about which type of vulnerability do they want to be informed. Who is going to take care of it, how much money do they want to spend on it, and how much time”.*
Allocate Resources and Define Processes Around RD	Companies need to allocate sufficient resources and define processes to administrate the RDP. As expert J describes: “*If you are a company and you start a responsible disclosure on your website, then you also need to set up a process around it. You need a detection mechanism, a response procedure in place. If a company does not have this capacity, then it is useless*”.
Patch the Vulnerabilities	Next to the process to analyze the reports, companies need to be able to actually fix the bugs. Expert A points out: "*If you disclose vulnerabilities without a patch, you will give possible attackers the time to exploit the vulnerability and to get access to users' data*”.
Effectively Communicate with Researchers	In order for responsible disclosure to work, companies have to make sure to communicate effectively with hackers. Expert K reports: "*In most cases, hackers submit something but do not get any response. And then the hacker gets angry and releases the information. Then companies have a problem. But if you keep in contact with them, you can make it work*".
Reward Researchers	Companies need to reward hackers for their effort in order for these individuals to stay motivated. Benefits that companies can offer can be public recognition, objects, or even money. According to the expert G: “*There should be a benefit in responsible disclosure for the researcher. It can also be giving credit and recognition. People care for status, and that motivates people to keep on searching. Otherwise, only a much small subset of people will look at your security*”.

Table 12. Best Practices for Integrating Bug bounty Programs into Security.

Best Practices for Integrating Bug Bounty Programs into Security	
Be Already Active with Vulnerability Management Practices	Companies should be already active with vulnerability management practices and should trust their level of security before implementing a BBP. Otherwise, BBP can turn into a very expensive and ineffective approach for companies to identify vulnerabilities. Expert G states: “*If you have just designed a device and never tested it, starting a bug bounty program would not be my recommendation. Because people will identify a lot of vulnerabilities, and that will cost the company a lot. I think that is when bug bounties are wrong, because then they are more money than a pen test*”.
Adopt Bug Bounty Programs After Pen Testing	Expert's advice is to start with pen testing, and then use BBPs to find additional vulnerabilities. With pen testing, companies pay a fixed amount and are able to find the major security flaws. As expert E suggests*: "I would recommend in the first place pen testing, not a bug bounty. Companies should do a pen test so that most of the bugs are eliminated upfront, and then have*

	their product onto the bug bounty. Because if they rely completely on a bug bounty and they have pay for all the bugs, then a pen test might be cheaper".
Small/Medium Enterprises Should Consider Starting with Platforms	Experts recommend the use of platforms to small and medium-size organizations or in general to all companies that do not feel confident administrating a BBP alone. Expert F states*: "Bug bounties are much more complicated than companies would think. In the case of platforms, there is always an experienced researcher who helps companies to validate every type of vulnerability. Moreover, they have a reporting system where it is easier for companies to manage vulnerabilities. Platforms can make this easier to attract hackers and to invite skilled researchers*. *For this reason, I think that for small and medium enterprises, they have to ask themselves if they want to do all of this, instead of just paying a company to do it for them*".
Start with a Small Trial	Experts recommend to all companies that have never adopted BBPs, to start with small trials. Particularly with the help of platforms. As expert E suggests: "*I would recommend companies to just take a small tour around the different programs available on the platforms like HackerOne or BugCrowd. Start where it's all done in a controlled manner. Set a small budget and see what happens. I think that al companies should do something with bug bounties, especially for consumer devices that are part of the private life of people*".

Moreover, in the case of RDPs, companies have to keep in mind that is very important to maintain an effective communication with hacker throughout the whole reporting process. Companies need to reward hackers for their effort in order for these individuals to stay motivated. Finally, before starting with responsible disclosure or bug bounties companies should make sure to have some product security already in place. This point is made more clear in the next section.

Additional Recommendations for the Integrating of Bug Bounty Programs into IoT Security Practices

Before starting with BBP, companies should already be active with vulnerability management practices to ensure that a sufficient amount of vulnerabilities have been previously identified and fixed. Otherwise, BBP can turn into a very expensive and ineffective approach for companies to identify vulnerabilities.

In the case of companies that developed a product and never tested it, the untested product will typically have many vulnerability issues. When BBP is used immediately on this product, hackers will start reporting a large number of vulnerabilities and for each vulnerability there is a price. It is possible that a company will pay a very high amount in a very short period of time. As expert G states: "*If you have just designed a device and never tested it, starting a bug bounty program would not be my recommendation. Because people will identify a lot of vulnerabilities, and that will cost the company a lot. I think that is when bug bounties are wrong, because then they are more money than a pen test*". To illustrate the cost related with a BBP in the event that a company has never tested the product's security, we present a theoretical graph in Figure 26. We note that there is no supportive data to validate the form and steepness of the cost curve.

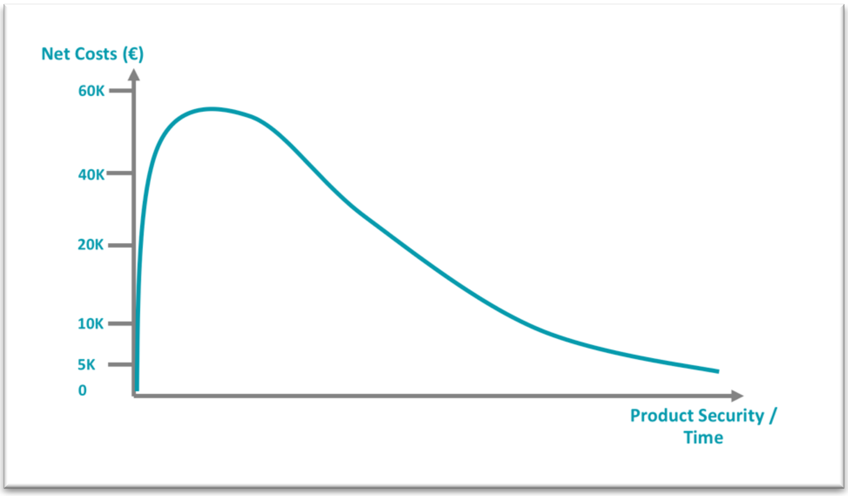


Figure 26. The Cost Curve of a BBP for a Product Never Tested.

In this respect, the literature reports that there is a key challenge of BBPs for companies, presented by a substantial number of invalid reports submitted by hackers (Lazka et al., 2016). In particular, Lazka et al., 2016, have attributed such problem to misaligned incentives for validating reports in BBPs. We argue that the reason for the large numbers of invalid reports might be rooted in the incorrect adoption strategy of BBPs by companies. As our results present, once a firm starts a BBP for a product that has never been tested, hackers will immediately start reporting a large number of vulnerabilities. Instead, once companies have previously identified the majority of the vulnerabilities, for instance with a pen test, we suppose that the number of low-value reports in a BBP would decrease. This lead to our second recommendation: adopt BBPs after pen testing. Experts advise to start with pen testing, and then use BBPs to find additional vulnerabilities. With pen testing, companies pay a fixed amount and are able to find the major security flaws. For this reason, companies should do a pen test so that most of the bugs are eliminated upfront, and then have their product onto the bug bounty. Because if they rely completely on a bug bounty and they have pay for all the bugs, as described previously, then a pen test might be cheaper.

Based on the previous advice, our final recommendation is to launch BBP after a certain state of maturity. Before starting with BBP, companies should already be active with vulnerability management practices to ensure that a sufficient amount of vulnerabilities have been previously identified and fixed. Our suggestion of adoption sequence of security design, integrating conventional testing methods, such as pen testing, followed by crowdsourced approaches (see Figure 27).

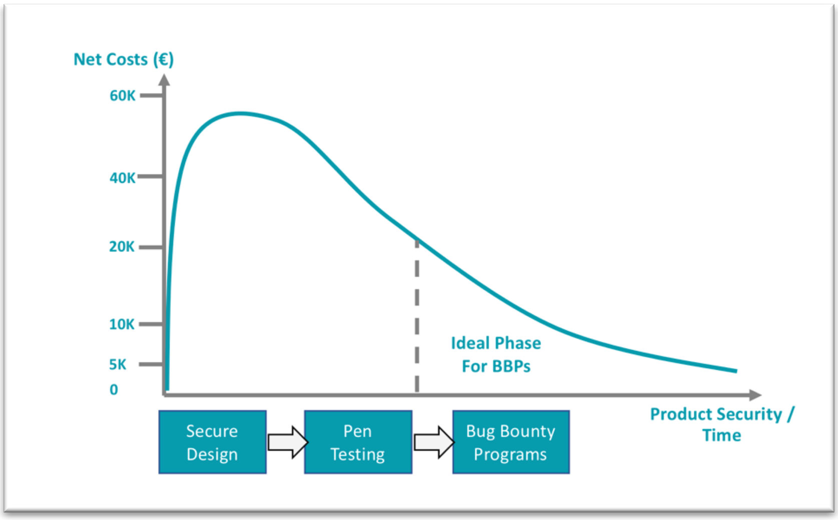


Figure 28. Recommended Adoption Strategy for BBPs.

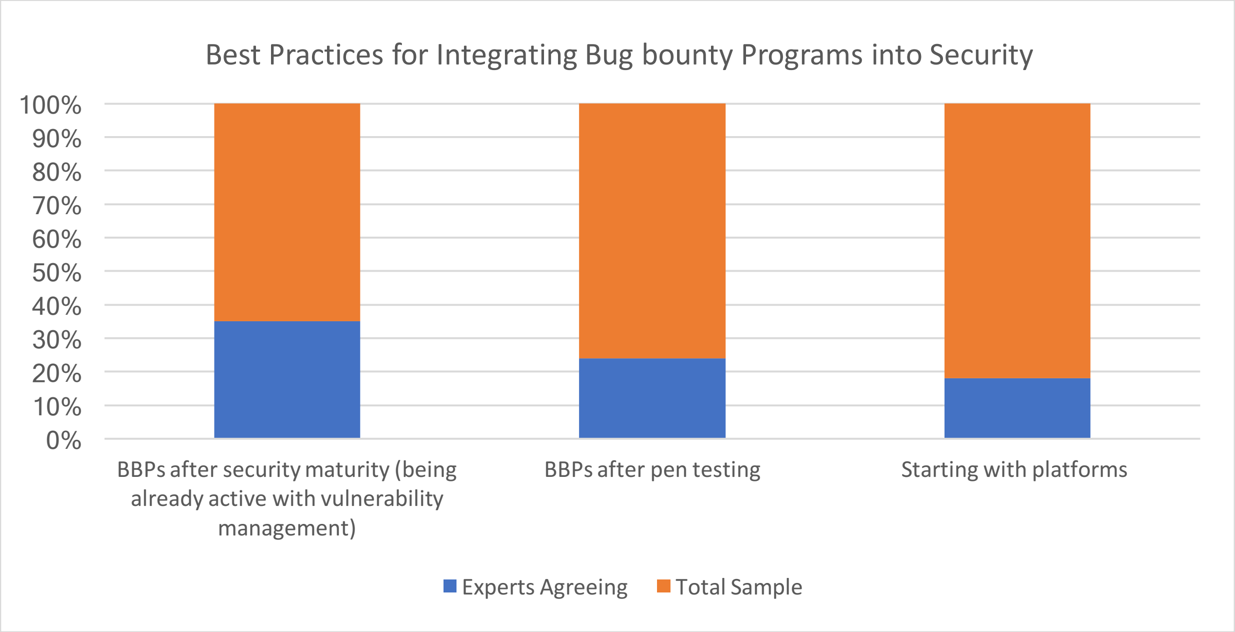


Figure 23. Best Practices for Integrating Bug bounty Programs into Security

5.4.3 Responsible Disclosure and Bug Bounty Programs Are a Best Practice for Vulnerability Management in IoT

Finally, we present the results recommending the implementation of RD and BBPs to all type of companies, in particular for those dealing with IoT. The literature review indicated that RD and BBPs effectively contribute to vulnerability management practices, and typically result in more cost-effective deals for organizations (Laszka et al., 2018; Gartner Inc., 2018; Finifter et al., 2013). In 2018, Gartner Inc.

reported that crowdsourced security testing methods have confirmed their ability to effectively augment existing security testing applications. As a result, the adoption of crowdsourced methods by organizations is growing. Granter Inc., predicts that by 2022, approximately 50% of companies will employ BBPs and related services as security testing practices (Gartner Inc., 2018). In our study we investigated the potential of adopting crowdsources security for IoT vulnerability management. The results from our research indicate that RD and BBPs are indeed a best practice to enhance the vulnerability management of IoT devices. According to expert C: *"Responsible disclosure definitely benefits companies. Especially with IoT technology. In IoT, there are too many relation and multiple places where you can make an error. This is unavoidable. So then as a company, you should be open for the feedback. It is free advice. And it really improves the quality of your products and protects your reputation*". Moreover, expert E mentions: "*I would say bug bounty is beneficial for every company because IoT is a critical asset. I would call it critical because accidents in IoT could really cause physical damage. So for whatever the company type, whatever the company assets, I would recommend it*".

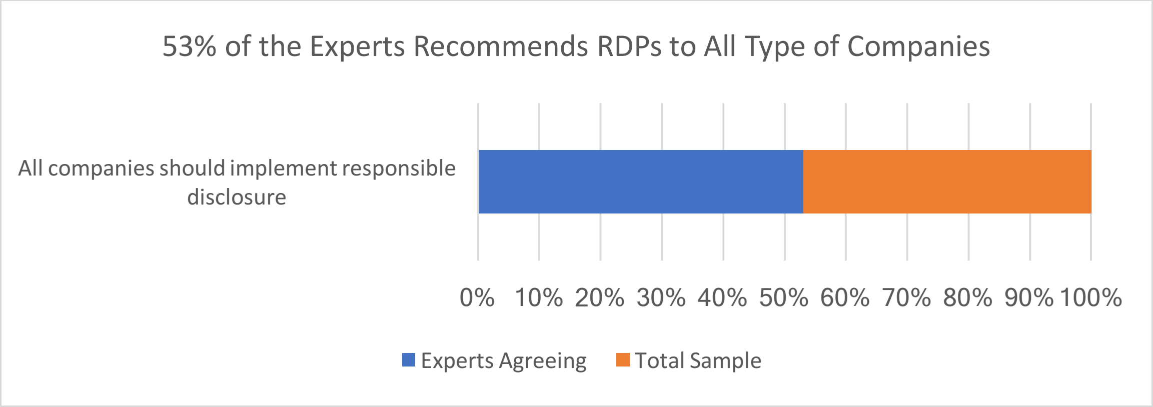


Figure 21. Experts Recommending Responsible Disclosure to All Type of Companies.

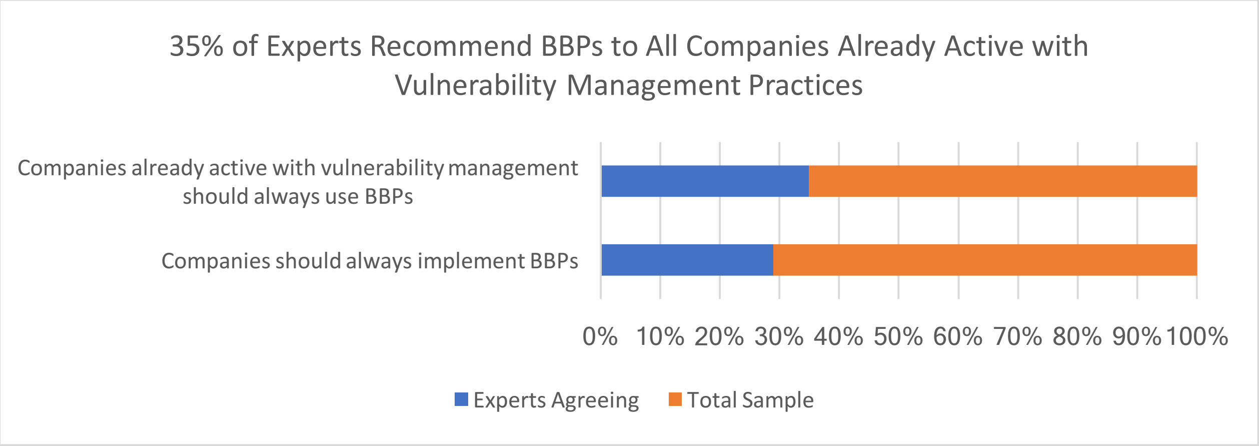


Figure 22. Experts Recommending the Adoption of Bug Bounty Programs to Companies.

5.5 Chapter Conclusion

To tackle our research question “How can developers, manufacturers, and vendors of consumer IoT products enhance vulnerability management practice with Bug Bounty Programs and Responsible Disclosure?”, our main recommendation is that companies should implement security from the design of products. Then whenever there is a release you do pen testing to make sure you follow a methodical process that validates that the security requirements are indeed implemented. But then in parallel with all of it, you also have a responsible disclosure policy on your website together with a bug bounty. This way you'll be able to cover other classes of vulnerabilities that pen testers missed.

In specific to BBP, incentives for both ethical hackers and companies are the most crucial element. In this respect, companies shall take initiative to provide more incentives to researchers through the means of sharing hardware and setting up credit/reputation system to recognize active participation. Our recommendation is to launch BBP after a certain state of maturity. Before starting with BBP, companies should already be active with vulnerability management practices to ensure that a sufficient amount of vulnerabilities have been previously identified and fixed. In implementation, BBP shall be applied after Pen Test to achieve a balance between cost and efficiency of detecting vulnerabilities. For IoT hardware challenge, given that shipping IoT hardware such as a smart car to testers is generally not feasible, we recommend organizing hacking events which can take the form of a live one to two-day hacking events. Such bug bounty event can connect the team from company together with the crowd of ethical hackers in a highly interactive environment to accelerate the discovery of critical vulnerabilities in IoT hardware and software. Alternatively, conferences and private BBPs can also be adopted.

For RD, we recommend the implementation of RD policies to all type of companies, in particular for those dealing with IoT. For companies, being open-minded is a condition to utilize crowdsource ethical hacking. The next step is to define policies for what happens after a vulnerability has been reported. In addition, companies need to define the internal processes to be able to accept and process the incoming reports.

Nevertheless, we acknowledge that security practices are different among countries. Some countries are advanced whereas others are still learning. There are many regions where responsible disclosure and bug bounties are just too sophisticated methods at the moment. For this reason, the recommendations are directed to companies advanced with security practices in western industries. Several of the proposed recommendations might be also generalized to other firms. We believe that the public will be able to determine the extent to which the findings and recommendations can be generalized and applied.

5.5.1 Further Policy Recommendations

To improve the security of consumer IoT devices, action will need to be taken by stakeholders, including companies, consumers, and institutions. In this study we have presented some recommendations for company action. To be effective, further solutions are expected to involve policymakers and industry to strike a balance between security and allowing innovation within the IoT market (McFadden et al., in 2019).

McFadden et al., in 2019, suggested a number of potential actions to address the security of consumer IoT devices. Many of the proposed action were also identified by the interviewees in this study. Therefore, we present the same recommendations. In particular, they encourage manufacturers to adopt a 'security-by-design', as we also advise in our research. The security measures, concern action against both inward and outward threats, in order to protect both consumers and third parties. The actions are depicted in Figure 29, and are described in greater detail thereafter. They are listed in order of the possible cost and difficulty of implementation. In particular, scholars propose the adoption of vulnerability disclosure, which is one of the main elements of our study. In particular, they also present RD as one of the most viable and cost-effective measures to enhance the security of consumer IoT devices. Additionally to this action, we also recommend the adoption of bug bounty programs.

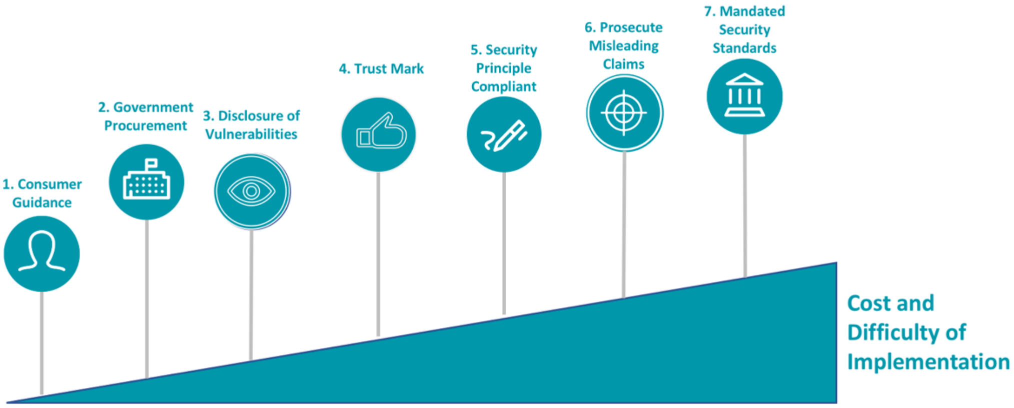

1. Consumer Guidance
2. Government Procurement
3. Disclosure of Vulnerabilities
4. Trust Mark
5. Security Principle Compliant
6. Prosecute Misleading Claims
7. Mandated Security Standards
Cost and Difficulty of Implementation

Figure 29. Potential Actions Against Poor IoT Security (McFadden et al., in 2019)

- **Consumer Guidance:** Industry and policymakers should promote awareness on consumer IoT security, and provide advice to users. In particular, delivering information to consumers on the risks of insecure.
- **Government Procurement:** Governments should leverage their position as major procurers to request companies for improved product security. The developments in security might spill over into the consumer market.
- **Vulnerability Disclosure:** Industry and policymakers should support responsible disclosure of vulnerabilities in consumer IoT. In particular, to reduce the legal risks faced by hackers. Currently, researchers can face legal threats for their actions, as we also present in our study.
- **Trust Marks:** Industry and policymakers should create a trust mark for secure IoT products. A trust mark would increase consumers' capability to discriminate between insecure devices. Such mark, would also raise the public awareness about cybersecurity issues. Several of the interviews from our study also mentioned the possibility of developing a trust mark for consumer.
- **Security Principle Compliant:** Policymakers should require that consumer IoT devices must comply with a set of generalized security principles such as necessary software/firmware updates, preclude easily-guessable passwords, and manufacturers complying with vulnerability disclosure action.
- **Prosecute Misleading Claims:** Policymakers should prosecute companies that create misleading claims on security. This measure would incentivize firms to either increase security or better information about their products.

- **Mandated Security Standards:** If the above actions are not effective, regulators could mandate a minimum set of security requirements for IoT devices.

In particular, few experts in our study believe that the lack of security in IoT can be corrected only if the government mandate for security. On the other hand, expert F reported: "*I think that if you have to be forced by regulations to implement security, that is exactly the same as not caring about security. If firms do security because they have to, that is the wrong motivation to do security. I believe that companies need to enhance security not because they have to but because they want to. I think that needs to happen with IoT*".

Finally, it is important to acknowledge that the risk from vulnerable IoT devices is a global problem given that countries face risks from insecure devices in other regions. The growth in IoT connected devices across the world will increase security and privacy issues if action is not taken. For this reason, national and cross-national multi-actor efforts, should be encouraged where possible to enhance the security of consumer IoT devices.

Chapter 6 – Conclusions

This study provides a first look into the potential of BBP and RD for IoT vulnerability management. Besides sharing insights on integration path, we also reveal hidden pitfalls and blind spots that deserve special attention from IoT stakeholders. As a solid step to demystify the potential of crowdsource ethic hacking for IoT, our work tackled the major research question, "How can developers, manufacturers, and vendors of consumer IoT products enhance vulnerability management practice with Bug Bounty Programs and Responsible Disclosure?". For IoT vulnerability management, our recommendation is to launch BBP only after companies have performed initial security testing and fixed the problems. The objective of BBP and RD policies should always be to provide additional support in finding undetected vulnerabilities, and never to be the only security practice. Follow-up procedures also need to be defined when vulnerabilities are found. Our findings raise the awareness on IoT security and present the global risk from vulnerable IoT devices. The growth in IoT connected devices across the world will likely increase security and privacy issues. For this reason, we call for further action from companies, consumers and regulators, for a multi-effort, to enhance the security of consumer IoT devices.

6.1 Academic contribution

There are multiple ways in which this study contributes to academic research. Firstly, little research is currently available on the topic of Bug bounties and Responsible disclosure. This thesis extends the academic work in this field and presents various insights on BBPs and RDPs. In particular, regarding the current state of adoption, benefits, limitations, barriers, solutions, and best practices. These topics were covered based on the consolidation and comparison of data from other studies and from interviews with experts in the field. Secondly, the combination of IoT security with crowdsource presented a completely novel research field. We believe that all the results presented on RDP and BBP in the field of IoT consist of very interesting material for the industry, but also scientific world.

6.2 Practical contribution

The presented research provides several tangible recommendations and potentially new options for stakeholders to tackle IoT-oriented vulnerabilities in consumer goods, which will help enhance the overall IoT security practices. The results present several recommendations for organizations from experienced security consultants that can be used to improve security practices. Moreover, the study demonstrates the threats posed to the security and privacy of people by the state of vulnerable IoT devices. Our findings raise the awareness on IoT security and present a call for further actions from companies, consumers and regulators in the consumer IoT domain.

6.3 Final Reflection

This thesis project has made several contributions, of both scientific and practical value. Previous research has investigated the potential of crowdsourced security methods. But this project, is the first that investigated the application RD and BBPs for IoT vulnerability management. Therefore, a void in the literature is addressed. The collaboration with Deloitte has been key, and made it possible to collect the valuable opinion of experienced security consultants. Moreover, we collected additional insights on the research topic by attending security conferences to seek qualified interviews. We acknowledge that crowdsourced security is still an avant-garde topic in the cybersecurity industry. For this reason, application is still limited and scientific research is scarce. Having more time, we would have attended more security events to encounter more field experts and companies involved with crowdsourced security.

6.4 Limitations

In this qualitative study, one limitation is that only experts that were conveniently available participated in the interview. Within judgmental sampling, there is a risk of selection bias. Therefore, the generalizability of our findings to the entire population should be done with care. In addition, it is worth noting that our sample is based on a population of security experts working as security advisors. Consequently, our research takes the point of view of experts that are generally providing solutions to companies that face security problems. We did not yet include in our study experts from other types of companies, and they might have a different view on the problems.

6.5 Future research

The results of this thesis are based on interviews with cybersecurity experts. In terms of future research, further empirical research might be conducted to investigate the perception of companies adopting BBPs and RDPs in IoT to assess the generalizability of our results. Moreover, follow up studies can be conducted to investigate the validity of our analyses. A possibility would be extending the same type of study to a broader population of experts, to leverage additional data sources. Lastly, the solutions that we identified for BBPs in IoT have never been mentioned by any research in the field and need to be further explored.

Bibliography

Asplund, M., & Nadjm-Tehrani, S. (2016). Attitudes and perceptions of IoT security in critical societal services. IEEE Access, 4, 2130-2138.

Bacchus, A. (2017). Bug bounty field manual. How to Plan, Launch, and Operate a Successful Bug Bounty Program (Rep.).

Baloch, R., (2014). Ethical hacking and penetration testing guide. Auerbach Publications.

Barriball, K. L., & While, A., (1994). Collecting data using a semi-structured interview: a discussion paper. Journal of Advanced Nursing-Institutional Subscription, 19(2), 328-335.

Ben-Shlomo, Y., Brookes S., Hickman M., (2013). Lecture Notes: Epidemiology, Evidence-based Medicine and Public Health (6th ed.), Wiley-Blackwell, Oxford.

Bertino, E., & Islam, N., (2017). Botnets and internet of things security. Computer, (2), 76-79.

Bing, C., (2017). How DJI fumbled its bug bounty program and created a PR nightmare. Retrieved from https://www.cyberscoop.com/dji-bug-bounty-drone-technology-sean-melia-kevin-finisterre/

Bouwman, H., (2018) “MOT2312 Qualitative Research”, MSc lecture, from TU Delft, Delft, 25/06/2018

Bugcrowd, (n.d.). What is Responsible Disclosure? Retrieved from https://www.bugcrowd.com/resource/what-is-responsible-disclosure/

Bugcrowd, (2015). The State of Bug Bounty. Retrieved form https://www.bugcrowd.com/resources/reports/state-of-bug-bounty-2018/

Bugcrowd, (2018). The Next Generation of Pen Testing - Crowdsourced Security. Retrieved from https://www.bugcrowd.com/the-next-generation-of-pen-testing-crowdsourced-security/

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2005). Emerging Issues in Responsible Vulnerability Disclosure. In WEIS.

Chandrika, V., (2014). Ethical hacking: Types of ethical hackers. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), 11(1).

Choi, J. P., Fershtman, C., & Gandal, N., (2010). Network security: Vulnerabilities and disclosure policy. The Journal of Industrial Economics, 58(4), 868-894.

Cois, C. A., Yankel, J., & Connell, A. (2014). Modern DevOps: Optimizing software development through effective system interactions. In 2014 IEEE International Professional Communication Conference (IPCC) (pp. 1-7). IEEE.

Deloitte, (2019). Tech Trends 2019 Beyond the Digital Frontier. Deloitte Insights. Retrieved from https://www2.deloitte.com/insights/us/en/focus/tech-trends.html

Deloitte, (2018). The Internet of Things A Technical Premier. Deloitte Insights. Retrieved from https://www2.deloitte.com/insights/us/en/focus/internet-of-things/technical-primer.html

DigiCert, (2018). State of IoT Security Survey 2018. Retrieved from https://www.digicert.com/wpcontent/uploads/2018/11/StateOfIoTSecurity_Report_11_02_18_F_am.pdf

DJI, (2019). Security Response Center. Retrieved from https://security.dji.com/

EC-Council, (2019). What is Ethical Hacking | Types of Ethical Hacking | EC-Council. Retrieved from https://www.eccouncil.org/ethical-hacking/#

Edureka! (2018). Internet of Things (IoT) Architecture. Retrieved from https://www.youtube.com/watch?v=FRxRT0DjE7A

European Commission, (n.d.). About EU-FOSSA 2. Retrieved from https://joinup.ec.europa.eu/collection/eu-fossa-2/about

Finifter, M., Akhawe, D., & Wagner, D., (2013). An Empirical Study of Vulnerability Rewards Programs. University of California, Berkeley. Paper presented at 22nd USENIX Security Symposium, Washington, DC.

Fruhlinger, J. (2018). "The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet." CSO Online, CSO, 9 Mar. 2018, www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html.

Gartner, Inc., (2017). IoT Technology Disruptions: A Gartner Trend Insight Report. By Ganguli, S., and Friedman, T.

Gartner, Inc., (2019). How to Select a Penetration Testing Provider. By Bussa, T., Neiva, C., and Bhajanka, P.

Gartner, Inc., (2018). Emerging Technology Analysis: Bug Bounties and Crowdsourced Security Testing. By Gardner D.

Gartner, Inc., (2018). Magic Quadrant for Application Security Testing. By Tirosh, A., Zumerle, D., and Horvath, M.

Gartner, Inc., (2017). Leading the IoT. Gartner Insights in How to Lead in a Connected World. Edited by Mark Hung, Gartner Research Vice President

Greenberg, A., (2015). Hackers Remotely Kill a Jeep on the Highway-With Me in It. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Hackerone, (2018). Vulnerability Disclosure Policy: What Is It, Why You Need One, and How To Get Started (Rep.).

Hackerone. (2018). Software Vulnerability Disclosure in Europe: Summary and Key Highlights of the European Parliament CEPS Task Force Report. Retrieved 2018, from https://www.hackerone.com/blog/Software-Vulnerability-Disclosure-Europe-Summary-and-Key-Highlights-European-Parliament-CEPS

Hackerone, (2019). The HackerOne Report. The Survey and Statistics of Ethical Hacker Community.

Hafeez, I., Ding, A. Y., Antikainen, M., & Tarkoma, S. (2018). Real-Time IoT Device Activity Detection in Edge Networks. In International Conference on Network and System Security (pp. 221-236). Springer, Cham.

Hafiz, M., & Fang, M. (2016). Game of detections: how are security vulnerabilities discovered in the wild?. Empirical Software Engineering, 21(5), 1920-1959.

Haus, M., Waqas, M., Ding, A. Y., Li, Y., Tarkoma, S., & Ott, J. (2017). Security and privacy in device-to-device (D2D) communication: A review. IEEE Communications Surveys & Tutorials, 19(2), 1054-1079.

Hewlett Packard, (2014). HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Retrieved from https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VOTykPnF-ok

Hoepfl, M. C. (1997). Choosing qualitative research: A primer for technology education researchers. Volume 9 Issue 1 (fall 1997).

Höst, M., Sönnerup, J., Hell, M., & Olsson, T. (2018). Industrial practices in security vulnerability management for iot systems – an interview study. In Proceedings of the International Conference on Software Engineering Research and Practice (SERP) (pp. 61-67). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

IoT For All., (2017). The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History. Retrieved from https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/

IoT ONE., (n.d.). Stakeholder. Retrieved from https://www.iotone.com/term/stakeholder/t669

Jansen, H. (2010). The logic of qualitative survey research and its position in the field of social research methods. In Forum Qualitative Sozialforschung/Forum: Qualitative Social Research (Vol. 11, No. 2).

Just, S., Premraj, R., & Zimmermann, T. (2008). Towards the next generation of bug tracking systems. 2008 IEEE Symposium on Visual Languages and Human-Centric Computing. doi:10.1109/vlhcc.2008.4639063

Kassarjian, H. H. (1977). Content Analysis in Consumer Research. Journal of Consumer Research, 4(1), 8. doi:10.1086/208674

Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. In 2012 10th international conference on frontiers of information technology (pp. 257-260). IEEE.

Krishnamurthy, S., & Tripathi, A. K. (2006). Bounty programs in free/libre/open source software. In The Economics of Open Source Software Development (pp. 165-183). Elsevier.

Kuehn, A., & Mueller, M., (2014). Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities. SSRN Electronic Journal. doi:10.2139/ssrn.2418812

Laszka, A., Zhao, M., & Grossklags, J. (2016). Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms. Computer Security – ESORICS 2016 Lecture Notes in Computer Science,161-178. doi:10.1007/978-3-319-45741-3_9

Laszka, A., Zhao, M., Malbari, A., & Grossklags, J. (2018). The rules of engagement for bug bounty programs. Extended version http://aronlaszka. com/papers/laszka2018rules. pdf (February 2018).

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 336-341). IEEE.

McFadden, M., Wood, S., Mangtani, R., & Forsyth, G. (2019). The economics of the security of consumer-grade IoT products and services. Internet Society. Retrieved from https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/

Microsoft, (n.d.). Microsoft Security Development Lifecycle. Retrieved from https://www.microsoft.com/en-us/securityengineering/sdl

Miles, M. B., & Huberman, A. M., (1994). Qualitative data analysis an expanded sourcebook. Thousand Oaks: SAGE.

Noble, H., & Smith, J., (2015). Issues of validity and reliability in qualitative research. Ev-idence-based nursing, 18(2), 34-35.

O'Neill, M. (2016). Insecurity by design: Today's IoT device security problem. Engineering, 2(1), 48-49.

OWASP, (2014). OWSAP Top Ten Internet of Things Vulnerabilities 2014. Retrieved from https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

OWSAP, (2018). OWASP Top Ten Internet Of Things Vulnerabilities 2018. Retrieved from https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf

OWASP, (2019). About The Open Web Application Security Project. Retrieved from https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

Pawar, A. B., & Ghumbre, S. (2016). A survey on IoT applications, security challenges and counter measures. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 294-299). IEEE.

Pen Test Partners (2018). Why is consumer IoT insecure? Retrieved from https://www.pentestpartners.com/security-blog/why-is-consumer-iot-insecure/

Rescorla, E. (2005). Is finding security holes a good idea?. IEEE Security & Privacy, 3(1), 14-19.

Rouse, M., (n.d.). What is pen test (penetration testing)? - Definition from WhatIs.com. Retrieved from https://searchsecurity.techtarget.com/definition/penetration-testing

Sauro, J., (2015). 5 Types of Qualitative Methods. MeasuringU. Retrieved from https://measuringu.com/qual-methods/

Sbaraini, A., Carter, S. M., Evans, R. W., & Blinkhorn, A. (2011). How to do a grounded theory study: a worked example of a study of dental practices. BMC medical research methodology, 11(1), 128.

Sekaran, U., (2000). Research methods for business: A skill-building approach. New York: J. Wiley.

Shahzad, M., Shafiq, M. Z., & Liu, A. X. (2012). A large scale exploratory analysis of software vulnerability life cycles. In 2012 34th International Conference on Software Engineering (ICSE) (pp. 771-781). IEEE.

Singh, J., Pasquier, T., Bacon, J., Ko, H., & Eyers, D. (2016). Twenty security considerations for cloud-supported Internet of Things. IEEE Internet of things Journal, 3(3), 269-284.

Smith, J. A., (2015). Qualitative psychology: A practical guide to research methods. Sage.

SoK, (n.d.). IoT Security Trends - SoK: Understanding IoT Security. Retrieved from https://sites.google.com/site/iotsecsok/iot-security-trends

Streubert, H. J., & Carpenter, D. R. (1999). Qualitative research in nursing: Advancing the humanistic imperative.

Symantec, (2016). IoT devices being increasingly used for DDoS attacks. Retrieved from https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks

Synac, (n.d.). Crowdsourced vs. Traditional Penetration Testing. Retrieved from https://www.srctechnologies.com/files/2018/05/Synack_vs_PenTest_042117.pdf

Technopedia, (2019). What is Hacking? - Definition from Techopedia. Retrieved from https://www.techopedia.com/definition/26361/hacking

Technopedia. (n.d.). What is a Denial-of-Service Attack (DoS)? - Definition from Techopedia. Retrieved from https://www.techopedia.com/definition/24841/denial-of-service-attack-dos

Ted Talks, (2018). Internet of Things Security | Ken Munro | TEDxDornbirn. Retrieved May 18, 2019, from https://www.youtube.com/watch?v=pGtnC1jKpMg

TechTarget, (n.d.). What is vulnerability management? - Definition from WhatIs.com. (n.d.). Retrieved from https://whatis.techtarget.com/definition/Vulnerability_management

Terrill, C. (2018). Is Your Company Ready For A Bug Bounty Program? Forbes. Retrieved from https://www.forbes.com/sites/christieterrill/2018/09/05/is-your-company-ready-for-a-bug-bounty-program/

TU Delft (n.d.). MSc Management of Technology. Retrieved from https://www.tudelft.nl/onderwijs/opleidingen/masters/mot/msc-management-of-technology/

Zhang, N., Demetriou, S., Mi, X., Diao, W., Yuan, K., Zong, P., ... & Gunter, C. A., (2017). Understanding IoT security through the data crystal ball: Where we are now and where we are going to be. arXiv preprint arXiv:1703.09809.

Zhao M., Laszka A., & Grossklags J., (2017). Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery. Journal of Information Policy,7, 372. doi:10.5325/jinfopoli.7.2017.0372

Zhao, M., Laszka, A., Maillart, T., & Grossklags, J. (2016). Crowdsourced Security Vulnerability Discovery: Modeling and Organizing Bug-Bounty Programs.

Appendix

1. Interview Guide

Interview Guide for Enhancing Vulnerability Management for IoT with Bug Bounty Programs and Responsible Disclosure – by Gianluca Limon De Jesus	
Interview opening	Interviewer present himself, present the research, and obtain consent for audio recording.
Interview questions	
A) On IoT security risks, perceptions and measures	
Questions	Notes
1. To what extent is security perceived as an important issue by companies that design, develop, and sell IoT products in the consumer goods market?	If it is not, why not?
2. Is there any difference in the way companies address security based on factors such as the firm's size, age, or industry?	
3. To what extent do companies have a define process for vulnerability management when it comes to IoT products?	If not, why not? If yes, what process?
4. What should be possible best practices by companies to identify and evaluate vulnerabilities in IoT?	
B) On the application of crowdsourced security methods in IoT	
Questions	Notes
5. Do you believe that Bug Bounty Programs and Responsible Disclosure can improve vulnerability management practices in IoT systems?	If yes, how? If no, why?
6. For what purpose should companies adopt one or the other?	
7. To what extent do companies adopt responsible disclosure policies?	If not, why not?
8. How can companies leverage responsible disclosure to enhance vulnerability management practices in IoT?	
9. To what extent do companies adopt bug bounty programs with IoT products?	If not, why not?
10. How can companies leverage Bug bounty programs to enhance vulnerability management practices in IoT?	

11. According to HackerOne, at the moment only 1.6% of bug bounty programs have to do with IoT. What are obstacles for the adoption of BBPs in IoT?	
12. To what extent should companies make use of intermediary platforms (e.g. HackerOne)?	How?
13. Gartner predicts that by 2022, 50% of companies will be adopting BBPs, what would benefit the broader use and adoption of responsible disclosure and bug bounties in IoT? What would benefit the broader adoption of BBPs and related services at the moment?	
C) Conclusion	
Question	Notes
14. Do you have any other comment or remark about this interview?	

2. Questionaire for Attitudes and Perceptions of IoT Security in Critical Societal Services – By Asplund, M., & Nadjm-Tehrani, S. (2016).

General background questions

What is your formal role in the organisation?

What types of customers/clients does the organisation have?

Approximately how many customers/clients do you have?

Questions on IoT

What do you associate with the term ”Internet of Things”?

Is IoT relevant in your field on a 5-10 year horizon?

a) Followup question if no: Do you not consider X to be part of IoT?

Can you see IoT contributing value to your sector (within 5-10 years)?

a) New services

b) Better services

c) Reduced costs

d) PR and marketing

e) Other

What factors do you believe will enable faster integration of IoT in your field?

a) Improved technical solutions

b) Knowledge of customers and operators

c) Guidelines for deployment of IoT

d) Regulation

e) Lower costs

f) Other

What are the obstacles to introduction of IoT in your sector?

a) Lack of security / reliability

b) Costs

c) Maintenance

d) Unproven technology

e) Lack of usability

f) Lack of know-how

g) Regulation

h) Other

Risks, threats and critical infrastructure

What risks or threats to you associate with IoT in your sector?

How severe do you rank the risk (low, medium, high) of:

a) Communication failure

b) Power failure

c) Failing equipment

d) Data loss

e) Confidentiality loss

f) Integrity loss

g) Deliberate hacking

h) Malicious code

What is the reliability/availability of power and communication to your critical operations today?

a) How well are your communication requirements met by your current Internet connection?

What do you think the requirements on power and communication will be in 2025?

What kind of measures/actions are needed to deal with the potential obstacles/risks that you have identified and thereby enable a faster adoption of IoT?

Do you have any final comments?

3. Questionnaire for Industrial Practices in Security Vulnerability Management for IoT Systems – an Interview Study, by Martin Höst (2018)

A) Background about the company and the product

A.1 Interviewer present themselves, presentation of study, and obtain consent (incl. audio record)

A.2 Interviewee presents him/herself

A.3 Tell us more about the product (architecture, functionality, customers, degree of OSS)

A.4 Tell us more about the company (age, maturity, history) <short!>

A.5 Tell us more about the development process, and the update process.

- Which roles (integrator, end-user, sysadmin, support, etc.) are involved in the update process and what do they do?

A.6 Where in IoT architecture [sensor/actuator, gateway, cloud, UI]?

A.7 Where in value chain [component producer, integrator, owner, support system developer, other]?

A.8 To what extent is security important for the product and in the development? What goals can attackers have for your product?

A.9 What type of attacks do you think is the largest threat for you?

A.10 Anyone responsible for security?

B) Questions about identification and evaluation (focus on OSS, but proprietary can also be discussed)

B.1 How do you identify vulnerabilities? I.e what process?

Who is responsible for identification? I.e. what is the organization?

- project management involvement?

- architect involvement?

- support/maintenance involvement?

B.1 If you don't identify vulnerabilities in any structured way,

- why not? conscious decision? what about the future?

- who do you think should do this? - how should it be done?

B.3 Based on what information do you identify vulnerabilities?

- chat, forum, mailing list

- CVE database, NVD, technical news

- Paid service? E.g. some consultancy firm?

B.4 How is evaluation done (process)?

- who evaluates? - What factors? - who takes decisions? - how are security issues prioritized vs other work? - formal decision forum?

B.5 What kind of information would you need in order to better assess vulnerabilities?

- for better decision quality

- for faster decisions

B.6 How do you communicate decision outside the company, with whom do you communicate?

B.7 To what extent is experience and knowledge from earlier evaluations used?

- documentation?

- Knowledge management system?

B.8 Do you follow up to what extent your decisions are correct?

- if yes, how?

- if no, why not?

C) Questions about implementation/distribution of changes (focus on OSS, but proprietary can also be discussed)

C.1 How is implementation/patching done? Relation to other development processes?

- What roles are involved in the decision? (product management, project management, architect, support/maintenance, customer support)

- Differences compared to other maintenance?

C.2 How would you like to implement changes? what main improvements can you see?

C.3 How is delivery/deployment carried out?

- Do you keep track of updated products (device management)?

- Push from central server, pull from devices, need physical person to go to each IoT device

D) Questions about quality indicators

D.1 How high is the confidence that decisions made about vulnerabilities are correct?

- How many % of these decisions are correct (your estimate)?

D.2 How much relative effort (and relative lead time) do you spend on

> identification

> evaluation & decision

> implementation

> V&V

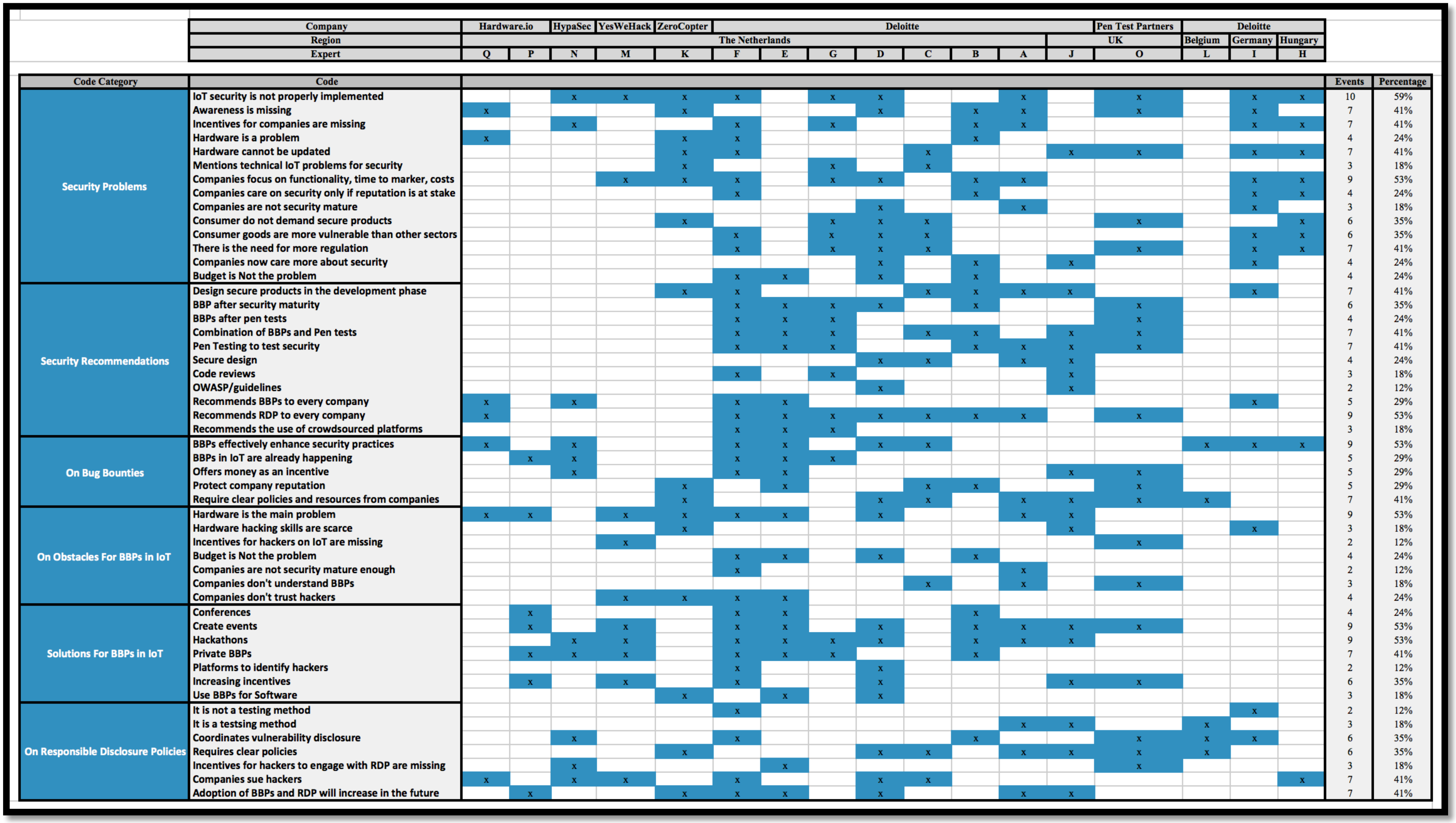
> deployment

- what major changes do you want to make?

D.3 What fraction of the developers have insight about how to take action when new vulnerabilities are discovered?

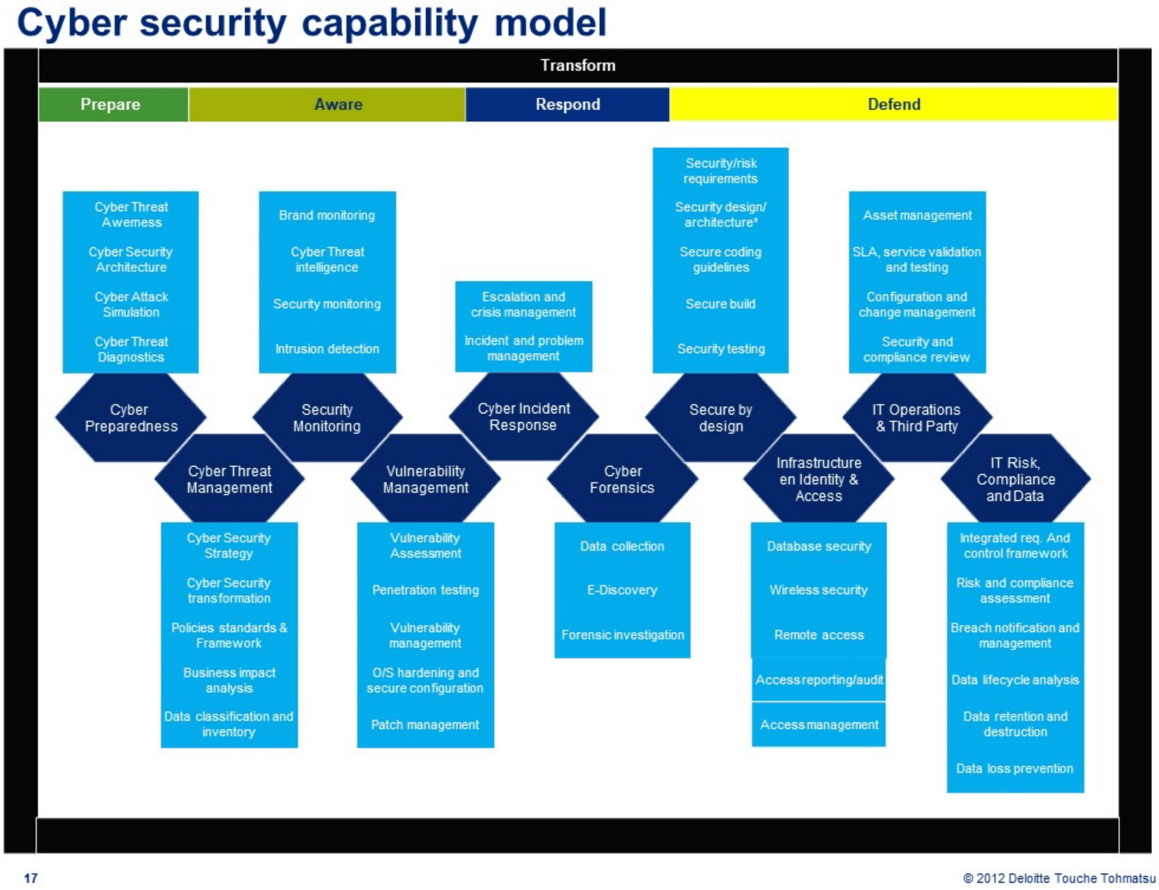
- what fraction do you want?

4. Coding Table



	Company	Hardware.io		HypaSec	YesWeHack	ZeroCopter	Deloitte								Pen Test Partners	Deloitte				
	Region	The Netherlands												UK		Belgium	Germany	Hungary		
	Expert	Q	P	N	M	K	F	E	G	D	C	B	A	J	O	L	I	H		
Code Category	Code																		Events	Percentage
Security Problems	IoT security is not properly implemented			x	x	x	x		x	x			x		x		x	x	10	59%
	Awareness is missing	x				x				x		x	x		x		x		7	41%
	Incentives for companies are missing			x			x		x			x	x				x	x	7	41%
	Hardware is a problem	x				x	x					x							4	24%
	Hardware cannot be updated					x	x				x			x	x		x	x	7	41%
	Mentions technical IoT problems for security					x			x		x								3	18%
	Companies focus on functionality, time to marker, costs				x	x	x		x	x		x	x				x	x	9	53%
	Companies care on security only if reputation is at stake						x					x					x	x	4	24%
	Companies are not security mature									x			x				x		3	18%
	Consumer do not demand secure products					x			x	x	x				x			x	6	35%
	Consumer goods are more vulnerable than other sectors						x		x	x	x						x	x	6	35%
	There is the need for more regulation						x		x	x	x				x		x	x	7	41%
	Companies now care more about security									x		x		x			x		4	24%
	Budget is Not the problem						x	x		x		x							4	24%
Security Recommendations	Design secure products in the development phase					x	x				x	x	x	x			x		7	41%
	BBP after security maturity						x	x	x	x		x			x				6	35%
	BBPs after pen tests						x	x	x						x				4	24%
	Combination of BBPs and Pen tests						x	x	x		x	x		x	x				7	41%
	Pen Testing to test security						x	x	x			x	x	x	x				7	41%
	Secure design									x	x		x	x					4	24%
	Code reviews						x		x					x					3	18%
	OWASP/guidelines									x				x					2	12%
	Recommends BBPs to every company	x		x			x	x									x		5	29%
	Recommends RDP to every company	x					x	x	x	x	x	x	x		x				9	53%
	Recommends the use of crowdsourced platforms						x	x	x										3	18%
On Bug Bounties	BBPs effectively enhance security practices	x		x			x	x		x	x					x	x	x	9	53%
	BBPs in IoT are already happening		x	x			x	x	x										5	29%
	Offers money as an incentive			x			x	x						x	x				5	29%
	Protect company reputation					x		x			x	x			x				5	29%
	Require clear policies and resources from companies					x				x	x		x	x	x	x			7	41%
On Obstacles For BBPs in IoT	Hardware is the main problem	x	x		x	x	x	x		x			x	x					9	53%
	Hardware hacking skills are scarce					x								x			x		3	18%
	Incentives for hackers on IoT are missing				x										x				2	12%
	Budget is Not the problem						x	x		x		x							4	24%
	Companies are not security mature enough						x						x						2	12%
	Companies don't understand BBPs										x		x		x				3	18%
	Companies don't trust hackers				x	x	x	x											4	24%
Solutions For BBPs in IoT	Conferences		x				x	x				x							4	24%
	Create events		x		x		x	x		x		x	x	x	x				9	53%
	Hackathons			x	x		x	x	x	x		x	x	x					9	53%
	Private BBPs		x	x	x		x	x	x			x							7	41%
	Platforms to identify hackers						x			x									2	12%
	Increasing incentives		x		x		x			x				x	x				6	35%
	Use BBPs for Software					x		x		x									3	18%
On Responsible Disclosure Policies	It is not a testing method						x										x		2	12%
	It is a testsing method												x	x		x			3	18%
	Coordinates vulnerability disclosure			x			x					x			x	x	x		6	35%
	Requires clear policies					x				x	x		x	x	x	x			6	35%
	Incentives for hackers to engage with RDP are missing			x				x							x				3	18%
	Companies sue hackers	x		x	x		x			x	x							x	7	41%
	Adoption of BBPs and RDP will increase in the future		x			x	x	x		x			x	x					7	41%

5. Deloitte Cyber Security Capability Framework



Cyber security capability model

Transform

Prepare

Aware

Respond

Defend

Cyber Threat Awerness

Cyber Security Architecture

Cyber Attack Simulation

Cyber Threat Diagnostics

Cyber Preparedness

Cyber Threat Management

Cyber Security Strategy

Cyber Security transformation

Policies standards & Framework

Business impact analysis

Data classification and inventory

Brand monitoring

Cyber Threat intelligence

Security monitoring

Intrusion detection

Security Monitoring

Vulnerability Management

Vulnerability Assessment

Penetration testing

Vulnerability management

O/S hardening and secure configuration

Patch management

Escalation and crisis management

Incident and problem management

Cyber Incident Response

Cyber Forensics

Data collection

E-Discovery

Forensic investigation

Security/risk requirements

Security design/ architecture*

Secure coding guidelines

Secure build

Security testing

Secure by design

Infrastructure en Identity & Access

Database security

Wireless security

Remote access

Access reporting/audit

Access management

Asset management

SLA, service validation and testing

Configuration and change management

Security and compliance review

IT Operations & Third Party

IT Risk, Compliance and Data

Integrated req. And control framework

Risk and compliance assessment

Breach notification and management

Data lifecycle analysis

Data retention and destruction

Data loss prevention

17

© 2012 Deloitte Touche Tohmatsu

6. Crowdsourced Security Testing Programs According to Gartner Inc, (2018)

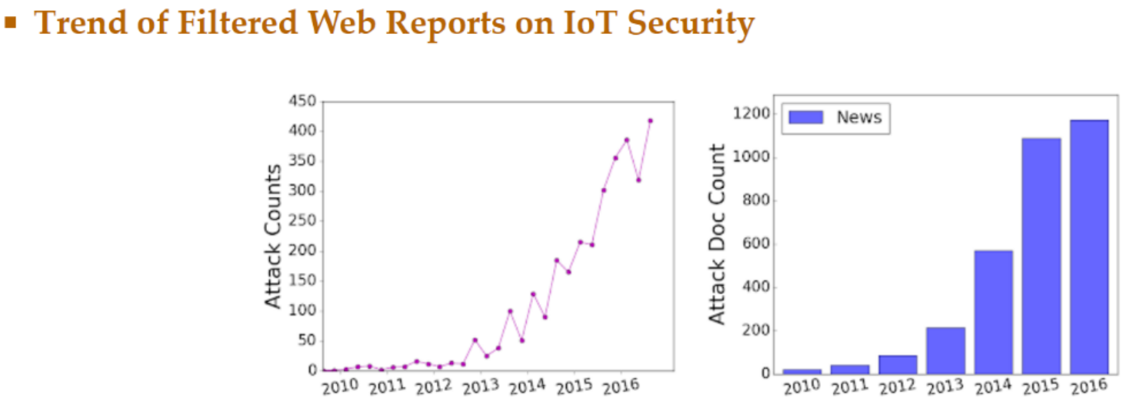
Community Programs: Large-scale bug bounty programs open to all members of a CSSTP vendor's security research community. In many regards, these programs mimic classic bug bounty programs. Vetting and evaluation of researchers vary from limited or essentially nonexistent, to extremely thorough. Entry into the community may be available to virtually all comers. Such programs are typically time-limited in duration, although they may also be ongoing. In the latter case, the program may well fall under the purview of a responsible disclosure program, as described below (Gartner Inc, 2018).

Public/Private Programs: These represent a more constrained and narrowly scoped bug bounty. Although such programs may be open to all members of a CSSTP vendor's security research community, these programs are more often limited to an invited subset of the community. Individuals may be sought out based on overall skills level, familiarity with a particular technology (for example, Internet of Things [IoT], automotive, mobile and specific application frameworks). Programs are usually tightly scoped in both their duration and the specific elements of an application to be tested. Specific areas of the application, or classes of vulnerabilities, may be considered out of scope. In some respects, such engagements are more similar to traditional penetration or red team testing efforts, and may be conducted early in the development cycle (that is, during unit or preproduction testing). Given the more constrained, and presumably better vetted, nature of the crowd, such programs are likely to appeal to firms specifically concerned about exposing intellectual property or sensitive data (Gartner Inc, 2018).

Responsible Disclosure Program Management: It's increasingly important organizations operate responsible disclosure programs (particularly, technology vendors and organizations that are highly dependent on technology and applications for delivery of products and services). These programs — which provide for the timely receipt, evaluation and response to vulnerability reports — provide a means for researchers to coordinate the disclosure of security vulnerabilities (and, ideally, their mitigation) with the vendors responsible for the flaw. Such programs are considered a vulnerability management best practice, and were included in the most recent draft of the U.S. NIST Cybersecurity Framework, the more widely known name for the Framework for Improving Critical Infrastructure Cybersecurity. This voluntary program is aimed at increasing the protection and resilience of critical infrastructure (Gartner Inc, 2018).

Management Platform: Originally, most bounty program management platforms were directed more toward security researcher participants, and provided information such as leaderboards (enabling an element of gamification) and information about available bounties. The scope of these platforms has expanded, and is becoming a critical component of a bug bounty program offering. Evolving systems now allow both researchers and bounty sponsors to perform a number of tasks. These include tracking the progress of researchers, assessing code coverage, controlling the scope researcher access to specific application components, and providing visibility to both security researchers and the buyers of discovered vulnerabilities and their status (Gartner Inc, 2018).

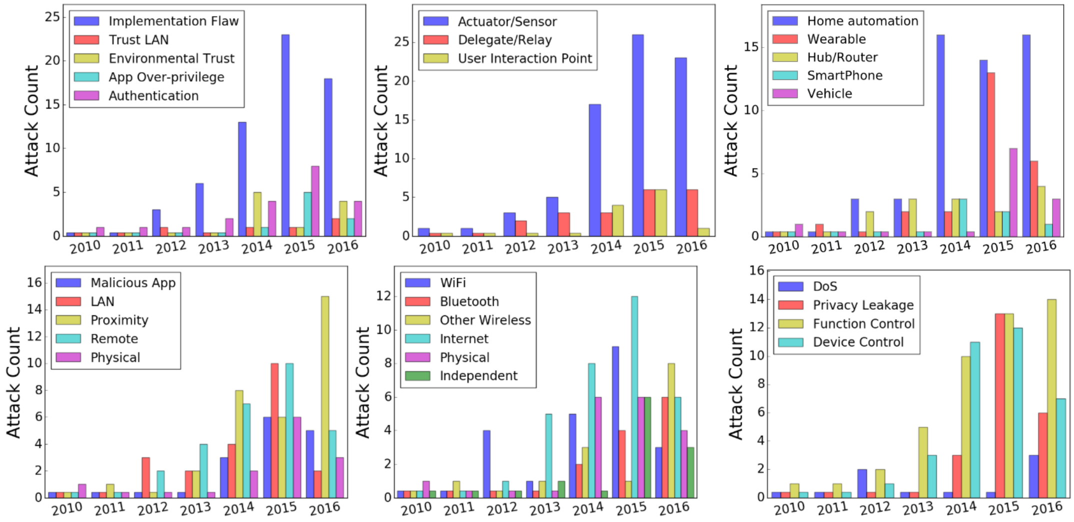
7. Panoramic Data Collection On 107 Unique IoT Attack Incidents Spanning From 2010 To 2016 IoT Attacks Reported In The Literature And Online. (Zhang, et al., 2017).



- Trend of Filtered Web Reports on IoT Security

Number of documented attack episodes reported on web reports (on the left) and of news on attacks (on the right).

- **Distribution By Year**



Each number on the vertical axes corresponds to the number of attack episodes counted for each category reported in the legend.